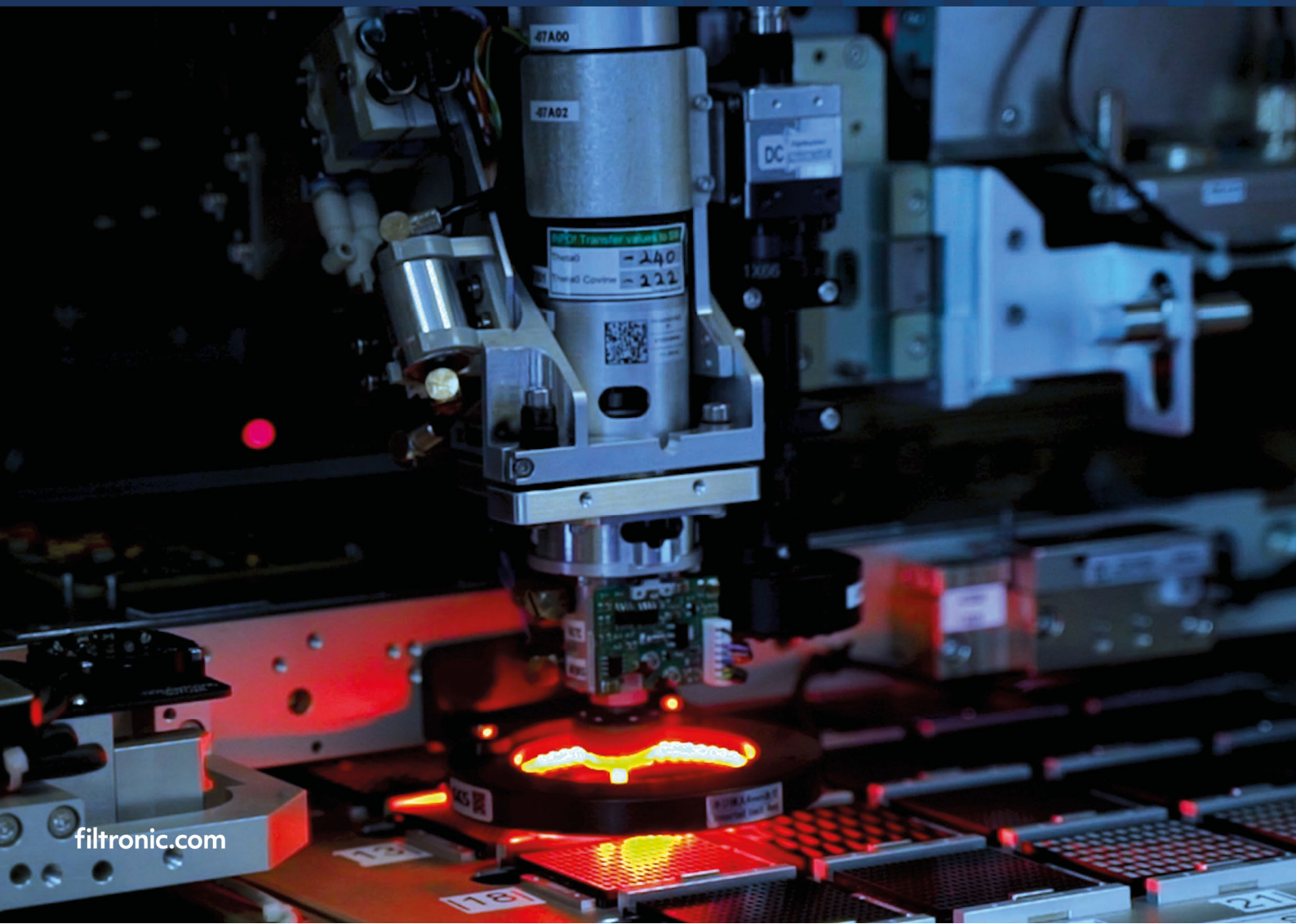
filtronic

November 2023

Group Values and Policies



filtronic.com

Contents

Filtronic plc

Introduction to Filtronic Group Values and Policies

Each of the policies within this document, the Filtronic Group Policies, are relevant to Filtronic plc ("the Company", "Filtronic" or "the Group") and all of its subsidiaries and associates.

Filtronic plc places a strong emphasis on promoting a culture that is based on ethical values and behaviours. We want to be a good corporate citizen and a trusted partner for our shareholders, customers, employees and other stakeholders. We are, therefore, committed to responsible corporate behaviour and compliance with all laws, regulations and other requirements that govern the conduct of our operations.

Whilst the Group Policies provide guidance on how we are to act in an ethical and compliant way, the Filtronic plc board recognises it is not possible to cover every situation that may arise in the day to day running of the business. Accordingly, the Board has defined and adopted a set of corporate values that are intended to guide the objectives, strategy and operation of the Company and be reflected in the behaviour of every employee.

The Filtronic Values and Behaviours can be found on our website and overleaf in this document. They act as a complement to the Group Policies. It is the responsibility of each employee to use their sound judgement in both implementing the policies and acting in line with them in the execution of your everyday work. Filtronic expects employees to conduct themselves, at all times, in a trustworthy and appropriate manner so as not to discredit or harm the Company.

Filtronic believes that a strong ethical culture depends in part upon creating an environment in which employees feel free to report instances of non-compliance of our Group Policies. We encourage all employees to be open and honest and report any breach of these Group Policies to management as soon as possible so corrective action can be taken quickly. By demonstrating our core value of integrity and reporting issues, we can tackle issues head on and resolve the matter in a positive way to become a stronger organisation. However, whilst very rare, some breaches or a deliberate failure to report a breach, may result in disciplinary action and/or criminal penalties depending on the seriousness.

If you have any suggestions in relation to the Group Policies and indeed comments on the Filtronic Values, and/or how they are recognised and respected, please speak to or email the Company Secretary, Head of HR or indeed myself.

Richard Gibbs
Chief Executive Officer
May 2023

Filtronic plc

Filtronic Values and Behaviours

We all wish to be thought of as "being of good character".

However, our character is not measured by the values we espouse, but by the values we demonstrate we live by and are guided by through our behaviour.

It is not enough to write a "Values & Behaviours Statement" and expect others to see us this way, we must be seen to be living them, or their very purpose is undermined.

Filtronic employs a special kind of person. They are experts in their field, confident communicators who love to collaborate, solve problems, and step up to a challenge.

At Filtronic, we aspire to live by, and demonstrate through our behaviour, the following fundamental values:

Integrity	Act with integrity; being honest and fair, always keeping our promises. Do the right thing, not the easy thing, speak up if it's not right. Deliver on your promises. Be truthful, always being honest and open. Be fair and ethical in your work and decision making. Take responsibility for your own actions, learn from mistakes when they happen.
Respect	Be respectful to all; it is the foundation of our culture. Be inclusive, always respecting and valuing others. Act how you want to be treated; being kind, considerate and respectful of others and their opinions. Be supportive and positive in all your working relationships. Value the importance of equality, diversity and inclusivity. Be open-minded and upfront with people.
Excellence	Strive for excellence; it is what our clients and colleagues expect and what we endeavour to deliver. Perform to the highest professional standards. Be innovative and pragmatic with problem solving. Take pride in our work, paying attention to detail. Be agile and flexible in your approach. Be curious and challenge constructively to improve how we work.

Living these values every day in our work is a tough ask. However, the more we aspire to do so, the more we will, and the better we will become as a business, as a partner to our external stakeholders and as a place to work with pride.

Our Purpose:	To be the trusted provider of innovative RF solutions.
Our Vision:	Enabling the future of RF, microwave and mmWave communication.
Our Mission:	Creating value for our clients through technology leadership.

Approved by the Board of Filtronic plc
May 2023

Filtronic plc

Code of Ethics

The Filtronic Code of Ethics applies to all employees including permanent and temporary staff, interns, secondees and staff provided by staffing agencies. It is important that everyone who this Code applies to has read it and understands it. Filtronic also expects its suppliers and other business partners to conduct themselves in the same manner.

This code provides guidance on how to act in certain situations but above all:

1) We are open and honest
2) We comply with all applicable laws and regulation
3) We do not engage in anti-competitive activity, bribery or corruption
4) We protect our company information and confidential information shared with us
5) We follow good standards of corporate governance and do not abuse market regulations

Legal Compliance
The Company will comply with all applicable laws and regulations and requires that all its employees conduct business in accordance with the law.

Conflict of Interest
Conflicts of interest can arise when our personal, family, financial, political or other interests interfere or conflict with our loyalty to the Company or our ability to make the right decisions on behalf of Filtronic. If an employee believes there is, or may be, an actual or perceived conflict of interest, we expect them to disclose it as soon as it has been identified so it can be considered and the right action taken. In many cases, simply disclosing the conflict to Management will be enough to resolve the problem but in more complex situations further action may be needed.

To mitigate conflict of interest, employees should avoid any relationships, influence or activity that might impair their ability to make fair and objective decisions when performing their job.

(Please see the separate Conflict of Interest Policy for more information).

Confidential Information
Employees must handle the property and information of the Company, its Customers and Suppliers with due care, in particular:

(i) Company Information should be treated as confidential; included in this are technical and financial data, company policies, procedures, letters, plans, drawings and computer programs, product developments, price and cost data and personal data.
(ii) Customer or Supplier Information should be treated as confidential except when this information has been obtained through publicly accessible sources, or when the Customer or Supplier explicitly releases the information.

Company Records and Data
Company Records and Data must be prepared accurately and honestly to represent the facts, meet regulatory requirements and comply with our internal controls.

Employees must understand that all work undertaken by them, including email, communications via any channel and content created under their employment belongs to Filtronic and, where legally permitted, may be accessed and used by the Company, even after you have left.

Ensure that the Security Controller and the IT Manager are aware before starting any new activity involving the collection of sensitive or personal information.

Data should only be kept in line with the Filtronic Data Retention Policy.

Procurement
Business will be awarded solely on the merits of the offered product or service; employees must not engage in any activity or allow any relationships to impair their judgment.

Gifts, gratuities, hospitality or favours of significant value must not be exchanged by employees with Customers or Suppliers except where they are publicly presented for noteworthy service or when explicitly authorised by an Executive Director.

(*Please see the Anti-Bribery and Corruption Policy for more information*).

Bullying and Harassment
The Company is committed to providing an organisation that is free from bullying and harassment in all its forms. Filtronic will work to ensure that its employees are treated in a respectful manner that acknowledges the dignity of each individual. Any alleged instance of such conduct should be reported to the appropriate management level or if necessary, through the whistleblowing procedure so that appropriate actions can be taken by the Company.

Quality
We are all responsible for ensuring that we sustain and grow the reputation of our brand by delivering the highest quality products and standards in all parts of our business.

Customer satisfaction is crucial, the extent to which the Company meets the needs and expectations of the Customers and the market they serve, shall be regularly reviewed.

(*Please see the separate policy on Quality*).

Health and Safety
We work safely, or not at all. We never walk by if we notice unsafe actions or situations.
We support health and wellbeing.

External Communication and Social Media

Everything we do, everything we say, and everything our stakeholders say about us can affect Filtronic's reputation. In a world where information travels in an instant, it is crucial we carefully manage communications with our external stakeholders, including investors, the media, customers and government representatives.

The Board are exclusively responsible for communication with investors whilst communication with the media including trade press must be approved by the Marketing department or an Executive Director. Employees should refer or seek approval before proceeding to engage with the media.

As a plc on the AIM market, employees and stakeholders must be aware that 'price sensitive' information capable of impacting the share price must not be communicated either externally or internally other than through an Executive Director. The consequences for the employee and the Company could lead to criminal convictions if not adhered to.

If employees want more information on communication, there is a detailed explanation in the Procedures and Authorities Manual ("PAM").

Outside of work, employees are strongly advised not to comment on social media platforms about the Company. Before you make a comment, you should ask yourself the question: "Could what I am saying have a negative impact on Filtronic or its stakeholders?" If the answer is yes, or possibly, you should not proceed.

(Please see the separate Social Media Policy).

Financial Controls and Risk Management:

A review of the effectiveness of the Company's internal controls shall be conducted at least annually and shall be documented and shall include financial operational and compliance controls and risk management systems.

Approved by the Board of Filtronic plc
May 2023

Filtronic plc

Management Policy

Management Code of Conduct

The directors of Filtronic plc ("the Company") and the directors and managers of each of the subsidiaries shall behave in relation to the Company (and subsidiaries as applicable) in a manner that complies with the statutory duties for directors as set out in the Company's Act 2006. In particular they shall: act within their powers for proper purposes; promote the success of the company; exercise independent judgement; exercise reasonable care, skill and diligence, avoid conflicts of interest; not accept benefits from third parties; declare interests (where such interests exist) in proposed transactions or arrangements.

Promoting Success

The management of Filtronic plc and of each of its subsidiaries shall manage the Company (and subsidiaries as applicable) in the way it considers, in good faith, would be most likely to promote the success of the Company for the benefit of members as a whole having regard to amongst other matters: the likely long-term consequences of decisions; interests of employees; need to foster business relationships with suppliers, customers and others; impact of company operations on the community and the environment; desirability of maintaining a reputation for high standards of business conduct and the need to act fairly between members.

Management shall determine the structure and operation most appropriate to achieve its business objectives within the Company's strategy and ensure compliance with the Company policies within the Code of Ethics.

Consultative Management

The process of planning, risk assessment, progressing, reviewing and reporting is applicable at all levels. Management will operate in a consultative manner; meetings and discussions shall involve all employees whose knowledge contributes to and whose skills and commitment is crucial to the execution of the task. The Company shall operate at all levels in a consultative manner.

Communication

Operational performance and progress against strategic targets shall be communicated regularly throughout the Company.

Financial Controls

The provisions of the financial Procedures and Authorisations Manual ("PAM") and the Distribution of Authority must be adhered to by all.

Risk Management

A review of the effectiveness of the Company's internal controls shall be conducted at least annually and shall include financial, operational and compliance controls and risk management systems.

Community Support

The Company shall engage with the communities within which it operates through, where appropriate, charitable donations (to be authorised at Board Level), sponsorship and participation in local educational and welfare initiatives.

Reports to the Group Board

The following should be brought to the attention of the Board of Directors of Filtronic plc without delay:

i. **Breach of the Code of Ethics**

Any breach which could adversely affect the Company's legal or ethical standing should be promptly reported.

ii. **Significant Customer Complaints and Product Liability Claims:**

Customer Complaints should be answered speedily, courteously and truthfully. The Company shall maintain a record of significant complaints (including product liability claims) and should promptly advise the Group Board of the background circumstances and of the steps taken to answer the complaint (or deal with the claim). Significant complaints or claims should, where possible, be expressed in writing by the Customer to avoid ambiguity or misunderstanding. The initial recipient of the complaint, or an appointee, shall be responsible for keeping the complainant advised of the progress of the complaint subject always to advice and guidance from the Company Secretary/General Counsel.

iii. **Contractual Terms:**

Any request to trade with the Company on terms other than Filtronic plc's standard conditions, within authorised limits, should be approved in line with the Distribution of Authority.

iv. **Whistleblowers:**
(Please see the separate policy on Whistleblowing).

Each Manager is responsible for the communication of the Filtronic plc PAM (and any updates thereof) and other governance documents including the Group Policies and the Distribution of Authority to all relevant employees within their reporting line.

Approved by the Board of Filtronic plc
May 2023

Filtronic plc

Employment Policy

Filtronic plc, its subsidiaries and business units shall abide by the following principles and expects its suppliers to abide by these or equivalent principles:

- **Child Labour**
  Not to condone or engage in the use of child labour or require persons below 18 years to work at night or in hazardous conditions. By child, we mean any person under 15 years of age, or older where there is a higher school leaving age, in which case the higher age applies. If the local law is set at 14 in accordance with developing-country exceptions under ILO Convention 138, this age applies.
- **Forced/Compulsory Labour**
  Not to condone or engage in the use of any form of compulsory or forced labour directly or indirectly such as by requiring personnel to lodge "deposits" or identity papers upon commencing employment with the Company.
- **Disciplinary Practices**
  The Company's disciplinary procedures shall not condone mental or physical coercion, verbal abuse, sexual or other harassment.
- **Working Hours**
  Shall comply with national laws. Required overtime and remuneration for overtime shall be specified in the individual's terms of employment.
- **Equal Opportunities and Diversity**
  To ensure equal treatment and not to condone or engage in discrimination in hiring, compensation, access to training and promotion, based on arbitrary criteria such as race, caste, national origin, religion, age, disability, gender, marital status, sexual orientation, union membership or political affiliation.
- **Freedom of Association and Collective Bargaining**
  To respect the rights of all staff to form and join trade unions of their choice and bargain collectively. If these rights are restricted under law, to facilitate the development of parallel means for independent and free association and collective bargaining.

Managers must ensure that relevant local legislative requirements are addressed and to brief, train and monitor compliance to these Policies.

Procedures should be generated, based upon the above, and reflect the legal requirements of the territories, within which we operate, and shall make those procedures accessible to all its employees.

Approved by the Board of Filtronic plc
May 2023

Filtronic plc

Diversity and Equal Opportunities Policy

Filtronic plc ("the Company") together with its subsidiary companies (herein "Filtronic") sets out its Diversity and Equal Opportunities Policy below.

This policy forms part of your Terms and Conditions of Employment. Failure to comply with this policy will be regarded as a breach of your contract of employment and could lead to disciplinary action.

Purpose

This policy applies to all colleagues, including contractors, agency workers and stakeholders of Filtronic. Filtronic is committed to promoting a culture where colleagues are supported, respected, valued for their difference (diversity) and treated consistently and fairly through equal opportunities for all.

Policy Principles

Filtronic will be guided by the requirements of the Equality Act (2010) and is committed to providing a working environment in which everyone feels valued and respected and is able to pursue a rewarding career whilst contributing to the success of our business. We will apply the standards set out in this policy and will establish monitoring and other supporting processes to ensure fair employment-related decisions. The main areas where these processes are established include: recruitment; career planning; promotion and transfer; training and personal development; performance management, redundancy, appropriate remuneration and general well-being.

In particular, we will maintain the explicit commitments set out in our Code of Conduct. It is our aim to provide equal opportunities for all without discrimination, directly or by association) on the grounds of:

- Race, ethnic origin, skin colour or nationality
- Religious or political beliefs and affiliations
- Sex, gender reassignment, or sexual orientation
- Marriage/civil partnership
- Age
- Disability
- Pregnancy or maternity
- Membership or non-membership of a trade union.

We aim to ensure that no-one in our business, or seeking employment with us, receives less favourable treatment on the above grounds or is disadvantaged by requirements or conditions which cannot be shown to be justifiable. In some countries in which we operate, local laws dictate that preference must be given to particular groups and this is a justifiable reason for discrimination. Access to employment, training and promotion is based solely on the objective assessment of ability and other relevant job-related criteria. In the case of training and career development access will also be based on assessed need.

