FILTRONIC PLC

GROUP POLICIES – 2019

www.filtronic.com

Contents

Filtronic plc
Health and Safety Policy

Filtronic plc ("the Company") acknowledges its responsibility to provide, so far as is reasonably practicable, working environments which do not impair the health or jeopardise the safety of its employees, customers, contractors or the general public. The Company is committed to compliance with health and safety legislation and other relevant requirements.

The Company considers that the operation of a health and safety management system in establishing and supporting an active health and safety culture is a high priority in its operations. The Management of each Business Unit within the Filtronic Group shall ensure that relevant local legislative requirements are addressed and shall brief, train and monitor compliance with this Policy. Each Business Unit shall generate procedures that reflect this policy and the legal requirements of the territories within which they operate.

Company employees have a vital role in both the implementation and the operation of the Health and Safety Management System, in particular:

- Each operational site shall ensure that all matters relating to health and safety are effectively communicated to all employees, contractors and visitors.
- Safe practices shall be employed in the installation, operation and maintenance of equipment and facilities.
- Safe practices shall be employed in the transport, handling, storage, use and disposal of potentially dangerous articles and substances.
- Employees shall be selected for tasks with consideration for their physical and mental suitability for safe performance.
- Training programmes for employees shall be prepared and implemented on safe working, occupational risks and on the identification and elimination of potential hazards.
- Accidents, dangerous occurrences and occupational diseases shall be minimised through a continuous program of assessment and improvement.
- All employees shall act responsibly on all matters affecting the health and safety of themselves, fellow employees and visitors to the Company including contractors working on Company premises.
- All visitors to the Company and contractors working on Company premises shall be accounted for and made aware of workplace risks, if visitors are on site they must be adequately supervised at all times.

This Policy will be reviewed regularly and updated as necessary. This policy is available to interested parties upon request.

Rob Smith
Chief Executive Officer
Filtronic plc
21 June 2017

Filtronic plc
Environmental Policy

Filtronic plc, its subsidiaries and their business units, are strategically committed to being a world leader in the design and manufacture of RF & Microwave products and services whilst protecting the environment. Filtronic will operate in compliance with all relevant statutory and regulatory obligations through the adoption of environmental best practices throughout its activities.

The effectiveness of our Environmental Management systems is maintained through a process of monitoring and continual improvement versus 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.

Rob Smith
Chief Executive Officer
Filtronic plc
21 June 2017

Filtronic plc
Intellectual Property Rights (IPR) Policy

Policy Statement

Filtronic plc ("the Company") together with its subsidiary companies (herein "Filtronic") 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

Each business division shall seek to protect existing businesses, to increase market share and to develop new profitable businesses 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 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.

Filtronic plc Board of Directors shall approve assignment or licensing of a substantial interest in the IPR of any business divisions *(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.)*

Each business division in consultation with Filtronic plc shall be responsible for:

- Defining the IPR strategy of their operation within the framework of this Policy.
- Identifying a person for promoting IPR awareness and co-coordinating IPR activities.
- Compiling a Business Specific database of the IPR it owns and inputting required data onto a central IPR database.
- Monitoring third party IPR and competitors' products to identify possible infringements.
- Establishing an adequate mechanism for securing evidence of date and origin of invention or design.
- Ensuring 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 is in place.

Rob Smith
Chief Executive Officer
Filtronic plc
21 June 2017

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 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 and the need to act fairly between members.

The Management of each Business Unit 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 following guidelines (Code of Ethics):

- **Code of Ethics:**
  - **Legal Compliance:** The Company shall aim to comply with all applicable laws and regulations and requires that all its employees conduct its business in accordance with the law.
  - **Good Stewardship:** All employees shall handle the property and information of the Company, its Customers and Suppliers with due care, in particular:
  - **Company Information** should be treated as confidential; included in this are technical or financial data, company policies, procedures, letters, plans, drawings and computer programs, product developments, price and cost data and personal data.
  - **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** should be prepared accurately and honestly.
  - **Company Funds**. Every employee who has control over Company funds is accountable for such funds and must ensure they are legitimate and justifiable.
  - **Procurement Ethics.** Business shall be awarded solely on the merits of the offered product or service; employees should not engage in any activity or allow any relationships to impair their judgment. *(Please see separate policy on Anti-Bribery and Corruption).*
  - **No Gifts, Gratuities or Favours** of significant value shall be given/accepted by employees to/from Customers or Suppliers except where they are publicly presented for noteworthy service or when explicitly authorised by Filtronic's Board of Directors. *(Please see separate policy on Anti-Bribery and Corruption)*.