In addition to this:

- We respect the dignity of individuals and their beliefs
- We do not tolerate any harassment or bullying (whether physical or mental) in the workplace, or at functions connected with the workplace.

By valuing diversity and being an inclusive employer we understand that we will:

- attract the best people with the right skills and experience
- develop and use the talents of our workforce effectively
- improve motivation and performance
- support each other to balance work and home responsibilities
- attract customers from across the community and enhance the trust and loyalty demonstrated by our brand.

Responsibilities

As a Filtronic colleague, you will be expected to be responsible and treat others with dignity. Any individual who breaches this policy may be subjected to disciplinary action under the Filtronic Conduct Policy and, in serious cases; this may result in their dismissal. Individual colleagues who have been involved in bullying or harassment may also be personally guilty of unlawful harassment and, in some cases, at risk of criminal prosecution.

Everyone has a strict responsibility to:

- respect and act in accordance with this policy
- treat all colleagues fairly and without discrimination
- ensure that their own behaviour does not cause offence or distress
- report any incident or behaviour which contravenes this policy and not indirectly support unfair treatment by ignoring what is happening around them.

In addition, those who manage people are responsible for:

- ensuring that the policy is fairly and consistently applied in all areas under their control
- eliminating and addressing any unfair practices of which they are aware, whether or not a complaint has been made
- promoting an environment in which people feel comfortable in reporting incidents which are causing them concern.

Procedure

What should I do if I believe I have been discriminated against or treated unfairly?

If you believe that you have been subjected to discrimination, you should contact your immediate manager in the first instance. If the matter is not resolved to your satisfaction, then please contact your HR Department or use the Filtronic grievance procedure.

Approved by the Board of Filtronic plc
May 2023

Filtronic plc

Conflict Minerals Policy

Policy Statement

In support of the efforts outlined in the global Conflict-Free Sourcing Initiative (CFSI) and Filtronic's commitment to corporate social responsibility and respecting human rights in our own operations and in our global supply chain, it is our goal to use tantalum, tin, tungsten and gold in our products that do not directly or indirectly finance or benefit armed groups in the DRC or adjoining countries while continuing to support responsible mineral sourcing in the region.

"Conflict minerals originating from the Democratic Republic of the Congo (DRC) are sometimes mined and sold, "under the control of armed groups", to "finance conflict characterised by extreme levels of violence" (ref. US Dodd-Frank Act Section 1502). Some of these minerals can make their way into the supply chains of the products used around the world, including those in the electronics industry.

Since a limited number of Filtronic's suppliers acquire and use conflict minerals from multiple sources worldwide and Filtronic may as a result be many levels away from the beginning of the supply chain for some of the components used in the products it manufactures or contracts to manufacture, we expect our suppliers to have in place policies and due diligence measures that will enable us to reasonably assure that products and components supplied to us containing conflict minerals are DRC conflict free.

In support of this policy, Filtronic will:

- Exercise due diligence with relevant suppliers consistent with the **OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas** and encourage our suppliers to do likewise with their suppliers.
- Provide, and expect our suppliers to cooperate in providing, due diligence information to confirm the tantalum, tin, tungsten and gold in our supply-chain are "conflict free".
- Collaborate with our suppliers and others on industry-wide solutions to enable products that are DRC conflict free.
- Commit to transparency in the implementation of this policy by making available reports on our progress to relevant stakeholders and the public (via website – request for information).

Filtronic is committed to:

- Help our suppliers understand the due diligence steps they can take to investigate the source of any Conflict Minerals in the products they sell to Filtronic.
- Not continue to source from a supplier any product that contains Conflict Minerals if Filtronic determines the product is not DRC Conflict Free and the supplier fails to implement reasonable steps to transition to DRC Conflict Free sources.

Filtronic expects their suppliers to:

- Comply with the Electronic Industry Citizenship Coalition (EICC) Code of Conduct and conduct their business in alignment with Filtronic's supply chain responsibility expectations.
- Source Conflict Minerals only from sources that are DRC Conflict Free.

- Develop Conflict Minerals policies, due diligence frameworks, and management systems that are designed to prevent Conflict Minerals that are not DRC Conflict Free from being included in the products sold to Filtronic. This includes:
  - implementing and communicating to their personnel and suppliers, policies that are consistent with this policy;
  - putting in place procedures for the traceability of Conflict Minerals, working with their direct and indirect suppliers as applicable;
  - using reasonable efforts to source Conflict Minerals from smelters and refiners validated as being DRC Conflict Free;
  - advising Filtronic of any determination the supplier either has concluded or has a reasonable basis to believe that products it currently sells or has sold to Filtronic are not DRC Conflict Free;
  - maintaining reviewable business records supporting the source of Conflict Minerals; and
  - periodically, at Filtronic's request, providing information concerning the origin of Conflict Minerals included in products sold to Filtronic, which Filtronic shall be entitled to use or disclose in satisfying any legal or regulatory requirements or in any customer or marketing communications, notwithstanding the terms of any confidentiality agreements that do not specifically reference this paragraph.

Conflict Minerals Reporting:
Filtronic will utilise the Conflict Minerals Reporting Template (CMRT – latest version) to report conflict minerals data associated with the products and processes related to Filtronic and its supply chains. This template will be a live document and updated whenever new information is obtained from the supply chain as a result of changes to current products and/or materials or any new product introduction utilising previously unreported materials.

Where required, Filtronic will comply with specific customer reporting methods and frequency.

Approved by the Board of Filtronic plc
May 2023

Filtronic plc

Modern Slavery Policy

Policy Statement

Modern slavery is a crime and a violation of fundamental human rights. It takes various forms, such as slavery, servitude, forced and compulsory labour and human trafficking, all of which have in common the deprivation of a person's liberty by another in order to exploit them for personal or commercial gain. Filtronic plc ("the Company") together with its subsidiary companies (herein "Filtronic" and "we") have a zero-tolerance approach to modern slavery and we are committed to acting ethically and with integrity in all our business dealings and relationships and to implementing and enforcing effective systems and controls to ensure modern slavery is not taking place anywhere in our own business or in any of our supply chains.

We are also committed to ensuring there is transparency in our own business and in our approach to tackling modern slavery throughout our supply chains, consistent with our disclosure obligations under the Modern Slavery Act 2015. We expect the same high standards from all of our contractors, suppliers and other business partners, and as part of our contracting processes, we include specific prohibitions against the use of forced, compulsory or trafficked labour, or anyone held in slavery or servitude, whether adults or children, and we expect that our suppliers will hold their own suppliers to the same high standards.

This policy applies to all persons working for us or on our behalf in any capacity, including employees at all levels, directors, officers, agency workers, seconded workers, volunteers, interns, agents, contractors, external consultants, third-party representatives and business partners.

This policy does not form part of any employee's contract of employment and we may amend it at any time.

Responsibility for the Policy

The board of directors has overall responsibility for ensuring this policy complies with our legal and ethical obligations, and that all those under our control comply with it.

The relevant Business Unit Manager has primary and day-to-day responsibility for implementing this policy, monitoring its use and effectiveness, dealing with any queries about it, and auditing internal control systems and procedures to ensure they are effective in countering modern slavery.

Management at all levels are responsible for ensuring those reporting to them understand and comply with this policy and are given adequate and regular training on it and the issue of modern slavery in supply chains.

You are invited to comment on this policy and suggest ways in which it might be improved. Comments, suggestions and queries are encouraged and should be addressed to the Company Secretary or any plc director.

Compliance with the Policy

You must ensure that you read, understand and comply with this policy.

The prevention, detection and reporting of modern slavery in any part of our business or supply chains is the responsibility of all those working for us or under our control. You are required to avoid any activity that might lead to, or suggest, a breach of this policy.

You must notify your manager or the contacts in the whistle-blower policy as soon as possible if you believe or suspect that a breach of this policy has occurred or may occur in the future.

You are encouraged to raise concerns about any issue or suspicion of modern slavery in any part of our business or supply chain at the earliest possible stage.

If you believe or suspect a breach of this policy has occurred or that it may occur you must notify your manager or any plc Director or Company Secretary OR report it in accordance with our Whistleblowing Policy as soon as possible.

If you are unsure about whether a particular act, the treatment of workers more generally, or their working conditions within any tier of our supply chain constitutes any of the various forms of modern slavery, raise it with your manager or any plc Director or Company Secretary.

We aim to encourage openness and will support anyone who raises genuine concerns in good faith under this policy, even if they turn out to be mistaken. We are committed to ensuring no one suffers any detrimental treatment as a result of reporting in good faith their suspicion that modern slavery of whatever form is or may be taking place in any part of our own business or in any of our supply chains. Detrimental treatment includes dismissal, disciplinary action, threats or other unfavourable treatment connected with raising a concern. If you believe that you have suffered any such treatment, you should inform the compliance manager immediately. If the matter is not remedied, and you are an employee, you should raise it formally using our Grievance Procedure, which can be found in the Employee Handbook or from the HR Manager.

Communication and Awareness of this Policy

Training on this policy, and on the risk our business faces from modern slavery in its supply chains, forms part of the induction process for all individuals who work for us, and regular training will be provided as necessary.

Our zero-tolerance approach to modern slavery must be communicated to all suppliers, contractors and business partners at the outset of our business relationship with them and reinforced as appropriate thereafter.

Breaches of this Policy

Any employee who breaches this policy will face disciplinary action, which could result in dismissal for misconduct or gross misconduct.

We may terminate our relationship with other individuals and organisations working on our behalf if they breach this policy.

Approved by the Board of Filtronic plc
May 2023

Filtronic plc

Employment of Connected Persons Policy

Employment decisions related to selecting, engaging, promoting, remunerating and terminating employees should be based solely on an individual's qualifications, ability and performance. When relatives work for the same employer, a potential for favouritism (nepotism) exists making it important for the relevant company ("the Company") to develop, publish and adhere to policies regarding the employment of family members. (This policy applies to all companies within the Filtronic group of companies.)

Nepotism may include but is not limited to:

- Helping someone get a job or promotion because he or she is a relative;
- Giving preferred work assignments to a relative;
- Overlooking performance issues;
- Making other decisions that impact favourably on a relative based solely on kinship.

The Filtronic policy provides that members of an employee's immediate family will be considered for employment on the basis of their qualifications/skills.

Immediate family may not be engaged, however, if employment would:

(i) Create a supervisor/subordinate relationship (directly or indirectly) with a family member;

(ii) Have the potential for creating an adverse impact on work performance; or

(iii) Create either an actual conflict of interest or the appearance of a conflict of interest.

This policy must also be considered when assigning, transferring, or promoting an employee. For the purpose of this policy, immediate family includes: spouse, civil partner, parent, child, sibling, in-law, aunt, uncle, niece, grandparent, grandchild, members of the same household. This policy also applies to romantic relationships.

Employees who become immediate family members or establish a romantic relationship may continue employment as long as it does not involve any of (i), (ii) or (iii) above.

If one of the conditions outlined should occur or be likely to occur, reasonable attempts will be made to find a suitable position within the Group to which one of the employees will transfer. If employees become immediate family members or establish a romantic relationship, the Company (involving the Filtronic HR function) will make reasonable efforts to reassign job duties so as to minimise problems of supervision, safety, security or morale.

If it is not possible to transfer an employee to an alternative role or to find alternative duties (if, for example, one of the individuals is in a significantly senior e.g. Board or executive role whether at company or group level) the Company may have to consider terminating the employment of one of the employees. The Company would consult with both employees before any such decision is taken.

Approved by the Board of Filtronic plc
May 2023

Filtronic plc

Health and Safety Policy

The Board of Filtronic plc ("the Company") aims to achieve the highest standards in the management of health and safety at all our sites. These standards apply to everybody who accesses our sites.

The Board considers that the operation of an effective health and safety management system is fundamental in establishing and supporting an active health and safety culture and ensuring continual improvement. The Board's objective is to ensure all Filtronic sites take appropriate steps to protect the Health and Safety of employees, contractors, agents, customers, visitors and the general public.

To this end, the Board requires the Chief Executive Officer ("CEO") to maintain and publish a site-specific Health and Safety Policy which ensures an integrated approach to Health & Safety is applied to the site in support of sending everybody "Home Safe Every Day". The CEO must ensure that each site:

- Actively involves employees, including consultation on matters affecting their health and safety.
- Provides a framework for setting Health and Safety objectives.
- Identifies health and safety risks which will be eliminated or reduced.
- Provides appropriate safe and healthy working conditions for the prevention of work-related injury and ill health.
- Employ safe practices in the installation, operation and maintenance of equipment and facilities.
- Employ safe practices in the transport, handling, storage, use and disposal of potentially dangerous articles and substances.
- Regularly review and comply with all legal requirements, and applicable Filtronic standards.
- Commit to monitoring and continually improving its Health and Safety performance, including its leadership and management systems.
- Consult with our workforce and communicates to all interested parties, ensuring that they are aware of the wider Health and Safety objectives and performance, as well as their individual health and safety obligations.
- All visitors and contractors working on Company premises must be inducted and made aware of workplace risks. Visitors on site must be adequately supervised.

Filtronic will maintain a positive and progressive approach to Health and Safety issues, and our CEO will ensure that each site has the capability to discharge their duties with respect to this policy statement. This policy will be reviewed regularly and updated as necessary. This policy is available to interested parties upon request or via our website.

Approved by the Board of Filtronic plc
May 2023

Filtronic plc

Quality Policy

Filtronic plc ("the Company") together with its subsidiary companies and business units (herein "Filtronic") are strategically committed to being a world leader in the design and manufacture of RF & Microwave products and services offering complete solutions to meet or exceed customer and applicable statutory and regulatory requirements at competitive prices.

Filtronic plc has established a Quality Management System that:

- Is appropriate for the purpose and context of our organisation and supports our strategic direction
- Provides a framework for setting quality objectives that are relevant to the conformity of our products and enhance customer satisfaction
- Is committed to satisfying applicable requirements
- Maintains effectiveness through a process of monitoring and continual improvement versus measurable objectives at all levels of the organisation
- Is committed to continually improving our Quality Management Systems

Approved by the Board of Filtronic plc
May 2023

Filtronic plc

Environmental Policy

Filtronic plc, its subsidiaries and their business units, are strategically committed to protecting the environment:

- Through prevention of pollution and minimising our impact on natural resources;
- By operating in compliance with all relevant statutory and regulatory obligations through the adoption of environmental best practices throughout our activities;
- By continually improving our environmental management system to enhance our environmental performance.

The effectiveness of our Environmental Management System is maintained through a process of monitoring and continual improvement against measurable objectives at all levels of the organisation.

As part of our activities and decision-making process, we will:

- Integrate the consideration of environmental concerns and impacts into the design and manufacture of our products;
- Promote environmental awareness among our employees, customers and supply chain;
- Minimise waste through re-use and recycling and promote efficient use of materials and resources; Strive to prevent pollution and to continually improve our environmental performance;
- Minimise the social impact and damage from our activities by periodically reviewing our environmental policy based on our current and planned future activities.

Approved by the Board of Filtronic plc
May 2023

Filtronic plc

Intellectual Property Rights ("IPR") Policy

Policy Statement

Filtronic recognises intellectual property as a valuable asset. Therefore, we will respect the Intellectual Property Rights ("IPR") of others and protect Filtronic IPR through our own processes and those of our supply chain with the aim of enhancing shareholder value.

Implementation

We will seek to protect existing business activities, to increase market share and to develop new profitable business activities worldwide by:

- Always seeking to retain control of the IPR of its products.
- Promoting IPR awareness.
- Actively seeking patent protection on inventions and designs appropriate to its business strategies.
- Maintaining international IPR portfolios.
- Reviewing research and development, to determine whether there is a risk of infringing any known third party IPR.
- Defending and enforcing its IPR against infringement by third parties.
- Resisting any challenge to the ownership of its IPR.
- Respecting the IPR of others.
- Investigating appropriate opportunities for licensing its IPR to generate revenue.
- Complying with the rules of standardisation bodies on IPR.

The authority to approve the assignment or licensing of a substantial interest in the IPR of any business division is reserved for the **Filtronic plc Board of Directors** *(for example, the grant of an IPR licence which would prejudice the ability of the division in carrying out its business would require approval whereas the grant of non-exclusive licences to customers in the normal course of business would not.)*

In delivering these objectives we shall:

- Maintain a clearly defined IPR strategy within the framework of this Policy.
- Appoint a person for promoting IPR awareness and co-coordinating IPR activities.
- Maintain a database of the IPR it owns.
- Monitor third party IPR and competitors' products to identify possible infringements.
- Establish an adequate mechanism for securing evidence of date and origin of invention or design.
- Ensure that applications are filed before an invention or design is disclosed or, if for compelling commercial reasons that is not possible, ensuring that disclosure is strictly 'In Confidence' and that an appropriate Confidentiality Agreement/Non-disclosure agreement (NDA) is in place.

Any invention that has been disclosed to the public may not be patented. Information is deemed to have been disclosed to the public if anyone is free to disclose it without breaking obligations of confidentiality.

You should not, therefore, send potentially patentable information in unencrypted emails, or across public domains, which may be accessed by unauthorised individuals. Patents will not be granted for inventions that are deemed obvious to a person skilled in the area that has access to all the information available on the subject. Equally, employees and other stakeholders must not make careless publications that might lead someone to deduce the Company's ideas.

Approved by the Board of Filtronic plc
May 2023

Filtronic plc

Counterfeit/Grey Goods Policy

Filtronic undertakes to use reasonable commercial endeavours (which are appropriate in all the relevant circumstances) to ensure that neither it nor its suppliers use or supply counterfeit goods or use counterfeit goods in its supply chain.

According to the OECD, counterfeit products encompass all products made to closely imitate the appearance of the product of another so as to mislead consumers. Those can include the unauthorised production and distribution of products that are protected by intellectual property rights, such as copyright, trademarks and trade names.

Approved by the Board of Filtronic plc
May 2023

Filtronic plc

Technology Leadership Recognition Policy

Introduction & Purpose

Filtronic operates in highly technically competitive markets and can only succeed through product, technology and service excellence. Establishing and protecting a high market profile for product excellence and technical leadership are thus essential prerequisites for us achieving a competitive edge.

The company therefore places a high value on developing and owning our own protectable Intellectual Property Rights and Copyrights to provide us with a "Defensive Moat"

In order to recognize this value and encourage innovative thinking and professional personal development amongst our engineering and technical community the company has established a **"Technical Leadership Recognition Policy"**

Policy Statement

Filtronic plc places great importance on the value of internally generated Intellectual Property Rights ("IPR") and will actively seek patent protection on inventions and designs appropriate to its business strategies. Additionally, Filtronic values the contribution to enhancing long term shareholder value through the promotion of the Company in peer reviewed technical publications and conferences and symposia. Recognising that it is our employees who are key to success in this area, Filtronic has implemented a Patent and Technical Publication Incentive to reward staff for achieving such recognition outcomes.

Implementation

In keeping with the policy objectives, the following rewards shall be payable to qualifying employees for completion of the following activities.

Achievement	Reward per Achievement (iv)
Patent Application (i)	£1,000
Patent Grant (ii)	£2,000
Delivery of a Technical Symposium Presentation (iii)	£1,000
Peer Reviewed Proceedings or Conference Papers (IEE, MTT etc.) (iii)	£1,000

In the case of Patent Applications, authorisation to proceed with the generation of a patent application for an idea, invention, novel design or product process will be authorised after approval from the Strategic Engineering Team (SET). This also applies to all technical articles, papers and presentations at conferences and symposia incorporating the Company's IPR. Initiation of a request to undertake one of the qualifying activities can be made to and must receive the approval of the Chair of the Strategic Engineering Team (SET).

Upon receipt of written authorisation to proceed with an application or technical publication, the relevant managers will be informed to ensure that suitable time is made available to employees

during their day activities.

Filtronic intends that employees will see this as not only recognising the importance of product and technology innovation to the future prosperity of the company but also recognising the role that our innovators play in delivering this strategically important objective.

Notes to Table

Note (i) *– Reward payable on filing of the first Patent Application for the invention (excludes subsequent equivalent filings in other territories/jurisdictions).*

Note (ii) *– Reward payable only when a patent is first granted for the relevant invention in any territory/jurisdiction (excludes any subsequent grants for the invention in other territories/jurisdictions). Reward is payable as soon as practicable following official notification of filing/grant as applicable.*

Note (iii) *Reward payable following delivery of the Presentation, or publication of the Paper*

Note (iv) *– The Reward is essentially payable per event originator / architect. Where more than one person is involved in creating / delivering the event, the SET will consider whether the scale and significance of the achievement warrants multiple Rewards.*

This scheme will be administered in good faith but is discretionary and does not form part of any employee's terms and conditions of employment. The policy may change or be withdrawn or suspended at the discretion of the Board of Directors of the Company.

Approved by the Board of Filtronic plc
May 2023

Filtronic plc

IT Policy

Policy Statement

Filtronic aims to ensure that it has adequate IT systems in place to conduct the business of the Company and that these systems are used properly and effectively to promote and protect the Company's interests.

Departmental managers within the Group must ensure their employees are briefed and trained on the content of this policy and monitor for compliance.

IT Policy Implementation

This policy applies to all users of the Filtronic IT and telephone systems (including, without limit, all directors, employees and third-parties) who use email, bulletin boards, the intranet and the internet through devices based at the Company's premises or through any device situated at other locations (including personal equipment) via the Company's network or any network provided at your workplace either by the Company or a third party at the Company's request or using the Company's telephone lines.

N.B. All communications and stored information sent, received, created or contained within the Company's systems are the property of the Company and accordingly should not be considered private or personal.

Email Policy

Employees must use the company provided Filtronic email account for company business and not a private or public email account such Hotmail or Yahoo. They must act responsibly and appropriately when using the Company's computers and when sending email**,** whether internally within the Company or externally using the internet. All communications sent via the Company's system may be legally regarded as bearing the Company letterhead and, should therefore, be treated as official company communication.

Employees are strictly prohibited from sending any emails that are:

- threatening or aggressive
- abusive, anti-social or sexually biased
- obscene or offensive
- in breach of Company policy or government regulations/legislation
- from someone else's account, except under proper "delegated" arrangements, which retain individual accountability.

Employees must not send or receive any unauthorised executable programs through the email system and must exercise caution when receiving any documents or attachments which are received unsolicited.

Some tips to recognise malicious emails are listed below:

- **Use of urgent or threatening language**
  By pressuring you to reply quickly or issuing ultimatums, criminals hope to instil panic and fear to trick you into providing confidential information. Be wary of emails with phrases such as 'urgent action required' or 'your account will be terminated. If you have good reason to believe it is a scam, delete the message immediately.

  Promises of attractive rewards
  False offers of amazing deals or unbelievable prizes are commonly used by cybercriminals to encourage you to act immediately. If all you need to do is to click on a pop-up or complete an email survey to win a prize, it is safe to presume that it is a scam.

  Requests for confidential information
  Most organisations will never ask for your personal information login credentials and credit card details to be sent over the Internet. If the sender claims to be from your bank and requests your bank account number, it should raise a red flag immediately. When in doubt, contact the company directly to clarify, but be sure not to use the contact information provided in the email.

  Unexpected emails
  Cybercriminals often test their luck by sending mass emails to large groups of people, in hopes that someone responds. If you receive an email about an invoice for an item you did not purchase, do not click on the links and attachments and delete the email immediately.

- **Suspicious attachments**
  Cybercriminals include attachments in their emails as a method to infect a user's device with malware and steal their data. It may be instinctive to open attachments we receive but it is important to exercise caution. Look out for suspicious attachment names and file types. If the attachment is for something you have no recollection of or uses an uncommon file type such as .exe, delete it.

If you are unsure whether an email is legitimate, please ask IT who will review the email and attachment in a safe environment where malcontent can't enter our systems.

Internet Policy

Employees will need to be familiar with the type of information that the Company deems to be sensitive or secret and must ensure that this is not made available to the public. Examples of this can be found in the Procedures and Authorities Manual (PAM) within the external communications section and within the Data Protection Policy in the Group Policies. If anybody is uncertain whether information is sensitive or secret, please ask an Executive Director or the Security Controller.

Employees must not deliberately visit, view or download any of the following material and are strictly prohibited from sending any material, whether downloaded from the internet or otherwise which contains or refers to material such as:

- Sex or pornography whether illegal material or material comparable to that available on the top shelf in a newsagent
- Terrorism, Cults
- Controlled Drugs
- Extreme material which may be likely to cause offence to another person
- Hate sites (racial or other)
- Gambling
- Criminal skills (including software hacking)
- Advertisement or the conduct of any personal trade, service or profession.

Should any employees mistakenly locate an internet site containing any prohibited material (as above) they should notify the IT department so that steps can be taken to avoid other people making the same mistake.

Employees must not post any material on to the internet, which incites or encourages or enables others to gain unauthorised access to the Company's computer system. It is vital that all staff take all necessary steps to safeguard the Company's computer system from viruses.

Unauthorised use of email and/or the Internet may expose both the Company and/or yourself to court proceedings attracting both criminal and civil liability. Employees will be held responsible for any claims brought against the Company for any legal action to which the Company is, or might be, exposed as a result of unauthorised use of email and/or the Internet.

Employees must not subscribe to any bulletin boards, newsgroups or any other internet services without the approval of the IT Manager. It is a criminal offence to publish or distribute obscene material or to display indecent material in public. The internet or any computer 'message boards' qualify as a public place.

Password Policy

All system passwords and security codes must be set in accordance with the IT password complexity requirements as detailed in the Filtronic IT procedure (GP-0004). The use of someone else's identity and password to access computers, systems, the internet or send email is strictly forbidden and will result in disciplinary action.

Software

All software must be approved by the IT department before being downloaded and must be correctly licenced for its intended use. Employees must not breach the terms of any licence by unauthorised copying, sharing or distributing software.

All software licences that have been found to have expired or are otherwise invalid for the activities being carried out will be withdrawn and the application may not be used until a valid licence has been obtained and allocated.

Employees must notify their departmental manager or the IT department of any misuse of software or associated documentation as soon as they become aware of it.

The use of software packages, including cloud computing services, other than those licensed by the Company requires the approval of the IT department and the purchase of appropriate licences from the owner or reseller. Installation of software and modification of PCs must be performed by a member of the IT department, unless otherwise authorised by IT, your departmental manager, or a competent staff member. Users are responsible for any third-party software that is installed, and they are responsible for ensuring it does not breach any of the Company's policies and procedures for content or IP/licensing and the Company has the right to prohibit the use of any specific third-party software as it deems appropriate.

Virus checking of new software will be carried out by the IT systems or may be implemented on a case-by-case basis as appropriate.

Bring Your Own Device ("BYOD")

Filtronic allows the use of personal devices, commonly referred to as BYOD, to access corporate data and information systems including cloud computing services such as email, the ERP, CRM and HR systems. To facilitate this policy the personal device must be approved and registered with the IT Department and have the mobile device management ("MDM") software and policies installed.

Filtronic, as the Data Controller, remains in control of the data regardless of the ownership of the device. As a user you are required to keep Filtronic information and data secure. This applies to information held on your own device, as well as Filtronic systems.

You are required to assist and support Filtronic in carrying out its legal and operational obligations, including co-operating with IT management or the Data Protection Officer ("DPO") should it be necessary to access or inspect Filtronic data stored on your personal device. Filtronic reserves the right to refuse, prevent or withdraw access to users and/or particular devices or software where it considers that they are unacceptable in terms of security, or other risks, to its staff, business, reputation, systems or infrastructure.

From time to time, Filtronic may require that you install, or update Filtronic approved device management software on your own device. Please note that in the event of a security incident, personal data may be impacted. Therefore, the Company recommends you backup your data regularly to avoid losing personal information.

It is your responsibility to familiarise yourself with the device sufficiently to keep data secure which means:

- Preventing theft and loss of data (using Biometric/PIN/Password/Passphrase lock)
- Preventing theft and loss of your device.
- Keeping information confidential, where appropriate.
- Maintaining the integrity of data and information.

You Must:

- Allow the IT Department to deploy MDM software to your device.
- Use the device's security features, such as a biometric, PIN, password/passphrase and automatic lock to help protect the device when not in use.
- Keep the device software up to date, for example using Windows Update or Software Update services.
- Activate and use encryption services and anti-virus protection if your device features such services.
- If required, install and configure tracking and/or wiping services, such as Apple's 'Find My iPhone app', Android's 'Where's My Droid' or Windows' 'Find My Phone', where the device has this feature. This is to enable you to locate or wipe your device should it go missing.
- Remove any Filtronic information stored on your device once you have finished with it including deleting copies of attachments to emails, such as documents, spreadsheets, and data sets.
- Remove all Filtronic information from your device and return it to the manufacturers' settings before you sell, exchange or dispose of your device.

You Must Never:

- Store data that is classified as 'commercial in confidence' or above from Filtronic systems on your own device.
- Personal data as defined by the GDPR may not be stored on your personal device or personal cloud services. You should use Filtronic provided storage.

Note: If you are in any doubt as to whether particular data can be stored on your device, you are required to consult with your manager or seek advice from the IT department.

The loss or theft of a device:

- In the event that your device is lost or stolen, or its security is compromised, you MUST promptly report this to the IT Manager, so they may assist you to change the password to all relevant Filtronic systems (it is also recommended that you do this for any other services that have accessed via that device, e.g., social networking sites, online banks, online shops).
- If it is necessary to do so, you must also cooperate with the IT department in wiping the device remotely, even if such a wipe results in the loss of your own data, such as photos, contacts and music.
- You MUST NOT attempt to circumvent the device manufacturer's security mechanisms in any way, for example to 'jailbreak' the device.
- Further advice on securing personal devices (including advice on the risks of downloading untrusted Apps) is available from the IT Department.

Monitoring of BYOD equipment

- Filtronic will not monitor the content of your personal devices. However, Filtronic reserves the right to monitor and log data traffic transferred between your device and Filtronic systems, both over internal networks and via the internet.
- Under some circumstances, for example, where you legitimately need to access or store certain types of information on your own device, you must seek authority from the IT Department. Filtronic may then need to monitor the device at a level which may impact your privacy by logging all activity on the machine. This is to ensure the privacy, integrity, and confidentiality of that data.
- You are required to conduct work-related activities in line with Filtronic's Information Security policies. This requirement applies equally to use of your personal devices for work purposes.
- Filtronic reserves the right to audit the device if there are concerns over usage or security. This may result in permission to use the device with Filtronic systems being revoked.

Responsibilities Regarding Device Support

- Where possible, Filtronic will support all devices, but you have a responsibility to learn how to use and manage your own device effectively within the context of this policy.
- Filtronic takes no responsibility for supporting, maintaining, repairing, insuring or otherwise funding employee-owned devices, or for any loss or damage resulting from support and advice provided.

Remote Working Policy

Filtronic employees are allowed to access information and work systems from multiple locations using a multitude of devices while also being able to do so remotely from home. Filtronic employees have a duty to protect company information by ensuring compliance to remote working protocols; including the use of encryption, access control, company-provided VPN, password protection, multi-factor authentication, and any other protocols that may be deemed necessary.

Filtronic employees are required to protect any hardware issued by the company and all losses or damages must be immediately reported to the IT department.

Mobile and Storage Device Policy

Filtronic employees use mobile and storage devices such as laptops, notebooks, smart devices (tablets, phones) capable of connecting (whether by a wired or wireless connection) to a computing device and storing information, external portable hard disk drives, USB memory sticks, and similar storage devices. All mobile and storage devices must be approved by the IT department before they are connected to the corporate network or accessing company information. Filtronic employees must ensure that access to the company network and information is for legitimate work purposes only.

Employees have full responsibility for the security of the mobile devices issued to them, taking necessary precautions to avoid loss, theft or damage. In the event of loss or damage, users must report this immediately to the IT department. If a mobile device has been stolen, the police should also be notified, and a crime reference number obtained.

All employees issued with mobile devices must:

- Take all reasonable care to prevent the theft or loss of this device. Any mobile computing device, including smart phones, is an attractive item for thieves and must not be left unattended in a public place or in vehicles on view, unattended or overnight. When transporting the device, ensure that it is safely stowed out of sight.
- Be extra vigilant if using any mobile computing device during journeys on public transport to avoid the risk of theft of the device or unauthorised disclosure of the company's information by a third party "overlooking".
- Don't leave the device unattended for any reason unless the session is "locked" and it is in a safe working place, not left in an unattended publicly accessible room for example. If it is anticipated leaving the device unattended it must be locked, logged out, or shut down to secure the device. If it is possible employees should take the device with them. Where circumstances necessitate extra precautions, laptop tethering locks should be considered.
- Ensure that other 'non' authorised users are not given access to the device or the data it contains.
- Carry the device in a suitable protective case or luggage

Passwords are an integral part of the Access Control mechanisms. All devices used for remote working must comply with Filtronic's Password Policy.

Staff must ensure they understand and comply with Filtronic's BYOD Policy when making use of user-provided devices.

Staff using mobile devices must only use encrypted devices authorised by the company.

The Filtronic Security Controller or the IT Security Officer must be consulted before using mobile devices to transport sensitive or confidential information. Information should not be stored permanently on mobile devices. Always transfer documents back to their normal storage area as soon as possible. Failure to do so may result in problems with version control or loss of information if the mobile device is lost or corrupted.

Employees must ensure that any suspected or actual breaches of security are reported to the IT department immediately by emailing the IT helpdesk and then immediately having a conversation with the IT Manager or Security Controller.

External visitors (suppliers, contractors, clients, company representatives, etc.) must use the public Wi-Fi, and not the Filtronic private Wi-Fi, and may only connect mobile devices, including USB sticks and laptops, to Filtronic assets where authorisation has been granted by the IT Manager or the Security Controller.

Authorisation for the use of mobile devices by external visitors will only be given following consultation with the IT department, they will ensure that the device is virus- scanned before any documents are opened.

Any device owner leaving the company or no longer requiring use of a company procured device must return the device to their line manager who will then give the equipment to the IT department. Line managers will be responsible for ensuring that any member of their staff having temporary ownership of a device has returned it to them or the IT department before they leave the company. All media containing the company's information must be returned for retention or appropriate destruction.

If in doubt, employees should consult with the IT department before connecting the device.

Removable Storage Media Policy

Removable storage media includes USB sticks, USB portable hard disk drives and DVDs/CDs.

- Only company-provided removable storage media shall be used to copy business data.
- Users must seek authorisation and approval from the IT department to use removable storage media. An IT ticket to IThelp@filtronic.com explaining the purpose and location of use must be submitted, as part of the authorisation and approval process.
- Approved removable media will be encrypted where possible and tracked in the Computer Systems Inventory (GF-0006).
- Information shall not be stored permanently on removable storage media.
- Removable Storage Media must be scanned for viruses before being used.
- Removable media should only be used to transfer information. Permanent storage of information on memory sticks and portable hard disk drives should be avoided. Storage of information on DVD/CD should also be avoided or the DVD/CD should be registered and stored in a central location.
- Where indicated by the risk assessment, the system will be prevented from using removable media.

IT Change Management Policy

The Company has robust procedures in place to manage the IT environment. This is an important framework as to how the IT infrastructure is controlled and forms the defence against vulnerabilities in our system. Changes to IT systems within Filtronic are subject to change control procedures.

Employees wanting to add or amend applications, systems and services, including cloud-based systems, must ensure the changes are in compliance with the IT procedures in GP-0004 and approved by the IT department.

Any security breaches must be reported in line with the IT Security Incident Response ("ISIRT") procedure found in GP-0004.

Information Security Policy

Employees must not disclose company information to third parties unless authorised to do so or a Non-Disclosure Agreement is in place and has been signed by an Executive Director.

Filtronic will manage information security using a combination of physical and software controls including asset management, restricted access, encryption, password protection, multi-factor authentication, unique user accounts, privilege controls, monitoring and auditing, firewalls, endpoint protection, and retention protocols.

Only authorised personnel who have a valid and approved business need will be given access to areas containing information systems or stored data.

An audit trail of system access and data use by staff will be maintained wherever practical and reviewed on a regular basis.

Access to the organisation's information systems by external parties will only be allowed where a contract that requires compliance with this Information Security Policy is in place. Such a contract will require that the staff or sub-contractors of the external organisation comply with all appropriate security policies and procedures.

Contractors and suppliers, including Cloud service providers, that have access to Filtronic information/data are required to have policies and procedures in place for information security that are the same or more comprehensive than Filtronic.

Employees should be aware that information and emails sent across the internet may be read by persons unknown to the sender. Even if some information has been deleted it may not necessarily be deleted from the internet system which provides backup saving mechanisms. Any message or information requiring security or elevated confidentiality should be distributed by an appropriate channel – if you are unsure, you should see the IT Manager or Security Controller.

Sensitive documents must not be saved to public file shares and should be physically protected when leaving them unattended. All sensitive information must be disposed of in a secure manner as detailed in the Filtronic Security Instructions (CSP-0062) – if you are unsure, you should see the Security Controller.

Any contract entered into by the Company that contracts with a third party for goods and services (e.g. suppliers, contractors, partners, customers) should contain clear and comprehensive security conditions in respect of the access by the third party to the system and protection of the Company's information and IT services. The department responsible for the contract must regularly monitor compliance with such security conditions and liaise with the IT department where necessary.

Employees are required to lock their screens when away from their computer to avoid inadvertent security breaches. Equally, they should be aware of their surroundings and ensure that confidential or secure data can't be seen by somebody in the same proximity not authorised to view the

information. All breaches of information security must be reported immediately to the IT Manager or the Security Controller.

Equally, any similar security and licensing requirements associated with the use of third-party information by the Company must be followed.

IT Breach Policy

All information security breaches and incidents must be reported, without delay, to the Security Controller or a member of the IT Security Incident Response Team ("ISIRT") as per the Filtronic IT Procedure (GP-0004).

When the breach may involve a member of the ISIRT, it must be reported to the Chief Executive Officer (CEO).

Monitoring

In accordance with the Company's Data Protection Policy, the Company reserves the right, at any time and without notice, to monitor, keep a record of, access, listen to or read any communication made or received by you on its computers or telephone system for the following purposes:

- to establish the existence of business-related facts;
- to ascertain compliance with regulatory or self-regulatory practices and procedures;
- for quality control and staff training purposes;
- to prevent or detect crime (including 'hacking');
- to intercept for operational purposes, such as protecting against viruses and making routine interceptions such as forwarding emails to correct destinations;
- to detect or investigate unauthorised use of the IT resources; or
- to check email and voice mail systems when you are on holiday, on sick leave or have left the business.

The Company reserves the right to log all internet activity and monitor time spent by employees accessing the internet for browsing. The Company may monitor sites visited, the content viewed, or information downloaded where necessary.

The Company also reserves the right to make and keep copies of telephone calls or emails and data documenting use of the telephone, email and/or the internet systems, for the purposes set out above. The Company may bypass any password you set.

Approved by the Board of Filtronic plc
May 2023

Filtronic plc

Data Protection Policy

Introduction

Purpose

Filtronic is committed to being transparent about how it collects and uses the personal data of its workforce, and to meeting its data protection obligations. This policy sets out Filtronic's commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of employees and workers, contractors, volunteers, interns, apprentices, job applicants and former employees, referred to as HR-related personal data. The policy applies to all Filtronic sites across the globe.

Definitions

"Personal data" is any information that relates to an individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sexual orientation and biometric data.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Data Protection Principles

Filtronic processes HR-related personal data in accordance with the following data protection principles:

- Filtronic processes personal data lawfully, fairly and in a transparent manner.
- Filtronic collects personal data only for specified, explicit and legitimate purposes.
- Filtronic processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- Filtronic keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- Filtronic keeps personal data only for the period necessary for processing.
- Filtronic adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

Filtronic tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons.

Where Filtronic processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with a policy on special categories of data and criminal records data.

Filtronic will update HR-related personal data promptly if an individual advises that his/her information has changed or is inaccurate.

Personal data gathered during the employment, worker, contractor or volunteer relationship, or apprenticeship or internship is held in the individual's personnel file in hard copy or electronic format, or both, and on HR and HR related finance systems. The periods for which Filtronic holds HR-related personal data are contained in its privacy notices to individuals.

Filtronic keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

Individual Rights

As a data subject, individuals have a number of rights in relation to their personal data.

Subject Access Requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, Filtronic will tell him/her:

- whether or not his/her data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long his/her personal data is stored (or how that period is decided);
- his/her rights to rectification or erasure of data, or to restrict or object to processing;
- his/her right to complain to the Information Commissioner if he/she thinks Filtronic has failed to comply with his/her data protection rights; and
- whether or not Filtronic carries out automated decision-making and the logic involved in any such decision-making.

Filtronic will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless, he/she agrees otherwise.

If the individual wants additional copies, Filtronic will charge a fee, which will be based on the administrative cost to Filtronic of providing the additional copies.

To make a subject access request, the individual should send the request to:

(i) by email: datasubjectaccessrequest@filtronic.com

or

(ii) by post: Head of HR, Filtronic, NETPark, Thomas Wright Way, Sedgefield, Co Durham TS21 3FD, UK with a copy to the Company Secretary

In some cases, Filtronic may need to ask for proof of identification before the request can be processed. Filtronic will inform the individual if it needs to verify his/her identity and the documents it requires.

Filtronic will normally respond to a request within a period of one month from the date it is received. In some cases, such as where Filtronic processes large amounts of the individual's data, it may respond within three months of the date the request is received. Filtronic will write to the individual within one month of receiving the original request to tell him/her if this is the case.

If a subject access request is manifestly unfounded or excessive, Filtronic is not obliged to comply with it. Alternatively, Filtronic can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which Filtronic has already responded. If an individual submits a request that is unfounded or excessive, Filtronic will notify him/her that this is the case and whether or not it will respond to it.

Other Rights

Individuals have a number of other rights in relation to their personal data. They can require Filtronic to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override Filtronic's legitimate grounds for processing data (where Filtronic relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override Filtronic's legitimate grounds for processing data.

To ask Filtronic to take any of these steps, the individual should send the request to: datasubjectaccessrequest@filtronic.com

Data Security

Filtronic takes the security of HR-related personal data seriously. Filtronic has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties. Where Filtronic engages third parties to process personal data on its behalf, such parties do so on the basis of (i) written instructions, (ii) are under a duty of confidentiality and (iii) are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Impact Assessments

Exceptionally, some of the processing that Filtronic carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, Filtronic will carry out a data protection impact assessment to determine the necessity and proportionality of processing.

This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

Data Breach

If Filtronic discovers that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, it will report it to the relevant/UK Information Commissioner, within 72 hours of discovery. Filtronic will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

International Data Transfers

HR-related personal data may be transferred to countries outside the EEA where it is necessary to comply with contractual obligation, including payroll and payment obligation owed to workers and very occasionally where a sale of the business might be contemplated to an entity with operations outside of the EEA. Data is transferred outside the EEA on the basis of declaration of adequacy of controls from directors or senior managers, binding corporate rules or other safeguards.

Individual Responsibilities

Individuals are responsible for helping Filtronic keep their personal data up to date. Individuals should let Filtronic know if data provided to Filtronic changes, for example if an individual moves house or changes his/her bank details.

Individuals may have access to the personal data of other individuals including those of our shareholders, customers' and suppliers' employees and workers' and clients in the course of their employment, contract, volunteer period, internship or apprenticeship. Where this is the case, Filtronic relies on individuals to help meet its data protection obligations to staff and to shareholders, customers and suppliers.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside Filtronic) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from Filtronic's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under Filtronic's disciplinary procedure. Significant or deliberate breaches of this policy, such

as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Training

Filtronic will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

Questions about this policy, or requests for further information, should be directed to Filtronic's HR department

Data Retention Policy & Schedule

Under UK GDPR and the DPA 2018, personal data processed by Filtronic must not be retained for longer than is necessary for its lawful purpose. Accordingly, it is Filtronic's policy is to retain personal data for the minimum period required by law and good business practice and to handle, store and dispose of personal data responsibly and securely. This policy applies to all Filtronic employees, directors, officers, contractors, consultants and advisers who have access to personal data. It is the responsibility of all of the above to familiarise themselves with this policy and ensure adequate compliance with it.

Data Retention Schedule

The Schedule in the Table overleaf (which shall be updated from time to time) provides for various category of record the relevant retention period and other information.

Table 1 – Filtronic Retention Schedule

Record Type	Description	Reason for Retention	Retention Periods (years)	Applicable Law
Payroll	Record of pay including, standard and overtime pay, performance related payments, payment for untaken leave, bonuses, maternity/paternity payments, taxable allowances	Inland Revenue / Contractual Claims	6+1 years after tax year end or 6+1 years after end of employment whichever is the later	Income Tax Act(s); Limitation Act 1980
	Expense Records	Inland Revenue & Internal investigations	6+1 after end of employment	Limitation Act 1980
Pension	Records relation to all pension details	Statutory Obligation and responsible business practice	For employee's lifetime	
HR Files		Statutory Obligation and good business practice	Indefinitely – as per statutory obligation and good business practice.	
H&S Records	Accident Book records	H&S at Work Act	For former / current employee's lifetime	Limitation Act 1980 H&S at Work Act

Approved by the Board of Filtronic plc
May 2023

Filtronic plc

Social Media Policy

This policy applies to all directors, employees, contractors, interns and secondees of Filtronic plc (the "Company") and its subsidiaries including staff provided by staffing agencies. It is important that anyone using social media, whether for business or personal reason, has read and understands this policy.

The Company appreciates that many people enjoy using social media and it is now entrenched in daily life with most people accessing the various platforms multiple times a day. Employees can be great ambassadors to promote and reinforce the human side of our business but at the same time, recognising comments they make on social media should be respectful. Employees represent Filtronic, at all times, so they should understand the pitfalls of inappropriate posting as the Company has a right to protect its reputation, intellectual property, trade secrets, confidential and sensitive data. The aim of our Social Media Policy is to provide guidance and explain the risks further.

In this policy the Company aims:

- To encourage employees to promote the business on social media platforms whilst respecting we are a public company listed on the London Stock Exchange. Some of the information, which if made public, could constitute 'price sensitive' news or 'inside information' and have an impact on the share price. Our policy prohibits the disclosure of price sensitive news on social media;
- To establish clear rules of engagement including personal usage of social media and engagement for the benefit of the Filtronic brand;
- To remind you that what you say on social media sites, even outside of your working time, is not private and can be damaging to the Filtronic brand;
- To understand that posts on social media are ever-present; always pause and think before posting. If you delete a post, the chances are someone has copied, retweeted or shared it;
- To emphasise that Filtronic will not tolerate comments which bring the Company, its employees, customers or other stakeholders into disrepute or which infringe the Company's other policies including, but not limited to, the IT Policy, Code of Ethics, Data Protection Policy and any other confidential or sensitive information. Always remember that passion is healthy, but anger is not;
- To explain the possible consequences of policy breaches; and
- To remind you that monitoring is taking place.

Social media means:

- Professional networking sites such as LinkedIn
- Social networking sites such as Facebook, Twitter, Snapchat and Instagram
- Social question-and-answer websites such as Quora and Reddit
- Other social media such as YouTube, SlideShare and WhatsApp
- Any media yet to be invented but fulfils the accepted definition of social media

Please note TikTok is not permitted on any company-owned devices following the UK government's decision to ban TikTok on government devices.

Social media guidelines

Below are links to Filtronic's official accounts. All employees are encouraged to follow, view and share official Filtronic posts to help amplify our brand:

LinkedIn	https://www.linkedin.com/company/filtronic
Twitter	https://twitter.com/Filtronic
YouTube	https://www.youtube.com/@Filtronic_plc

If you are creating social media posts associated with Filtronic for example, our technology, your role and the industry in general then please follow these simple rules to protect our brand and your own personal and professional brand:

1. Focus on the good – Play nice, have fun and connect. Don't use it as an opportunity to be negative about any stakeholders including our competitors or customers.
2. Be upfront - Your presence in social media must be transparent, please clarify your opinions are your own.
3. Respect – Take extra care to protect Filtronic and yourself. Be aware of the language you use
4. Use common sense – Always be professional and adhere to our values.
5. Permanent – Please be aware that whatever you say is permanent.

Before you make a comment, you should ask yourself the question: "Could what I am saying have a negative impact on Filtronic or its stakeholders?" If the answer is yes, or possibly, you should not proceed.

Use of company equipment for personal social media activities

You may use company equipment, including PCs, laptops and smartphones to access social media outside of your working hours or during breaks if your role requires it. However, you must not access any inappropriate or offensive websites (further details can be found in the IT Policy) and you must comply with the rules on responsible content.

Use of your own equipment to access social media sites whilst you are at work

You must not use your own equipment (e.g. your iPhone, iPad) to access social media when you are supposed to be working other than for the benefit of your role such as LinkedIn posts. Any usage should be restricted to breaks.

Posting responsible content on social media sites

When using social media sites such as Facebook, Instagram, TikTok (only on personal devices), Twitter, YouTube, blogs etc. you are operating in a public space and your conduct may have serious consequences for the Company, its employees, its customers/suppliers and other affiliates.

Remember, even when you are on a personal account, your social media activity could be seen by customers or potential customers, so you should treat every interaction on social media as if you are dealing with a potential customer.

All Filtronic team members are encouraged to share news and information. If you see something being shared related to Filtronic on a social media platform that shouldn't be happening or is potentially damaging to the brand, immediately inform the Marketing department, the HR department or your manager. Always remember that anything posted in social media can go viral or be screenshot, reshared or reposted as there is very little privacy protection for anything shared on social media, no matter what your privacy settings may be.

You should comply with the following basic rules whenever you are using social media sites, whether using company equipment or your own equipment and whether you are doing so during or outside of working time.

Do:

- Act within the guidelines within this policy;
- Be professional and a good citizen - When posting please be professional about the information you share;
- Write what you know – when commenting on Filtronic we encourage you to write in the first person and stick to your area of expertise if it relates to Filtronic technology;
- Remember that conversations between 'friends' on social media are not truly private and can still have the potential to cause damage;
- Focus on the good - Make sure that when posting about Filtronic that you focus on the positive impact of Filtronic;
- Support transparency, equality, diversity, and inclusion in what you say online; and
- Report to HR, Marketing or IT if you see anything on a social media site that indicates that a colleague may have breached this policy.

Do not:

- Make comments which could damage the reputation of the Company or its employees;
- Make comments which could damage the Company's relationships with its customers/suppliers and other affiliates;
- Express opinions on the Company's behalf;
- Use social media to insult, embarrass or offend a colleague, customer, supplier or other stakeholder;
- Post comments or pictures which are inconsistent with our values;
- Use social media to bully, harass, discriminate or anything that breaches the Filtronic Code of Ethics;
- Write something on social media when angry, upset or having had alcohol. If you feel strongly about something, we'd encourage you to talk to your manager or a director rather than posting your opinion on social media. It is often helpful to take some time away from your computer to clear your mind before sending, when something has made you feel emotional.
- Communicate anything sensitive, confidential or information that could be considered 'price sensitive' or 'inside information' i.e. financial or contract information;

- Communicate anything that would violate the local law; and
- Use a company e-mail address to register on social media sites except for Filtronic owned accounts where personal email addresses must not be used to register the account.

Monitoring

The Company logs and audits the use of company computers, laptops and handheld devices, including email, internet and other computer use. Software has been installed to monitor which internet sites you visit. The Company will look at the content of what you have posted or uploaded where the Company has good reason to do so. The Company does this in order to investigate and detect unauthorised use of our equipment in breach of our policies, including social media use. For further details of how the Company monitors and the purpose of monitoring, please see the IT Policy.

Breaches of this policy

Any breach of this policy will be taken seriously and may lead to disciplinary action. In serious cases, such as posting material which could damage the company's reputation, or which amounts to bullying and harassment or the disclosure of confidential information, this could include dismissal under the Company disciplinary procedure.

AIM rules dictate information of a 'price sensitive' and 'inside information' nature should be disclosed through the regulatory service on the RNS system before being released on the Company's website or social media channels. If found to be in breach of AIM Rules, it could lead to substantial fines for the Company and potentially criminal proceedings for employees.

You must remove any material posted on social media platforms in breach of this policy upon our request. Failure to comply with such a request may in itself result in disciplinary action being taken or contracts being terminated.

You must co-operate to the fullest extent possible in any investigation into suspected breaches of this policy. This may include handing over any relevant passwords in situations where we need these passwords in order to investigate a suspected breach.

Social Media Account Ownership

If you participate in social media activities as part of your job at Filtronic on an account created for that purpose, that account is considered Filtronic's property. It remains the property of Filtronic if you leave the Company meaning you will not try to change the password, account name, create a similar sounding account, assert any ownership of the account or the contacts and connections you have gained through the account. Any materials created for or posted on the account will remain Filtronic's property. This doesn't apply to personal accounts that you may access at work but does apply to all Filtronic branded accounts.

Approved by the Board of Filtronic plc
May 2023

Filtronic plc

Anti-Bribery and Corruption Policy

Filtronic is committed to the practice of responsible corporate behaviour and compliance with all laws, regulations and other requirements which govern the conduct of our operations.

The Company is fully committed to instilling a strong anti-corruption culture and is fully committed to compliance with all anti-bribery and anti-corruption legislation including, but not limited to, the Bribery Act 2010 ("the Act") and has processes to ensure that no bribes or other corrupt payments, inducements or similar are made, offered, sought or obtained by us or anyone working on our behalf.

Definition of Anti-Bribery and Corruption

This Policy should be read in conjunction with the Company's Management Policy and Code of Ethics. For the purpose of this policy, bribery and corruption are defined as giving someone a financial or other advantage to encourage that person to perform improperly in their functions or activities or to reward them for having already done so. The principles of this policy apply to all employees, agents, contractors, subcontractors, consultants, business partners and any other parties associated with the Company or its subsidiaries. This includes all employees and agents of people conducting business with the Group. Filtronic staff should take reasonable steps to ensure that there is compliance with these principles throughout the Filtronic supply chain.

It is the responsibility of all the above-mentioned parties to ensure that bribery is prevented, detected and reported.

Filtronic's Stance on Bribery and Corruption

This policy applies to all parties listed in the definition above. They will, at all times, comply with the law and have a duty to inform themselves and their direct and indirect reports about this policy and the national and international laws relating to their business activities.

Filtronic will not engage in bribery or corruption.

Parties described above must:

- Be aware and alert at all times of all bribery risks as described in this policy;
- Exercise due diligence at all times when dealing with third parties on behalf of the Company; and
- Report any, and all, concerns relating to bribery to the Chief Executive Officer, or in the case of non-employees to their normal point of contact within the Company, or otherwise in accordance with the Group's Whistleblowing Policy.

Anyone or any organisation found guilty of bribery under the Act may face fines and/or prison terms. In addition, high legal costs and adverse publicity are likely to result from any breach of the Act.

Facilitation payments

A facilitation payment is defined as a small payment made to officials in order to ensure or speed up the performance of routine or necessary functions.

Facilitation payments constitute bribes and, subject to the following paragraph, may not be made at any time irrespective of prevailing business customs in certain territories.

Facilitation or similar payments may be made in limited circumstances where your life is in danger but under no other circumstances. Any payment so made must be reported to the Chief Executive Officer as soon as is reasonably possible and practicable.

Gifts and Hospitality

Gifts and hospitality remain a legitimate part of conducting business and should be provided only in compliance with the Management Policy.

Gifts and hospitality can, when excessive, constitute a bribe and/or a conflict of interest. Care and due diligence should be exercised at all times when giving or receiving any form of gift or hospitality on behalf of the Company.

The following general principles apply:

- Gifts and hospitality may neither be given nor received as rewards, inducements or encouragement for preferential treatment or inappropriate or dishonest conduct.
- Neither gifts nor hospitality should be actively sought or encouraged from any party, nor should the impression be given that the award of any business, custom, contract or similar will be in any way conditional on gifts or hospitality.
- Cash should be neither given nor received as a gift from third parties under any circumstances.
- Gifts and hospitality to or from relevant parties should be generally avoided at the time of contracts being tendered or awarded.
- The value of all gifts and hospitality, whether given or received, should be proportionate to the matter to which they relate and should not be unusually high or generous when compared to prevailing practices in our industry or sector.
- Certain gifts which would otherwise be in breach of this Policy may be accepted if refusal would cause significant and/or cultural offence; however, the Company will donate any gifts accepted for such reasons to a charity of the Company's choosing.
- All gifts and hospitality, whether given or received, must be recorded in the Gifts and Hospitality Register.

Examples of acceptable gifts to exchange with a third party include modest, of an appropriate type and value, Christmas presents and retirement gifts. There may be instances where gift receipts will

be placed into a pool and distributed via a raffle of all employees to ensure fairness with those who are not externally facing.

Periodically, the Company will issue small gifts to its employees to acknowledge performance, effort or a special occasion. In these circumstances, the gift must be approved by an Executive Director of the Company prior to issue.

Charitable Donations

Charitable donations are permitted only to registered (non-profit) charities. No charitable donations may be given to any organisation which is not a registered charity.

All charitable donations must be fully recorded with the Finance department.

Proof of receipt of all charitable donations must be obtained from the recipient organisation.

Under no circumstances may charitable donations be made in cash.

No charitable donation may be made at the request of any party where that donation may result in improper conduct.

Political Donations

The Company does not make political donations and the Company is not affiliated with any political party, independent candidate, or with any other organisation whose activities are primarily political.

Employees and other associated parties are free to make personal donations provided such payments are not purported to be made on behalf of the Company and are not made to obtain any form of advantage in any business transaction.

Due Diligence and Risks to be aware of:

The following issues should be considered with care in any and all transactions, dealings with officials, and other business matters concerning third parties:

- Territorial risks and cross-border payments, particularly the prevalence of bribery and corruption in a particular country;
- Requests for cash payment, payment through intermediaries or other unusual methods of payment;
- Activities requiring the Company and/or any associated party to obtain permits or other forms of official authorisation; or
- Transactions involving the import or export of goods.

Reporting a Breach

Any complaints or allegations of breach of this policy may be reported directly to a Board member or confidentially through the procedure set out in the Company's Whistle Blowing Policy.

Anti-Bribery and Corruption Procedure

Procedures that should be followed during business transactions Filtronic's policy on Bribery and Corruption applies to all employees, agents, contractors, subcontractors, consultants, business partners and any other parties associated with the Company or its subsidiaries and requires that:

1 Directors and Managers should ensure that staff are aware of the Company's Anti-Bribery Policy and that the Company will not tolerate bribery;

2 Evidence of the staff communication exercise communicating the policy and procedure to all staff should be retained.

3 The risk of bribery should be considered as part of the risk assessment exercise for the business and such consideration should be evidenced;

4 Due diligence on suppliers and agents should be considered particularly before engaging them in business dealings.

5 Stakeholders of the company should:

- **(i)** Not offer or make any bribe, unauthorised payment (whether in cash or kind) or inducement of any kind;
- **(ii)** Not solicit business by offering any bribe, unauthorised payment (whether in cash or kind) or inducement to customers or potential customers. For the avoidance of doubt, providing appropriate and "proportionate" hospitality to customer or potential customers' representatives (e.g. dinner at a good quality restaurant) is not be considered unauthorised provided it has been authorised by either the CFO or CEO;
- **(iii)** not accept any kind of bribe or unusual payment or inducement that would unlikely be authorised by the Board of Filtronic in the ordinary course of business; for the avoidance of doubt, attending a training course or dinner or lunch provided by a professional firm or company is not regarded as unauthorised. For other corporate hospitality, (e.g. tickets to a sporting event) the offeree should, before accepting the offer, discuss the matter with his line manager and consider the benefits and risks to the business before accepting or refusing. Employees and agents should refuse any bribe or unorthodox payment and to do so in a manner that is not open to misunderstanding or giving rise to false expectation and to report any such offers;
- **(iv)** Not make "Facilitation Payments". These are payments made to secure or accelerate the performance of a routine action to which the payer has a legal entitlement. Filtronic does not condone such payments being made unless required for medical or safety emergencies in jurisdictions where such payments are considered normal. Where this occurs, a record of any such payment should be kept.
- **(v)** Maintain a record of all donations to charities and to political parties;
- **(vi)** Report any breaches of this policy, or the Company's Management Policy and Code of Ethics.

6 If in doubt about accepting any offer or making any offer that might be misconstrued, the employee or agent should consult his /her direct line manager/Board Director or Company Secretary.

Approved by the Board of Filtronic plc
May 2023

Filtronic plc

Anti-Trust and Competition Policy

Policy Statement

Filtronic is committed to ensuring that business is conducted in a straight-forward and ethical manner that encourages fair and open competition. This policy sets out Filtronic's position on anti-trust and competition law compliance and provides guidance to employees on the prevention, detection and reporting of behaviours which fail to comply with the requirements of these laws.

This policy applies to all persons working for Filtronic or on our behalf in any capacity, including employees at all levels, directors, officers, agency workers, seconded workers, volunteers, interns, agents, contractors, external consultants, third-party representatives and business partners.

What is anti-trust and competition?

Anti-trust and competition law prohibits behaviour that aims to reduce competition in the market. Infringement presents significant risk for every business with breaches of these laws potentially leading to significant fines for companies and imprisonment for individuals. In addition, third parties may bring damage claims against the Company to recover their losses arising from any anti-competitive practices. The enforcement of anti-trust and competition laws in many countries is increasingly stringent and encompasses activities undertaken by a company through its employees or third parties acting on its behalf.

The Company does not engage in or tolerate any form of conduct which fails to comply with the requirements and spirit of anti-trust and competition laws. The fundamental objective of anti-trust and competition law is to regulate anti-competitive behaviour by businesses and individuals which may be to the detriment of customers and competitors.

Examples of anti-trust and competition include:

- Fixing prices of services among competitors within the domestic or international market;
- Rigging bids among competitors in order to enable a competitor to win the bid;
- Limiting production or capacity in unison with competitors;
- An agreement or conduct in a certain geographic market among competitors which has a detrimental impact on competition;
- Unlawful exclusivity arrangements among entities that encourage monopolisation; and
- Unlawful mergers and acquisitions among companies.

The concept of agreement under competition law is generally very broad and can include formal or informal agreements, in writing or otherwise (ie. ranging from written contracts to informal understandings).

Procedure

Our employees and persons connected with Filtronic are prohibited from engaging in any activity that promotes unlawful anti-trust and competition behaviour. This includes formal or informal agreements with competitors, trade associations or industry bodies which result in price fixing, bid rigging, market allocation and arrangements to limit supply. Arrangements like this are almost always illegal and are often criminal.

Be extremely careful in any discussions (including any acquisition negotiations) with actual or potential competitors. Anti-trust and competition law concerns all dealings or communications (including emails and reports) with or relating to suppliers, distributors, customers, competitors and/or markets. Use words carefully, careless use of words can make legitimate competitive activity appear suspect.

Ensure agreements with suppliers, distributors and customers containing restrictions on price, products or territory and/or including any elements of exclusivity, are carefully analysed with the benefit of legal advice before being entered into. Such arrangements should not be entered into with competitors, save for very limited exceptions and any such arrangement should not be entered into without clearance following legal advice.

Address any issues of concern prior to engaging in any particular conduct, the impact of which may be potentially anti-competitive and seek immediate legal advice in the event of any concerns or doubts regarding compliance with anti-trust and competition law requirements.

Prevention of Anti-Competitive Practices

Our anti-trust and competition preventative measures consists of the following elements:

- Consideration of anti-competition risks when exploring new business opportunities;
- Ensure adequate policies and procedures are formulated;
- Investigate allegations relating to anti-competitive behaviour and take appropriate action accordingly; and
- Communicating the message of fair and open competition to the business.

The responsibility for the implementation of this policy rests with all Filtronic employees, our partners and those who represent us. In particular, anybody approving legal documents should pay close attention to adherence with anti-trust and competition laws before entering into the agreement.

When anti-competitive behaviour is found, any transactions that may have been affected will be reviewed retrospectively. An investigation will be conducted by the directors to determine the extent of the breach and the intentions of the parties involved. Where anti-competitive behaviour has been identified the affected stakeholders will be notified.

Reporting suspected anti-trust and competition behaviour

When an employee understands or suspects that anti-competitive practices have been undertaken, they should bring this matter to the attention of an Executive Director as soon as discovered. Managers and Supervisors must also keep an eye on potential anti-competitive behaviour arising relating to the employees that report to them.

In the event that the employee feels the anti-trust and competition issue falls into any of the three categories below:

a) The matter is not resolved to a satisfactory level and an Executive Director is already aware;
b) The employee feels compromised that reporting anti-competitive behaviour involving another member of staff, their manager or an Executive Director would adversely impact their position; or
c) It is an Executive Director that has engaged in anti-trust and competitive behaviour that the employee is uncomfortable with and feels that speaking to the Executive Director would adversely impact their position.

In these circumstances, employees can use the procedure within the Filtronic whistleblowing policy which is set out within the Filtronic Group Policies.

Failure to comply with this policy may result in disciplinary action, which may lead to dismissal, and may expose the Company and/or its employees to criminal or civil liability.

Approved by the Board of Filtronic plc
October 2023

Filtronic plc

Conflict of Interest Policy

Policy Statement

Filtronic is committed to ensure that a conflict of interest does not arise between an employee's personal interest and the interests of the Company. This policy outlines the rules and responsibilities of employees and the Company to resolve any such discrepancies so an employee's judgement and commitment to the Group is not compromised.

This policy applies to all persons working for Filtronic or on our behalf in any capacity, including employees at all levels, directors, officers, agency workers, seconded workers, volunteers, interns, agents, contractors, external consultants, third-party representatives and business partners.

Policy elements

The relationship of the Company with its employees is based on mutual trust. As the Company is committed to preserve the interests of people under its employment, or indeed working on behalf of it, it expects them to act only towards Filtronic's interests.

A conflict of interest may occur when an employee's interest in a particular subject may lead them to actions, activities or relationships that undermine Filtronic and may place it at a disadvantage.

What is an employee conflict of interest?

A conflict of interest can take many different forms that include, but are not limited to, conflict of interest examples:

- Employees' ability to use their position with the Company to their personal advantage;
- Employees engaging in activities that will bring direct or indirect profit to a competitor;
- Employees owning direct shares of a competitor, customer or supplier's stock;
- Employees using connections obtained through the Company for their own private purposes;
- Employees using company equipment or means to support an external business; and
- Employees acting in ways that may compromise the Company's legality (eg. taking bribes or bribing representatives of legal authorities).

Procedure

The responsibility for resolving a conflict of interest starts with the immediate manager and depending on the status and severity may reach the directors of the Group. All conflicts of interest will be resolved as fairly as possible, and steps taken to address the conflict. The directors have the responsibility of the final decision when a solution can't be found.

When an actual conflict of interest is found, any transactions that may have been affected will be reviewed retrospectively. An investigation will be conducted by the directors to determine the extent of the conflict and the intentions of the parties involved. Where a conflict of interest has been identified the affected stakeholders will be notified. However, if no conflict exists, the investigation may be documented, but no further action will be taken.

In general, employees are advised to refrain from letting personal and financial interests as well as external activities come into opposition with the Company's interests.

Reporting a suspected conflict of interest

The majority of conflict of interests can be addressed and resolved before any actual damage is done and controls put in place to mitigate any instance arising. Therefore, when an employee understands or suspects that a conflict of interest exists, they should bring this matter to the attention of their manager so corrective actions may be taken. Managers and Supervisors must also keep an eye on potential conflict of interests arising relating to the employees that report to them.

If the conflict of interest involves an employee's manager, and the employee feels they can't approach their manager, or the employee feels sufficiently uncomfortable that the conflict of interest may adversely impact their own position within the Company if an Executive Director is not aware, but later finds out, then it is advisable to make an Executive Director of the Company aware of the situation as well as your manager.

In the event that the employee feels the conflict of interest falls into any of the three categories below:

d) The conflict of interest is not resolved to a satisfactory level and an Executive Director is already aware;
e) The employee feels compromised that reporting a conflict of interest involving another member of staff, their manager or an Executive Director would adversely impact their position; or
f) It is an Executive Director that has the conflict of interest that the employee is uncomfortable with and feels that speaking to the Executive Director would adversely impact their position.

In these circumstances, employees can use the procedure within the Filtronic whistleblowing policy which is set out within the Filtronic Group Policies.

Approved by the Board of Filtronic plc
May 2023

Filtronic plc

Anti-Facilitation of Tax Evasion Policy

Policy statement

Filtronic is committed to conducting all our business in an honest and ethical manner. We take a zero-tolerance approach to the facilitation of tax evasion, whether under UK law or under the law of any foreign country. We are committed to acting professionally, fairly and with integrity in all our business dealings and relationships wherever we operate, and to implement and enforce effective systems to counter tax evasion facilitation.

We take our legal responsibilities very seriously. We will uphold all laws relevant to countering tax evasion in all the jurisdictions in which we operate, including the Criminal Finances Act 2017.

About this policy

The purpose of this policy is to:

- set out our responsibilities, and the responsibilities of those working for us, in observing and upholding our position on preventing the criminal facilitation of tax evasion; and
- provide information and guidance to those working for us on how to recognise and avoid tax evasion.

Who does this policy apply to?

This policy applies to all persons working for Filtronic or on our behalf in any capacity, including employees at all levels, directors, officers, agency workers, seconded workers, volunteers, summer placements, agents, contractors, external consultants, third-party representatives and business partners, sponsors, or any other person associated with us, wherever located.

In this policy, third party means any individual or organisation you come into contact with during the course of your work for us, and includes actual and potential clients, customers, suppliers, distributors, business contacts, agents, advisers, and government and public bodies, including their advisers, representatives and officials, politicians, and political parties.

Responsibility - Who is responsible for the policy?

The Board has overall responsibility for the effective operation of this policy but has delegated responsibility for overseeing its implementation to the Executive Directors and the Company Secretary.

Line managers have day-to-day responsibility for this policy. You should refer any questions or suggestions about this policy to an Executive Director, the Company Secretary or the Head of HR where appropriate.

Points of Contact and Reporting

For further information or queries relating to this policy including training offered in relation to it please contact the CEO, the CFO or the Company Secretary. If there is any suspicion of an employee or an associate attempting to commit tax evasion, please get in touch with either the CEO or the CFO or alternatively follow the Group's Whistleblowing Policy. All communications will be dealt with in the strictest confidence.

Responsibilities of all Employees and Associates

(i) Not engage in any form of tax evasion or facilitation of tax evasion.

(ii) Understand and adhere to this policy at all times.

(iii) Promptly report any known or suspected tax evasion.

What is tax evasion and tax evasion facilitation?

Tax evasion - means the illegal or fraudulent evasion of taxes by individuals or entities. It involves deliberate and dishonest conduct. This is not the same as tax planning, which is not illegal (and involves taking steps, within the law, to minimise tax payable).

Tax evasion facilitation - means the facilitation of tax evasion means knowingly aiding or abetting an individual or entity in evading tax.

What taxes are covered? Tax means all forms of taxation, including but not limited to corporation tax, income tax, value added tax, all types of stamp duty, and national insurance contributions (and their equivalents in any non-UK jurisdiction).

"Red Flags"/Examples - The following is a list of examples of possible red flags that may arise during the course of your working for Filtronic and which may raise concerns related to tax evasion or foreign tax evasion:

- A contract being set up with a new customer as a contract for services, despite it being a provision of goods, to help the customer evade the higher tax that would be due under a contract for goods arrangement;
- Agreeing to send a bill to a different person / entity than who the work was done for, or to a different address, or with a misleading description, in each case knowing that this gives the purchaser or supplier a better tax position;
- Staff being resourced via an agency, with full knowledge of the agency's practice to pay these staff in cash and not declare their income to HMRC;
- A manager signs off an employee's expense claims knowing that they are also using the same receipts to reduce their personal tax bill;
- Intentional manipulation of documents, for example, falsifying dates on dividend documents to alter the tax year in which tax would become due;
- A third party to whom we have provided services requests that their invoice is addressed to a different entity, where we did not provide services to that entity directly;
- Third-party requests that payment is made to a country or geographic location different from where the third party resides or conducts business; or
- A third party insists on the use of side letters or refuses to put terms agreed in writing or asks for contracts or other documentation to be backdated.

Approved by the Board of Filtronic plc
May 2023

Filtronic plc

Share Dealing Policy and Dealing Code

This policy applies to all directors and employees of Filtronic plc (the Company) and its subsidiaries. It has been designed to ensure that you do not misuse, or place yourself under suspicion of misusing inside information about the Group which you have and which is not public. Directors and employees must comply with their obligations under the Market Abuse Regulation ("MAR").

1 You must not ***deal*** in any ***securities*** of the ***Group*** if you are in possession of ***inside information*** about the ***Group***. You must also not recommend or encourage someone else to ***deal*** in the ***Group's securities*** at that time – even if you will not profit from such ***dealing***.

2 You must not disclose any confidential information about the ***Group*** (including any ***inside information***) except where you are required to do so as part of your employment or duties. This means that you should not share the ***Group's*** confidential information with family, friends or business acquaintances.

3 You may, from time to time, be given access to ***inside information*** about another group of companies (for example, one of *the* ***Group's*** *customers* or suppliers). You must not ***deal*** in the ***securities*** of that group of companies at those times.

4 The Group also operates a Dealing Code which applies to the ***Company's*** directors and to employees who are able to access restricted information about the ***Group*** (for example, employees who are involved in the preparation of the ***Group's*** financial reports and those working on other sensitive matters). Because of the relatively small number of employees in the Filtronic Group of Companies, all Filtronic employees are required to comply with the Dealing Code. Directors and employees who are required to comply with the Dealing Code must also comply with this policy.

5 Failure to comply with this policy may result in internal disciplinary action. It may also mean that you have committed a civil and/or criminal offence.

6 If you have any questions about this policy, or if you are not sure whether you can deal in securities at any particular time, please contact the Company Secretary who will request clearance to deal on your behalf from the Chairman or CEO as appropriate.

Glossary: For the purposes of this policy:

- ***deal*** and ***dealing*** covers any type of transaction in a company's ***securities***, including purchases, sales, the exercise of options and using ***securities*** as collateral for a loan
- the ***Group*** means the ***Company*** and its subsidiaries
- ***inside information*** is information about a company or its ***securities*** which is not publicly available, which is likely to have a non-trivial effect on the price of such ***securities*** and which an investor would be likely to use as part of the basis of his or her investment

decision

- ***securities*** are any publicly traded or quoted shares or debt instruments, and any linked derivatives or financial instruments. This would include shares, depositary receipts, options and bonds

Share Dealing Code

Part A of this code contains the Dealing clearance procedures which must be observed by the Company's PDMRs and those employees who have been told that the clearance procedures apply to them. This means that there will be certain times when such persons cannot Deal in Company Securities.

At present, all employees of the Filtronic plc Group must comply with the clearance procedures in Part A

Part B sets out certain additional obligations which only apply to PDMRs.

Failure by any person who is subject to this code to observe and comply with its requirements may result in disciplinary action. Depending on the circumstances, such non-compliance may also constitute a civil and/or criminal offence.

Schedule 1 sets out the meaning of capitalised words used in this code.

Part A – Clearance procedures

Clearance to Deal

You must not Deal for yourself or for anyone else, directly or indirectly, in Company Securities without obtaining clearance from the Company in advance.

Applications for clearance to Deal must be made in writing and submitted to the Company Secretary* (and in the absence of the Company Secretary any executive director of Filtronic plc) using the form set out in Schedule 2.

You must not submit an application for clearance to Deal if you are in possession of Inside Information. If you become aware that you are or may be in possession of Inside Information after you submit an application, you must inform the Company Secretary as soon as possible and you must refrain from Dealing (even if you have been given clearance).

You will receive a written response to your application, normally within five business days. The Company will not normally give you reasons if you are refused permission to Deal. You must keep any refusal confidential and not discuss it with any other person.

If you are given clearance, you must Deal as soon as possible and in any event within two business days of receiving clearance.

Clearance to Deal may be given subject to conditions. Where this is the case, you must observe those conditions when Dealing.

Programme under which Company Securities may be purchased or sold unless clearance has

been given to do so.

Different clearance procedures will apply where Dealing is being carried out by the Company in relation to an employee share plan (e.g. if the Company is making an option grant or share award to you, or shares are receivable on vesting under a long-term incentive plan). You will be notified separately of any arrangements for clearance if this applies to you.

If you act as the trustee of a trust, you should speak to the Company Secretary about your obligations in respect of any Dealing in Company Securities carried out by the trustee(s) of that trust.

You should seek further guidance from the Company Secretary before transacting in:

(A) units or shares in a collective investment undertaking (e.g. a UCITS or an Alternative Investment Fund) which holds, or might hold, Company Securities; or

(B) financial instruments which provide exposure to a portfolio of assets which has, or may have, an exposure to Company Securities.

This is the case even if you do not intend to transact in Company Securities by making the relevant investment.

Further guidance

- If you are uncertain as to whether or not a particular transaction requires clearance, you must obtain guidance from the Company Secretary before carrying out that transaction.
- In the absence of the Company Secretary please speak to any Executive Director of Filtronic plc.

Part B – Additional Provisions for PDMRs

Circumstances for refusal

You will not ordinarily be given clearance to Deal in Company Securities during any period when there exists any matter which constitutes Inside Information or during a Closed Period.

Notification of transactions

You must notify the Company and the FCA in writing of every Notifiable Transaction in Company Securities conducted for your account as follows:

(C) Notifications to the Company must be made using the template in Schedule 3 and sent to the Company Secretary as soon as practicable and in any event within one business day of the transaction date. You should ensure that your investment managers (whether discretionary or not) notify you of any Notifiable Transactions conducted on your behalf promptly so as to allow you to notify the Company within this time frame.

(D) Notifications to the FCA must be made within three business days of the transaction date. A copy of the notification form is available on the FCA's website. If you would like, the Company Secretary can assist you with this notification, provided that you

ask him or her to do so within [one business day] of the transaction date.

If you are uncertain as to whether or not a particular transaction is a Notifiable Transaction, you must obtain guidance from the Company Secretary.

PCAs and investment managers

You must provide the Company with a list of your PCAs and notify the Company of any changes that need to be made to that list.

You should ask your PCAs not to Deal (whether directly or through an investment manager) in Company Securities during Closed Periods and not to deal on considerations of a short-term nature. A sale of Company Securities which were acquired less than a year previously will be considered to be a Dealing of a short- term nature.

Your PCAs are also required to notify the Company and the FCA in writing, within the time frames given in paragraph 4.1, of every Notifiable Transaction conducted for their account. You should inform your PCAs in writing of this requirement and keep a copy; the Company Secretary will provide you with a letter that you can use to do this. If your PCAs would like, the Company Secretary can assist them with the notification to the FCA, provided that your PCA asks the Company Secretary to do so within [one business day] of the transaction date. A copy of the form for notifying the FCA is available on the FCA's website.

You should ask your investment managers (whether or not discretionary) not to Deal in Company Securities on your behalf during Closed Periods.

Schedule 1 Defined terms

'**Closed Period**' means any of the following:

(E) the period of 30 calendar days before the release of the preliminary announcement of the Company's annual results (or, where no such announcement is released, the period of 30 calendar days before the publication of the Company's annual financial report);

(F) the period of 30 calendar days before the release of the Company's half-yearly financial report.

'**Company Securities**' means any publicly traded or quoted shares or debt instruments of the Company (or of any of the Company's subsidiaries or subsidiary undertakings) or derivatives or other financial instruments linked to any of them, including phantom options.

'**Dealing**' (together with corresponding terms such as 'Deal' and 'Deals') means any type of transaction in Company Securities, including purchases, sales, the exercise of options, the receipt of shares under share plans, using Company Securities as security for a loan or other obligation and entering into, amending or terminating any agreement in relation to Company Securities (e.g. a Trading Plan).

'**FCA**' means the UK Financial Conduct Authority.

'**Inside Information**' means information which relates to the Company or any Company Securities, which is not publicly available, which is likely to have a non-trivial effect on the price of Company Securities and which an investor would be likely to use as part of the basis of his or her investment decision.

'**Investment Programme**' means a share acquisition scheme relating only to the Company's shares under which: (A) shares are purchased by a Restricted Person pursuant to a regular standing order or direct debit or by regular deduction from the person's salary or director's fees; or (B) shares are acquired by a Restricted Person by way of a standing election to re-invest dividends or other distributions received; or (C) shares are acquired as part payment of a Restricted Person's remuneration or director's fees.

'**Market Abuse Regulation**' means the EU Market Abuse Regulation (596/2014) as amended pursuant to The Market Abuse (Amendment) (EU Exit) Regulations 2019.

'**Notifiable Transaction**' means any transaction relating to Company Securities conducted for the account of a PDMR or PCA, whether the transaction was conducted by the PDMR or PCA or on his or her behalf by a third party and regardless of whether or not the PDMR or PCA had control over the transaction. This captures every transaction which changes a PDMR's or PCA's holding of Company Securities, even if the transaction does not require clearance under this code. It also includes gifts of Company Securities, the grant of options or share awards, the exercise of options or vesting of share awards and transactions carried out by investment managers or other third parties on behalf of a PDMR, including where discretion is exercised by such investment managers or third parties and including under Trading Plans or Investment Programmes.

'**PCA**' also '**CAP**' means a person closely associated with a PDMR being:

(A) the spouse or civil partner of a PDMR; or

(B) a PDMR's child or stepchild under the age of 18 years who is unmarried and does not have a civil partner; or

(C) a relative who has shared the same household as the PDMR for at least one year on the date of the relevant Dealing; or

(D) a legal person, trust or partnership, the managerial responsibilities of which are discharged by a PDMR (or by a PCA referred to in paragraphs (A), (B), or (C) of this definition), which is directly or indirectly controlled by such a person, which is set up for the benefit of such a person or which has economic interests which are substantially equivalent to those of such a person.

'**PDMR**' means a person discharging managerial responsibilities in respect of the Company, being either:

(A) a director of the Company; or

(B) any other employee who has been told that he or she is a PDMR.

'**Restricted Person**' means:

(A) a PDMR; or

(B) any other person who has been told by the Company that the clearance procedures in Part A of this code apply to him or her.

'**Trading Plan**' means a written plan entered into by a Restricted Person and an independent third party that sets out a strategy for the acquisition and/or disposal of Company Securities by the Restricted Person, and:

(A) specifies the amount of Company Securities to be dealt in and the price at which and the date on which the Company Securities are to be dealt in; or

(B) gives discretion to that independent third party to make trading decisions about the amount of Company Securities to be dealt in and the price at which and the date on which the Company Securities are to be dealt in; or

(C) includes a method for determining the amount of Company Securities to be dealt in and the price at which and the date on which the Company Securities are to be dealt in.

Schedule 2

Clearance application template

Filtronic plc (the '**Company**')

Application for clearance to deal

If you wish to apply for clearance to deal under the Company's dealing code, please complete sections 1 and 2 of the table below and submit this form to the Company Secretary. By submitting this form, you will be deemed to have confirmed and agreed that:

(i) the information included in this form is accurate and complete;

(ii) you are not in possession of inside information relating to the Company or any Company Securities;

(iii) if you are given clearance to deal and you still wish to deal, you will do so as soon as possible and in any event within two business days; and

(iv) if you become aware that you are in possession of inside information before you deal, you will inform the Company Secretary and refrain from dealing.

Application Form for Clearance to Deal under Part A of the Filtronic plc Group Share Dealing Policy

1.	**Applicant**	
a)	Name	
b)	Contact details	*[For executive directors and other employees, please include email address and extension number.]* *[For non-executive directors, please include email address and telephone number.]*
2.	**Proposed dealing**	
a)	Description of the securities	*[e.g. a share, a debt instrument, a derivative or a financial instrument linked to a share or debt instrument.]*
b)	Number of securities	*[If actual number is not known, provide a maximum amount (e.g. 'up to 100 shares' or 'up to £1,000 of shares').]*
c)	Nature of the dealing	*[Description of the transaction type (e.g. acquisition; disposal; subscription; option exercise; settling a contract for difference; entry into, or amendment or cancellation of, an investment programme or trading plan).]*
d)	Other details	*[Please include all other relevant details which might reasonably assist the person considering your application for clearance (e.g. transfer will be for no consideration).]* *[If you are applying for clearance to enter into, amend or cancel an investment programme or trading plan, please provide full details of the relevant programme or plan or attach a copy of its terms.]*

Schedule 3

Notification template for PDMRs and their closely associated persons (PCAs also CAPs)

Filtronic plc (the '**Company**') Transaction notification

The form is electronic, and it is submitted by the PDMR, directly to the FCA, online, via this link: https://marketoversight.fca.org.uk/electronicsubmissionsystem/MaPo_PDMR_Introduction

After submission, please send your completed form to the Company Secretary, and in the Company's Secretary's absence, please send it to the CFO. The contents of the form (example set out below) will be announced by the Company via RNS.

If you require any assistance in completing this form, please contact the Company Secretary or the CFO.

1.	**Details of PDMR / person closely associated with them ('PCA')**	
a)	Name	[*Include first name(s) and last name(s).*] [*If the PCA is a legal person, state its full name including legal form as provided for in the register where it is incorporated, if applicable.*]
2.	**Reason for Notification**	
a)	Position / status	*For PDMRs, state job title e.g. CEO, CFO.*] [*For PCAs, state that the notification concerns a PCA and the name and position of the relevant PDMR.*]
b)	Initial notification / amendment	[*Please indicate if this is an initial notification or an amendment to a prior notification. If this is an amendment, please explain the previous error which this amendment has corrected.*]
3.	**Details of the Issuer**	
a)	Name	Filtronic plc
4.	**Details of the transaction(s): section to be repeated for (i) each type of instrument; (ii) each type of transaction; (iii) each date; and (iv) each place where transactions have been conducted**	
a)	Description of the financial instrument	[*State the nature of the instrument e.g. a share, a debt instrument, a derivative or a financial instrument linked to a share or debt instrument.*]
	Identification	GB0003362992

b)	Nature of the transaction	[*Description of the transaction type e.g. acquisition, disposal, subscription, contract for difference, etc.*] [*Please indicate whether the transaction is linked to the exercise of a share option programme.*] [*If the transaction was conducted pursuant to an investment programme or a trading plan, please indicate that fact and provide the date on which the relevant investment programme or trading plan was entered into.*]
c)	Price(s) and volume(s)	[*Where more than one transaction of the same nature (purchase, disposal, etc.) of the same financial instrument are executed on the same day and at the same place of transaction, prices and volumes of these transactions should be separately identified in the table above, using as many lines as needed. Do not aggregate or net off transactions.]* [*In each case, please specify the currency and the metric for quantity.*]
d)	Aggregated information - Aggregated volume - Price	[*Please aggregate the volumes of multiple transactions when these transactions:* *– relate to the same financial instrument;* *– are of the same nature;* *– are executed on the same day; and* *– are executed at the same place of transaction.*] [*Please state the metric for quantity.*] [*Please provide:* *– in the case of a single transaction, the price of the single transaction; and* *– in the case where the volumes of multiple transactions are aggregated, the weighted average price of the aggregated transactions.*] [*Please state the currency.*]
e)	Date of the transaction	*Date of the particular day of execution of the notified transaction, using the date format: YYYY-MM-DD and please specify the time zone.*]
f)	Place of the transaction	[*Please name the trading venue where the transaction was executed. If the transaction was not executed on any trading venue, please state 'outside a trading venue' in this box.*]

Filtronic plc

Pandemic Policy

Introduction

Viruses can be the cause of highly infectious illnesses that have the capacity to spread rapidly. A pandemic is likely to occur when a new viral strain emerges. It will spread rapidly because people will not have any natural resistance to it. It is difficult to predict the scale, severity and impact of a pandemic, but research suggests that it could affect the entire country and that up to half the population could develop the illness. There could also be more than one wave of the pandemic.

During a pandemic, Filtronic's overall aim will be to keep our staff safe while encouraging them to carry on as normal if they are well, while taking additional precautions to protect them from exposure to infection and to lessen the risk of spread to others and at all times adhering to relevant Government/State and Local Authority Guidelines as applicable in relation to the pandemic.

In terms of business continuity, this means that we will seek to sustain our core business and services as far as is practicable during the pandemic and therefore we will continue to operate largely within the existing framework of company policies and procedures. However, the company recognises that during such times some additional provisions will be required to support staff.

In the event a Pandemic is declared by the government, Filtronic will establish a Business Continuity Team (the "BCT") to monitor the latest Government advice in relation to the pandemic. The priority for the BCT will be to implement the relevant guidance and controls to keep our employees (as well as our visitors, customers and suppliers) safe whilst endeavouring to keep our business operational. Employees will be kept informed by the BCT and/or their immediate supervisors of the specific measures and protocols to be adopted and implemented by all employees.

During a Pandemic

During a recognised pandemic, the company will implement the following provisions:

Communications

During the period of a pandemic, regular guidance and sources of information and support will be made available via line managers/supervisors, noticeboards, the company's Intranet and Website. Staff should monitor these sources closely to stay up to date with what is happening within the workplace and what action is being taken to ensure the company meets its obligations to staff, customers and other stakeholders.

IN ORDER TO KEEP US ALL SAFE, IT WILL BE IMPERATIVE FOR ALL STAFF TO FOLLOW THE LATEST PROTOCOLS AND GUIDANCE ISSUED BY THE COMPANY/GOVERNMENT/LOCAL AUTHORITY/STATE FROM TIME TO TIME IN RELATION TO THE PANDEMIC.

Additional Hygiene Arrangements

- Employees should wash their hands more frequently with soap and water for a minimum of 20 seconds.

- The company will provide alcohol-based sanitiser located throughout company premises and staff will be encouraged and reminded to use these regularly.
- All surfaces, door handles, banister rails, telephones, computer keyboards etc. will be cleaned more frequently.
- All waste bins will be emptied daily.
- Staff are encouraged to always use clean tissues to cover their mouth/nose when they cough/sneeze (and not to use cloth handkerchiefs or re-use tissues).
- Staff should maintain good social distancing at 2 metre intervals from colleagues and visitors.
- Rooms will be limited to maximum occupancy.
- Employees must not touch or shake hands with another person during the pandemic.

Vaccination (when available)

- The company may identify certain key staff and with their consent, arrange for those staff to be given a vaccination at the company's expense.
- This would be a purely voluntary arrangement and staff may refuse to have this if they wish.

Visitors

- Visitor passes will largely be discontinued except in exceptional circumstances for the duration of the pandemic.
- Visitors will be asked if they have any of the relevant symptoms or visited an area of higher risk identified by the government before being allowed into company premises.
- Where elevated temperature is a symptom of the illness, visitors will be asked to have their temperature taken using the company's contactless temperature readers. The reading will be noted on their entry form and retained for a maximum of 30 days.
- Visitors will be asked to sanitise their hands before entering the company premises.
- Visitors will be accompanied and should be confined to meeting rooms where at all possible.
- Visitors will be asked to wear a mask or face covering whilst on site.

Face to Face Meetings

- Travel should largely be avoided unless absolutely essential and in particular if it involves the use of public transport. All travel and off-site meetings relating to Filtronic business must be approved by an Executive Director.
- Face to face meetings should be avoided wherever possible and use of telephone/teleconferencing/email facilities should be encouraged.
- Where face to face meetings are unavoidable, the Company's meeting rooms should be used which will have sanitiser pumps/tissues/waste bins and additionally appropriate screening will be provided and all surfaces cleaned after each meeting where required by either the relevant risk assessment and/or Government guidelines.

Staff Identified as Potentially At-risk

- Staff at risk of developing viral infection-related complications (e.g. pregnant workers and those with compromised immune systems) will be reassigned from high-risk work sites and locations in the event of a pandemic. If this is not possible it may be necessary to ask such staff to work from home or remain at home (medically suspended) until it is deemed safe to return to the workplace.

Staff with Symptoms of the Pandemic virus or disease (the most significant symptoms will be communicated to staff at the time of the outbreak)

Whilst at Work
If a member of staff feels ill with symptoms consistent with the viral pandemic, it is important that they do not simply carry-on working. They should report their illness immediately to their line manager and if the symptoms are consistent with the viral infection, they will be sent home, advised to contact their GP and told not to return to work until the symptoms have cleared or have had a test for the virus which has been confirmed negative.

Whilst not at Work
If they develop symptoms whilst not at work, they should adhere to the following advice:

- Inform their line manager that they are ill using the recognised process
- Stay at home and rest
- Not go to work until they are fully recovered or they have isolated for the prescribed period so that they are no longer infectious

As part of the reporting procedures, the line manager will seek the permission of the employee to inform their colleagues that they are suffering from the viral infection. This is really a private matter for the individual but allowing colleagues to know about it will allow them to self-isolate if required or advised, look out for early symptoms in themselves, and also allow any who may be at-risk in some way (e.g. pregnant) to seek medical advice.

Testing, Track and Trace
Where the Government operates a testing and, where relevant, a track and trace system, staff showing symptoms of the virus (or being told to isolate via track & trace) must make every effort to take a test, in line with government recommendations. It will be vital for the Company to know as soon as possible if any staff carry the virus so that appropriate action can be taken to secure that staff member's work bubble. Refusing to get a test would mean that the Company would be obliged to assume that the staff member is infected by the virus which would require the self-isolation of all members of that work bubble

Staff Who Have Difficulty Attending Work (where they themselves do not have symptoms and nor does anybody in their household/social bubble)
In general staff will have no right to refuse to attend work during a pandemic unless there is a clear health and safety risk. Their employment contract will oblige them to carry out their normal duties and refusal to do so may put them in breach of their contract. However, the company is aware that certain situations can occur:

a) **Public transport is shut down**
Where an employee has difficulty getting to work because of a failure in the public transport system due to the pandemic, then they will be encouraged to seek other methods of getting to work. In exceptional circumstances, it may be possible for some staff to work from home during this period of difficulty, to vary their start and end times, or to take annual or unpaid leave. Employees will not be paid if they fail to turn up for work and should discuss the options with their line manager as soon as possible.

b) **The employee reports that a member of their household has been diagnosed with the virus but that they themselves are OK and would be willing to attend work**
The Company recognises it has a duty of care to others in the workforce and the individual will be advised to remain at home until the ill relative is no longer infectious, however the company might wish to discuss the possibility of the employee working from home if possible. Under these circumstances, the employee will receive their full pay as if they had been working normally. If an employee is unable to fulfil their role effectively from home, then alternative paid or unpaid absence will be considered.

c) **The employee reports that their child or other dependant has the virus and they are unable to arrange care at short notice:**
Under these circumstances, the company recognises that the employee has a statutory right to a reasonable period of time off to care for these dependants. This is limited to sufficient time off to deal with the immediate issue and sort out longer-term caring arrangements; the individual should discuss their situation with their line manager. The company will apply the provisions of its Dependants Leave Policy in these circumstances after which annual or unpaid leave would need to be taken. However, if the sick individual is a member of the employee's household then the provisions of b) above would apply.

d) **The employee has school-age children and the school is closed due to the viral infection pandemic:**
The provisions of c) above would apply

Working Flexibly
The impact of any pandemic will normally mean an increased workload due to a reduction in the actual staff available for work. It will therefore be essential that we maximise the capacity of our available workforce by asking staff to work more flexibly and /or differently. Therefore, the company reserves the right to ask staff to undertake one or more of the following options:

- work additional hours to cover for sick colleagues
- work more flexibly as required
- work in a different job role for a period (with appropriate training)
- work from an alternative location, or even from home if appropriate
- cancel planned annual leave

The use of these flexible work practices will vary depending on the seriousness of the staff shortages and the needs of the business at that time. Staff will be paid based on the additional hours and responsibilities they undertake.

Post-Pandemic Considerations

After the first wave of a pandemic, the company acknowledges that staff will need time to completely recover their full fitness and performance levels. Managers will ensure that staff who had been asked to work extended hours, or were denied their planned leave, are given annual leave where at all possible. However, the possibility of subsequent pandemic waves has to be kept in mind and the company will discuss with staff the lessons learnt from the current pandemic and continue with the preparations required to cope with subsequent waves.

Approved by the Board of Filtronic plc
May 2023

Filtronic plc

Export Control Policy

Policy Statement

Filtronic plc ("the Company") together with its subsidiary companies (herein "Filtronic") is committed to a policy of compliance with the strategic export control laws, regulations and procedures of all relevant jurisdictions and regimes in which it operates. In addition, Filtronic is committed to complying with the sanctions laws and regulations of the United Nations (UN), and the United Kingdom ("UK") as well as applicable sanctions laws and regulations in the territories in which it does business.

Background

Export control is a complex regulatory area, and all Filtronic employees need to ensure that they comply with applicable export and import laws and regulations when transferring goods, services, software or technology within their country or across national borders. Filtronic maintains documented procedures which give a more comprehensive appreciation of the issues involved. Where appropriate they set out roles and responsibilities whether at individual, business-function, or corporate level. The detailed 'process flow' relating to export control is documented within the internal control system of the business to determine what is required of employees at each stage of the businesses process.

Filtronic's policy statement defines the minimum standards which all Filtronic entities must comply with, including:

(i) Screening potential, new and existing customers, suppliers and transactions relating to export against the sanctions lists issued by the United Kingdom, as well as the UN. (Current sanctions territories can be found at: https://www.gov.uk/guidance/current-arms-embargoes-and-other-restrictions.)

(ii) Ensuring that all exports of goods and services and the transfer of data comply with the Export Control Act of 2002 together with the UK Strategic Export Control Lists, applying for an export licence if necessary. (For information on applying for an export licence and export controls in general refer the UK Strategic Export Control Lists as updated from time to time and to https://www.gov.uk/guidance/beginners-guide-to-export-controls and https://www.gov.uk/guidance/current-arms-embargoes-and-other-restrictions.)

(iii) Prohibiting exports of goods and other business activity that Filtronic believes may violate applicable sanctions laws or this Filtronic's policy on sanctions. This includes individuals or entities named on an applicable sanctions list or directly or indirectly involving countries or territories subject to comprehensive sanctions. (Current sanctions territories can be found at: https://www.gov.uk/guidance/current-arms-embargoes-and-other-restrictions.)

(iv) Complying with the additional Insurance Requirements set out in Annex 1 of this policy.

Explanation
Strategic Export Controls is the term applied to the control regimes that most countries apply to the export licensing or authorisation process by which exports of certain categories of goods, technology, software and services are 'approved'. These control regimes embrace all 'military' items and significant areas of what are called ‘dual-use’ items (items that not designed or modified for ‘military’ purposes but could be used as such). This covers certain products, components, software and technology.

Strategic Export Controls’ impact on the operations of the Filtronic Group in four main areas:

- Controls on the export of ‘military’ goods, software, related technology and services. These controls are applied by the country where the exporting business unit is located.
- Controls on the export of ‘dual-use’ goods, software and related technology. These are also generally applied by the country where the exporting business is located.
- Extraterritorial application of regulations of some countries on the re-export of controlled goods, software, technology and services (both 'military' and 'dual-use'), regardless of the country where the business unit is located. This is particularly relevant to US Export Regulations, but also applies to the regulations of other countries including the UK.
- ‘End Use’ and/or ‘Destination’ controls applied to ‘dual-use’ goods, software and related technology under some jurisdictions.

Please note that Strategic Export Controls operates in parallel with Sanctions laws and regulations and what may be permitted under Strategic Export Control may be prohibited under Sanctions law and regulations.

Compliance with Export Control Policy

Filtronic's policy of compliance with the export control laws of all relevant jurisdictions and regimes in which it operates applies to:

- The physical transfer of controlled Goods, Software and Technology;
- The transfer of Technology using electronic media, for example, e-mail, and the use of the internet of shared data environments (“Intangible Transfers”);
- The provision of Technical Services associated with defence programmes and services or equipment associated with Weapons of Mass Destruction (WMD); and
- Transfers of US controlled Goods, Software or Technology to ‘approved’ foreign nationals or other legal entities wherever that transfer may occur.

Resource Commitment
To achieve compliance with applicable laws Filtronic:

- Provides adequate systems and resources to manage export control awareness and compliance in the UK and in the USA to support compliance activity in the operational business(es);

- Allow access to specialist consultants and resources at the request of the Export Control Compliance Officer to complement compliance activity globally and develop and provide access to training relating to the relevant controls applicable to the business globally;
- Incorporates Export Controls and Sanctions awareness into other business procedures, including but not limited to the Filtronic Quality Management System, to ensure that compliance is an integrated function of the business.

The Export Control Compliance Officer has put in place a framework for managing Export Control Compliance (see UK and US Procedures). Within Filtronic, export controls compliance is overseen by the Senior Management Team and the Directors of the relevant exporting company.

The individual appointed as the Export Control Compliance Officer is set out in the Filtronic plc Distribution of Authorities document issued from time to time.

Implementation and Procedures

- The UK Export Control Compliance Procedure and the US Export Control Compliance Procedure are included with the company internal quality management procedures.
- Both the UK Export Control Compliance Procedure and the US Export Control Compliance Procedure can be found in the Company Communications/Documents & Policies section of Sage People. The Quality Manager shall retain the master copies of both procedures and shall be responsible for maintaining version control as well as publishing the correct version of each on Arena as well as Sage People. You can also obtain a copy of the procedures from the Quality Manager.

Additional Insurance Requirements relating to Export Control and Sanctioned territories.

There are additional steps required by Filtronic Insurers that should be complied with as set out in Step 1 and Step 2 of Annex 1 attached to this Policy.

Approved by the Board of Filtronic plc
May 2023

Annex 1 to Filtronic Export Control Policy

(Additional Insurance Requirement)

Stage 1 – Sanctions/Embargoes & Other Restrictions

As a term of its business arrangements with our insurance broker and our insurers, Filtronic plc (and subsidiary companies) has undertaken to notify IN ADVANCE (due to the lead time required to obtain terms, assuming cover is available) should Filtronic:

1. Do business in or need cover for any activities that touch upon or relate to sanctioned territories;
2. Need cover for individuals located in or travelling to or through sanctioned territories;
3. Need cover for entities or operations located or incorporated in sanctioned territories;
4. Have any connection with the government of any sanctioned territory;
5. Need cover which extends to subsidiaries / associated companies / partners / company operations or joint venture arrangements in any of the sanctioned territories; or
6. Require cover for goods that are subject to Export Control Legislation.

Current sanctions territory information can be found at:
https://www.gov.uk/guidance/current-arms-embargoes-and-other-restrictions
https://www.un.org/sc/suborg/en/sanctions/information
https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx

Stage 2 – Military / Dual Use

In addition to territories, the insurance broker also needs to be similarly advised details of proposed shipments of goods, including end customer information relating to the following:
When a shipment involves the export of (1) military goods, (2) dual use goods, or (3) Category A goods ("controlled goods") originating from and going to ANYWHERE in the world, additional sanctions clearance is required via the insurance broker / insurers.

The below lists are not exhaustive and if you have any doubts at all about the goods being exported you must inform the CFO who will inform the insurance broker.

	List
Military Goods	Military Goods are defined under Schedule 2 of the UK Export Control Order 2008 and include: Weapons, ammunition, explosives/explosive compounds explosive devices (bombs, torpedoes, rockets, missiles, cluster bombs, anti-personal mines) military vehicles, vessels and aircraft, riot control equipment, chemical or biological toxic agents or toxins, armoured or protective goods, electronic equipment, software, technology or any other good specifically designed for military use.
Dual Use	Dual Use Goods are defined in the Export Control Order as: Goods, software or technology, which can be used for both civil and military purposes including in the manufacture of nuclear weapons.

Category A Goods	Category A Goods are defined under Schedule 1 of the Export Control Order and include: Gallows, guillotines, electric chairs, air-tight vaults for the purpose of execution, automatic drug injection systems, leg irons/shackles, gang chains, restraint chairs, shackle boards, thumb screws, thumb cuffs, electronic shock belts, electronic shock batons, stun guns and spiked batons.

Filtronic plc

Closed Circuit Television ("CCTV") Policy

Policy statement

Filtronic (which includes Filtronic plc, and its UK trading subsidiaries, Filtronic Broadband limited and Filtronic Wireless Ltd., referred to collectively in this policy as "we") believes that CCTV and other surveillance systems have a legitimate role to play in helping to maintain a safe and secure environment for all our staff and visitors. Additionally, following a recent assessment by an independent assessor, it was recommended that installation of a CCTV system in Yeadon was deemed to be critical to protect the security of Filtronic' s business and buildings. However, we recognise that this may raise concerns about the effect on individuals and their privacy. This policy is intended to address such concerns. Images recorded by surveillance systems are personal data which must be processed in accordance with data protection laws. We are committed to complying with our legal obligations and ensuring that the legal rights of staff, relating to their personal data, are recognised and respected.

This policy is intended to assist staff in complying with their own legal obligations when working with personal data. In certain circumstances, misuse of information generated by CCTV or other surveillance systems could constitute a criminal offence.

Definitions
For the purposes of this policy, the following terms have the following meanings:

CCTV: means cameras designed to capture and record images of individuals and property.

Data: is information which is stored electronically, or in certain paper-based filing systems. In respect of CCTV, this generally means video images. It may also include static pictures such as printed screen shots.

Data subjects: means all living individuals about whom we hold personal information as a result of the operation of our CCTV.

Personal data: means data relating to a living individual who can be identified from that data (or other data in our possession). This will include video images of identifiable individuals.

Data controllers: are the people who, or organisations which, determine the manner in which any personal data is processed. They are responsible for establishing practices and policies to ensure compliance with the law. We are the data controller of all personal data used in our business for our own commercial purposes.

Data users: are those of our employees whose work involves processing personal data. This will include those whose duties are to operate CCTV cameras and other surveillance systems to record, monitor, store, retrieve and delete images. Data users must protect the data they handle in accordance with this policy [and our [Privacy Standard **OR** Data Protection Policy]].

Data processors: are any person or organisation that is not a data user (or other employee of a data controller) that processes data on our behalf and in accordance with our instructions (for example, a supplier which handles data on our behalf).

Processing: is any activity which involves the use of data. It includes obtaining, recording or holding data, or carrying out any operation on the data including organising, amending, retrieving, using, disclosing or destroying it. Processing also includes transferring personal data to third parties.

Surveillance systems: means any devices or systems designed to monitor or record images of individuals or information relating to individuals. The term includes CCTV systems as well as any technology that may be introduced in the future such as automatic number plate recognition (ANPR), body worn cameras, unmanned aerial systems and any other systems that capture information of identifiable individuals or information relating to identifiable individuals.

About this policy

We currently use CCTV on our premises in Sedgefield (in the strong room) and we use CCTV cameras within our demise and reception area at our Yeadon premises. There are other CCTV cameras around the Sedgefield site, but these are controlled by Durham County Council ("DCC") and subject to DCC's privacy policies. This policy outlines why Filtronic uses CCTV, how we will use CCTV and how we will process data recorded by CCTV cameras to ensure we are compliant with data protection law and best practice.

We recognise that information that we hold about individuals is subject to data protection legislation. The images of individuals recorded by CCTV cameras in the workplace are personal data and therefore subject to the legislation covering data protection, including the General Data Protection Regulation (GDPR).

This policy covers all employees, directors, officers, consultants, contractors, volunteers, interns, casual workers, zero hours workers and agency workers, and may also be relevant to visiting members of the public.

This policy is non-contractual and does not form part of the terms and conditions of any employment or other contract. We may amend this policy at any time. The policy will be regularly reviewed to ensure that it meets legal requirements.

Personnel responsible

The Filtronic plc Chief Executive Officer has overall responsibility for ensuring compliance with relevant legislation and the effective operation of this policy. Day-to-day management responsibility for deciding what information is recorded, how it will be used and to whom it may be disclosed has been delegated to the Filtronic IT Manager. Day-to-day operational responsibility for CCTV cameras and the storage of data recorded is the responsibility of the IT Department (delegated to the Data Controller in Yeadon and the Security Officer in Sedgefield).

Responsibility for keeping this policy up to date has been delegated to the Filtronic IT Manager supported by the Head of HR and General Counsel.

Reasons for the use of CCTV

We currently use CCTV as outlined below. We believe that such use is necessary for legitimate business purposes, including:

- to prevent crime and protect buildings and assets from damage, disruption, vandalism and other crime;
- for the personal safety of staff, visitors and other members of the public and to act as a

deterrent against crime;

- to support law enforcement bodies in the prevention, detection and prosecution of crime;
- to assist in day-to-day management, including ensuring the health and safety of staff and others;
- to assist in the effective resolution of disputes which arise in the course of disciplinary or grievance proceedings;
- to demonstrate compliance with minimal security requirements to carry out work of a sensitive nature for particular customers.

This list is not exhaustive and other purposes may be or become relevant.

Monitoring

CCTV monitors the exterior of the building and both the main entrance and secondary exits in Yeadon as well as inside the strong rooms in both Yeadon and Sedgefield. In addition, DCC monitors the exterior and points around the secure room at the Sedgefield site This data is continuously recorded 24 hours a day.

Camera locations are chosen to minimise viewing of spaces not relevant to the legitimate purpose of the monitoring. As far as practically possible, CCTV cameras will not focus on private homes, gardens or other areas of private property but the CCTV coverage might incorporate the car parks and other areas around the Filtronic property.

Surveillance systems will not be used to record sound.

Images are monitored by authorised personnel. This monitoring is undertaken when required, not as a standard function.

Staff using surveillance systems will be given appropriate training to ensure they understand and observe the legal requirements related to the processing of relevant data.

How we will operate any Filtronic CCTV

Where Filtronic's CCTV cameras are placed in the workplace, we will ensure that signs are displayed at the entrance of the surveillance zone to alert individuals that their image may be recorded. Such signs will contain details of the organisation operating the system, the purpose for using the surveillance system and who to contact for further information, where these things are not obvious to those being monitored.

We will ensure that live feeds from cameras and recorded images are only viewed by approved members of staff whose role requires them to have access to such data. This may include HR staff involved with disciplinary or grievance matters. Recorded images will only be viewed in designated, secure offices. Live and recorded images may be viewed remotely over the internet during and immediately following the activation of the intruder alarm system.

Use of data gathered by CCTV

In order to ensure that the rights of individuals recorded by the CCTV system are protected, we will ensure that data gathered from CCTV cameras is stored in a way that maintains its integrity and security. This may include encrypting the data, where it is possible to do so.

We may engage data processors to process data on our behalf. We will ensure reasonable contractual safeguards are in place to protect the security and integrity of the data.

Retention and erasure of data gathered by CCTV

Data recorded by the CCTV system will be stored digitally using an onsite server. Cloud computing will not be used. Data from CCTV cameras will not be retained indefinitely but in will be permanently deleted once there is no reason to retain the recorded information. Exactly how long images will be retained for will vary according to the purpose for which they are being recorded. For example, where images are being recorded for crime prevention purposes, data will be kept long enough only for incidents to come to light. In the normal course and in all other cases, recorded images will be kept for no longer than sixty (60) days. We will maintain a comprehensive log of when data is deleted.

At the end of their useful life, all images stored in whatever format will be erased permanently and securely. Any physical matter such as tapes or discs will be disposed of as confidential waste. Any still photographs and hard copy prints will be disposed of as confidential waste.

Use of additional surveillance systems

Prior to introducing any new surveillance system, including placing a new CCTV camera in any workplace location, we will carefully consider if they are appropriate by carrying out a privacy impact assessment (**PIA**).

A PIA is intended to assist us in deciding whether new surveillance cameras are necessary and proportionate in the circumstances and whether they should be used at all or whether any limitations should be placed on their use.

Any PIA will consider the nature of the problem that we are seeking to address at that time and whether the surveillance camera is likely to be an effective solution, or whether a better solution exists. In particular, we will consider the effect a surveillance camera will have on individuals and therefore whether its use is a proportionate response to the problem identified.

No surveillance cameras will be placed in areas where there is an expectation of privacy (for example, in changing rooms) unless, in very exceptional circumstances, it is judged by us to be necessary to deal with very serious concerns.

Covert monitoring

We will never engage in covert monitoring or surveillance (that is, where individuals are unaware that the monitoring or surveillance is taking place) unless, in highly exceptional circumstances, there are reasonable grounds to suspect that criminal activity or extremely serious malpractice is taking place and, after suitable consideration, we reasonably believe there is no less intrusive way to tackle the issue.

In the unlikely event that covert monitoring is considered to be justified, it will only be carried out

with the express authorisation of the Chief Executive OR General Counsel. The decision to carry out covert monitoring will be fully documented and will set out how the decision to use covert means was reached and by whom. The risk of intrusion on innocent workers will always be a primary consideration in reaching any such decision.

Only limited numbers of people will be involved in any covert monitoring.

Covert monitoring will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected illegal or unauthorised activity.

Ongoing review of CCTV use

We will ensure that the ongoing use of existing CCTV cameras in the workplace is reviewed periodically to ensure that their use remains necessary and appropriate, and that any surveillance system is continuing to address the needs that justified its introduction.

Requests for disclosure

No images from our CCTV cameras will be disclosed to any third party, without express permission being given by the Filtronic Chief Executive Officer. Data will not normally be released unless satisfactory evidence that it is required for legal proceedings or under a court order has been produced.

In other appropriate circumstances, we may allow law enforcement agencies to view or remove CCTV footage where this is required in the detection or prosecution of crime.

We will maintain a record of all disclosures of CCTV footage.

No images from CCTV will ever be posted online or disclosed to the media.

Subject access requests

Data subjects may make a request for disclosure of their personal information and this may include CCTV images (**data subject access request**). A data subject access request is subject to the statutory conditions from time to time in place and should be made in writing, in accordance with Filtronic's Data Protection Policy.

In order for us to locate relevant footage, any requests for copies of recorded CCTV images must include the date and time of the recording, the location where the footage was captured and, if necessary, information identifying the individual.

We reserve the right to obscure images of third parties when disclosing CCTV data as part of a subject access request, where we consider it necessary to do so.

Complaints

If any member of staff has questions about this policy or any concerns about our use of CCTV, then they should speak to their manager OR the Head of HR in the first instance.

Where this is not appropriate, or matters cannot be resolved informally, employees should use our formal grievance procedure.

Requests to prevent processing

We recognise that, in rare circumstances, individuals may have a legal right to object to processing and in certain circumstances to prevent automated decision making (see Articles 21 and 22 of the General Data Protection Regulation). For further information regarding this, please contact Filtronic's Head of HR.

Approved by the Board of Filtronic plc
May 2023

Filtronic plc

Business Travel Policy

Introduction

The Company recognises that business travel is an essential part of conducting its business activities but believes that only essential travel should be undertaken and that when it is, it is done so in compliance with a clear policy framework.

Underlying Principles of the Travel Policy

The approach underlying this travel policy is to:

- encourage travellers and their managers to comply with health and safety considerations;
- minimise the burden on the environment;
- provide a framework that is fit for purpose to support the business needs for travel and its associated activities in a cost-effective way;
- expect travellers to use their common sense to judge what is reasonable for their requirements and circumstances within the spirit of the policy guidelines.

Key Elements for the Travel Policy

Health and Safety

- Travellers shall take all reasonable care for the environment, health and safety of themselves and of other persons who may be affected by their acts or omissions.
- Travellers should ensure that relevant inoculations are current before travel.
- Travellers should make enquiries of the Travel Co-ordinator for their insurance arrangements for their proposed trip to ensure they are adequately covered and take out additional personal cover for personal effects if required;
- Travellers should carry the relevant up to date health insurance/assistance card when overseas (to be sourced from the HR Department). Employees should carry a report on any medical problems including sufficient personal medication for the duration of their trip/secondment as relevant drugs may not be available at their destination. Note that over the counter drugs available in some countries are either banned severely restricted in others. Anyone travelling with quantities of either prescription or OTC drugs should ensure that doing so will not violate the laws of the country they are visiting.
- An up to date inoculation record card should be carried.
- It is advised that all personnel carry a first aid kit with a stock of over-the-counter remedies to treat minor ailments such as light fever, toothache, nausea, stomach upset.
- Travellers should not undertake long car journeys following long-haul air flights. Tiredness can result in significant risk whilst driving.
- In addition to the above, if an infrequent traveller, it is advisable to consult with their own doctor before travel.

- Travellers should exercise prudence in visiting countries that may be considered risk related to personal security; the appropriate EHS manager or General Counsel may be consulted for further information.
- Travellers must take personal responsibility for lifestyle choices that may impact on their health and safety or the health and safety of others.

Environment

Travellers should aim to minimise the burden on the environment of business travel through considering and choosing the options available and their associated environmental impact.

Air Travel

- Economy for any flight leg less than 10 hours long.
- Premium economy (or business class when not available or broadly equivalent in cost (or efficient equivalent travel fare)) when the individual flight leg is more than 10 hours long.
- Executive Director authority required to permit business class or premium economy when an individual flight leg is under 10 hours long (e.g. whilst being an overnight flight), depending on business needs.
- Business class permitted when no more expensive than the Economy fare (or Premium Economy where relevant) (i.e. when paired with a return leg in Business, or as part of a multi-leg trip).
- Lowest cost routes and carriers to be selected, regardless of Loyalty Programmes.

Train Travel

- Standard class, although First may be permitted with Executive Director approval
- Advance purchase and saver tickets to be used when adequate certainty on travel times.
- Day of departure tickets to be purchased directly at the station

Hotel Accommodation

- The preferred hotels, selected in each of the main locations, are to be used and use should be made of a general arrangement outside this with a major hotel group, once this is in place. Individuals using a hotel outside of these arrangements are to ensure that it is a lower price than the preferred/centrally available arrangements, and to provide this evidence when submitting expenses for approval
- Hotel charges to be paid by credit card, not re-invoiced to Filtronic. Where necessary (i.e. if a traveller does not possess a credit card) an advance (or prepayment) may be arranged from the Accounts Department.
- Hotel accommodation will usually be guaranteed, so the traveller is expected to cancel unwanted accommodation by the deadlines indicated in their reservation
- Please refer to the Travel Coordinator for the list of main location hotel arrangements and maximum expected room rates for the location/area

Car Hire

- The Company's global Car Hire arrangement provider must be used with a maximum rental category of compact cars outside of North America and mid-sized sedan inside North America
- Car hire should be booked through the travel agent, when appointed
- Hire cars to be refuelled by the user before return, when required

Ground Transportation

- Locally provided driver services should be used when the traveller is unfamiliar with driving in the country being visited (e.g. China, India).
- Travellers should use airport transfer buses for airport hotels and consider using other transfer services for transfers to city centres before use of taxis.

Communications

- When travelling, staff should look to minimise mobile phone roaming costs by, for example:
  - arranging to be rung back on fixed lines in hotels or offices;
  - using a local SIM card/mobile number to the destination (in the UK available from the Travel coordinators);
  - using dial through on central switchboards;
  - once arranged, through the use of a prepaid calling card.
- Similarly, for data connections, staff should look for cost-effective routes for connecting laptops including:
  - use of a local SIM data card
  - register for web access email if email access mainly expected from the office environment

Travelling Time

Any travelling which is undertaken outside normal working hours should be agreed in advance with the Authorising Manager. Compensation for travelling outside of normal working hours will not be allowed unless approved in advance by an Executive Director on a "needs-must" case-by-case basis.

Authorisation

- Authorisation will be as per the current PAM or below where not specifically covered in that document
- The authorisation procedure set out below is for air and longer distance train/car travel including overnight stays. It does not apply for local travel, for which reimbursement should be made through the reimbursement of expenses
- Travel forms to be signed off by the Business Unit managing director/director,
- Urgent or out of hours new bookings require usual level of sign off or upward delegation if usual approval authority is not available and may be confirmed to the travel agent electronically.
- Amendments during travel time to be approved retrospectively by original approval authority if costs increase by more than 10%.

- Business Managers and other Executive Directors requests to be signed off by the CEOor the Chairman in periods where there is no CEO.
- Other Board members' requirements to be signed off by Chairman or any other person authorised by the Chairman or CEO.
- Travel orders to Appointed regional travel agent to be carried out through current system of nominated administrators (Travel coordinators).
- Exceptions to policy implementation, requires prior Business Manager or CEO approval.
- Travellers who are required to have security clearance before making their trips are to ensure that this is secured in good time before booking travel arrangements.

Ticketing

- E-ticketing, and electronic copies of hotel reservations etc. will be used as much as possible

Monitoring

- Finance Team to provide a detailed monthly travel report to relevant Business Managers and the CFO

Approved by the Board of Filtronic plc
May 2023

Filtronic plc

Whistleblowing Policy

Filtronic plc ("the Company") together with its subsidiary companies (herein "Filtronic") believe it is important that any criminal behaviour or other wrongdoing by an employee or worker (in whatever position) undertaking work with any company in the group is reported and properly dealt with. Filtronic is committed to ensuring that no member of staff should fear disadvantage from raising legitimate concerns.

This policy (and the procedure below) applies to all employees, former employees, contractors, subcontractors or agents of Filtronic plc and its subsidiaries ('Workers').

The purpose of this procedure is to provide a framework to promote responsible whistleblowing. Whistleblowing is the reporting by workers of any malpractice or illegal act or omission by other workers.

Filtronic has established by this procedure a channel for communication of concerns that is independent, so far as is practicable, from the management of the Company.

Relationship of this Procedure to the Company's other Policies and Procedures

Filtronic's policies and procedures on grievance, discipline, harassment, etc. should be used in most situations. The use of this procedure should be restricted to where you reasonably believe one of the following has occurred, is occurring, or is likely to occur:

- A criminal offence, including fraud, bribery or corruption;
- Disregard for legislation, particularly in relation to health and safety at work;
- Malpractice, or ill treatment of a customer by a member of staff;
- Damage to the environment;
- Any other serious irregularity; or
- Deliberate concealment of any of the above
- Any matter of sufficient seriousness that cannot reasonably be addressed using Filtronic's grievance, discipline and harassment policies and procedures.

Whistleblowing should not be used in place of Filtronic's grievance procedures or be a route for raising malicious or unfounded allegations. Only those who use this policy in good faith will be protected under it (see below).

The Designated Officers

The following persons are the Designated Officers under this procedure.

Pete Magowan
Non-Executive Director

Email: pete.magowan@filtronic.com
Address: 85 Impington Lane
Impington, Cambridge,
CB24 9NJ

John Behrendt
Non-Executive Director

Email: john.behrendt@filtonic.com
Address: 1 The Old Flour Mills, Mills Road, Buckden, Cambridgeshire, PE19

Raising a Concern – The Line Manager Route

You should normally raise concerns about wrongdoing and malpractice with your immediate manager first, who will notify the matter to one of the Designated Officers.

Raising a Concern – The Designated Officer Route

If the matter is of a very serious nature, such as an allegation of fraud involving a Filtronic plc director, or if it involves your immediate manager, you may notify one of the Designated Officers directly. You must include the words 'Whistleblowing' in the subject heading of the email or letter you send.

The Investigative Stages

The Designated Officer will, if requested, arrange an initial interview. At this stage, you will be asked whether you wish your identity to be disclosed (You may not make anonymous complaints to the Designated Officer but your identity may remain confidential to the Designated Officer, as far as is reasonably practicable). You will also be asked whether or not you wish to make a written or oral statement. In either case, the Designated Officer will write a brief summary of the interview, which will be agreed by both parties.

The Designated Officer will report to both the Chairman of Filtronic plc and the other Designated Officers to the extent appropriate, having regard to the subject matter.

The Designated Officers and the Chairman (to the extent appropriate, having regard to the subject matter), will together decide on what further investigation, if any, should take place. They will report back to you within 10 working days of your interview or receipt of your complaint, whichever is the later.

Where, exceptionally, the complaint is about the Chairman of Filtronic plc, the Designated Officers will decide on how to proceed. This may include an external investigation. Again, you will be informed of progress within 10 working days.

The Investigation

It may be necessary that certain investigations will be carried out in strict confidence (with the employee under investigation not being informed until necessary). In certain other circumstances, the employee may have to be suspended pending the investigation.

If the investigation shows there is a case to answer, the Company's Disciplinary Procedure will be invoked against the employee concerned.

If there is found to be no case to answer, the Designated Officer will ensure that you are protected, provided the disclosure was made in good faith. Only where you are found to have made false allegations maliciously will the Disciplinary Procedure be invoked against you.

Inquiries

If the concern raised is very serious or complex, an inquiry may be held.

Following the Investigation

The Designated Officer, possibly in conjunction with the Chairman, will arrange a meeting with you to give feedback on the investigation (This will not include details of any disciplinary action, which will remain confidential to the individual concerned). The feedback will be provided within 10 working days of the conclusion of the investigation and any inquiry.

If you are not satisfied with the outcome of the investigation, Filtronic recognises your right to make disclosures to prescribed regulators, or, where justified, elsewhere.

The Law

This procedure has been written to take account of the UK's Employment Rights Act (Part IVA Whistleblowing Provisions) 1996 that protects workers making good faith disclosures about certain matters of concern.

Protection of Whistleblowers

Filtronic will not tolerate any harassment, victimisation or discrimination of a good faith whistleblower and will treat this as a serious disciplinary offence. The whistleblower's rights against retaliation are fully recognised by Filtronic.

Approved by the Board of Filtronic plc
May 2023

Filtronic plc

Business Continuity Policy

Policy Statement

This policy establishes the guidelines for business continuity at Filtronic plc ("the Company") together with its subsidiary companies ("Filtronic") to effectively detect, respond and manage a business disruption in order to maintain manufacturing and engineering operations at a level where we can continue to operate or recover the operation as quickly as possible.

Filtronic makes every effort to ensure it is protected against any risks or threats that could have a material impact upon, disrupt or interrupt its operations. The Group's business continuity plans provide a framework for improving its resilience to business interruption so that key business systems and processes can be recovered whilst at the same time limiting stoppage of business-critical activities.

Scope

The scope of this policy covers business-critical activities important to the manufacturing and engineering operations in Filtronic as well as its key IT systems. It is supported by a detailed business continuity plan which contains procedures to mitigate and respond to dependent on the business interruption.

Objectives

The objectives of this policy are:

- To improve the resilience of business-critical activities within Filtronic, by identifying and managing the operational risks inherent in the activity;
- To ensure the safety and welfare of employees;
- To minimise the effects of disruption to the business;
- To ensure employees are fully aware of the processes and technical controls needed to make sure Filtronic can continue to deliver core services, important to its manufacturing and engineering operations, in the event of a business disruption;
- To ensure stakeholders are fully aware of the importance we place on business continuity as well as the implications and consequences, both personally and to the Company, of not adhering to this policy; and
- To commit to regular reviews of the business continuity policy and plan to ensure they reflect the operational needs of the business and remain appropriate.

Roles & Responsibilities

The overall responsibility for the business continuity plan in Filtronic is the Chief Executive Officer ("CEO") with delegated authority to the Chief Financial Officer ("CFO") when appropriate. The CEO will determine the situations when the business continuity plan is invoked and ensure the business continuity team ("BCT") is established as quickly as possible.

To support the CEO the Group has established clearly defined roles and responsibilities within the BCT to manage the response to any incident. This team is clearly identified within the business continuity procedures and its makeup is defined by the nature of the situation. They have been selected based on their in-depth knowledge relating to the business-critical activities within the department impacted.

Policy Content

1.1 Risk Assessment Process

In order to identify a business priority rating of services required to maintain manufacturing and engineering operations, a risk assessment exercise known as a business impact analysis is conducted by using an agreed set of metrics which provides an overall score of the potential impact. The impact assessment criteria is based upon, but not limited to the following business impacts:

Impact	Rating	
Insignificant	1	No/insignificant loss of availability or business impact
Minor	2	Minor business impact with manual work workaround requiring little effort
Moderate	3	Major business impact with manual work workaround requiring little effort
Major	4	Major business impact with manual work workaround requiring significant effort
Catastrophic	5	Major business impact with no acceptable workaround

To determine the most likely scenarios, each business service is reviewed to determine the likelihood of a potential business disruption. This process will consider controls used to reduce the likelihood of an interruption occurring and the potential for it disrupting the availability of the service.

The risk assessment process identifies potential areas of improvement in controls to protect the service and reduce the likelihood of a disruption occurring which the service owner shall use to create an improvement action plan.

1.2 Scenarios and Triggers

Notification of a disaster will likely originate via the Filtronic incident management process because of a notification from one of the following:

- Internal member of staff
- Third party (e.g. service provider)
- Monitoring / detection tools

- Security Incident Management process

An incident can become a business continuity incident should it meet the following criteria:

- An incident relating to a key manufacturing or engineering service which is unlikely to be contained and/or managed by the service owner within a tolerated time period (four hours)
- A Filtronic Executive Director has declared a major incident following confirmation of one of the following incidents:

Incident	Potential disasters
Loss of manufacturing site	Man-made – fire, vandalism or act of terrorism Natural – fire, flood or storm
Loss of a site utility	Man-made – fire, vandalism or act of terrorism Natural – fire, flood or storm Power, water or compressed air outage
Loss of manufacturing components / inventory	Man-made – fire, vandalism or act of terrorism Natural – fire, flood or storm
Loss of manufacturing equipment / device	Man-made – fire, vandalism or act of terrorism Natural – fire, flood or storm Hardware failure
Loss of manufacturing software / system	Man-made – fire, vandalism or act of terrorism Natural – fire, flood or storm Power outage Network equipment failure Server hosting platform failure Software / database corruption Cyber attack (ransomware)

1.3 Communication Strategy

In the event of a business disruption occurring, it is vital that all internal Filtronic stakeholders, including the Filtronic plc board of directors, are kept up to date and informed, not only to ensure that recovery procedures are activated, and regulatory requirements are maintained, but to ensure that external stakeholders such as customers are aware, should there be a level of disruption.

The Filtronic Business Continuity Team will decide on the most effective communication method suitable for the business disruption to ensure the Communication Coordinator clearly communicates to all stakeholders. All communications (internal and external) must be authorised by an Executive Director. External communication regarding any business disruption must only be issued by an Executive Director although an Executive Director may delegate the task. Under no circumstances should any press releases or other communications be issued externally without the approval by an Executive Director.

1.4 Testing & Exercising

In order to validate the effectiveness of this policy and the associated Business Continuity Framework, Filtronic shall perform a business disruption rehearsal exercise at least annually.

These exercises will be tailored to present credible challenges (i.e loss of IT Systems, loss of Office/Infrastructure, or both) to the participants and provide all with an opportunity to review and discuss current continuity arrangements.

In addition to this, the technical disaster recovery procedures shall be tested at least annually through a full interruption test to validate that any automatic and manual disaster recovery procedures work as expected.

1.5 Training & Awareness

It is important that the Business Continuity Team members receive regular awareness training to ensure that they are aware of their role and associated responsibilities. As a minimum, the Business Continuity Team will receive a refresher of their role and responsibilities as part of the annual test rehearsal. Any further training shall be raised as an output of the rehearsal to ensure the team have the necessary skills to effective respond to a business disruption.

1.6 Continual Improvement

The output of any rehearsal shall include the identification of any areas for improvement which shall feed into the continual improvement of the business continuity management system.

Evaluating the Effectiveness of Business Continuity

The CEO is the person responsible for ensuring that stakeholders observe the requirements set out within this policy.

Filtronic may monitor the performance in the delivery of the objectives of this policy by reporting to Filtronic's Leadership Team on a range of measures including:

- The results of regular internal or external audits used to identify areas of non-conformance to this policy and to identify potential opportunities for improvement.
- The results of business continuity testing and exercise rehearsals used to identify areas of non-conformance to this policy and to identify potential opportunities for improvement.
- The statistics obtained from review which may follow the delivery of cyber security awareness training to ascertain the application and effectiveness of this policy.

The output of any performance review shall include the identification of any areas for improvement which shall feed into the continual improvement of the business continuity management system.

Approved by the Board of Filtronic plc
May 2023