- **Consultative Management:**
  The process of Planning, Risk assessment, Progressing, Reviewing and reporting is applicable at all levels. The Business units shall 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.

- **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.

- **Communication:**
  Operational performance and progress against strategic targets shall be communicated regularly throughout each Business unit.

- **Quality:**
  The Company shall provide products and services of a quality to fully satisfy the requirements of our Customers as well as achieving the Company's business objectives.

- **Customer Code:**
  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.

- **Financial Controls:**
  The provisions of the financial Procedures and Authorisations Manual ("PAM")/Authorisation Limits shall be adhered to by all Business units.

- **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.

- **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:
  - **Breach of the Code of Ethics:**
    Any breach which could adversely affect the Company's legal or ethical standing should be promptly reported.
  - **Significant Customer Complaints and Product Liability Claims:**
    Customer Complaints should be answered speedily, courteously and truthfully. Each Business unit should 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.
  - **Terms of Trade:**
    Any request to trade with the company on terms other than Filtronic plc's standard conditions, within authorised limits, should be forwarded to the Legal Department. All responses to such requests and the acceptance, acknowledgement or processing of relevant Orders or Contracts shall only be with the express authority of the Legal Department. The initial recipient of the request, or an appointee, shall be responsible for keeping the requestor advised of the progress of the enquiry.

- **Whistleblowers:**
  (Please see separate policy on Whistleblowing Policy and Procedure).

Each Business Unit Manager is responsible for the communication of the Filtronic plc PAM (and any updates thereof) to all relevant employees within that Business Unit.

The Business Unit managers are responsible for ensuring that the Management Policy is adhered to throughout their organisation.

Each Business Unit shall generate procedures, based upon the above Policy and shall ensure those procedures are accessible to all its employees.

Rob Smith
Chief Executive Officer
Filtronic plc
21 June 2017

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 wrong doing 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 feel at a disadvantage in 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 senior 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. They have direct access to the Chairman of Filtronic plc.

Michael Roller *Senior Non-executive Director*	Email: michaelroller@hotmail.com The Red House Wilsford-cum-Lake, Salisbury SP4 7BL
Maura Moynihan *Company Secretary and General Counsel*	Email: maura.moynihan@filtronic.com Tel: 01274 535 619

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 direct. 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 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, and the Designated Officers and the Chairman 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.

Each Business Unit shall incorporate this Procedure into its Staff Handbook.

Rob Smith
Chief Executive Officer
Filtronic plc
21 June 2017

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.

Each Business Unit shall instruct Human Resources staff specifically to ensure that relevant local legislative requirements are addressed and to brief, train and monitor compliance to these Policies.

Each Business Unit shall generate procedures, based upon the above and reflecting the legal requirements of the territories within which they operate, and shall make those procedures accessible to all its employees.

Rob Smith
Chief Executive Officer
Filtronic plc
21 June 2017

Filtronic plc
Business Travel Policy

Contents

Introduction

This note sets out the main points to bring the policy in line with current industry practice, in effect confirming the main points of the existing travel policy. It also acts as a reminder that the policy is to be followed and to assist the monitoring groups to achieve this. This clarification will assist senior management to give support as necessary to cover non-adherence to the policy.

Underlying Principles of the Travel Policy

The approach underlying this travel policy is to:

- 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 guidelines
- encourage travellers and their managers to comply with health and safety considerations
- minimise the burden on the environment.

Summary of Key Elements for the Travel Policy

Air Travel
- Economy within local continent e.g. Europe for UK based staff
- 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
- Management discretion to permit business class when an individual flight leg is under 10 hours long 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)
- Travel to be on preferred airline partners, where established regionally.

Train Travel
- Standard class, although First may be permitted when appropriate
- 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 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 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
- Continuation of current arrangements within a maximum rental category of compact cars outside of North America and mid-sized sedan for 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.
- Use of private cars is set out in the car policy.

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. When weekend travel is involved, any time off in lieu should also be authorised by the Manager.

Time Off in Lieu

Any weekend work or travel will be classed as straight time off in lieu on return to work, i.e., a day off for the day spent travelling if not a working day (weekend days, which involve neither work nor travel, will not warrant time off in lieu). The time off in lieu must be taken on first day/s due back to work or as agreed with the Departmental Manager. There will not be monetary payments for this. Regardless of overtime premiums within normal employment contracts, time in lieu will be on a day for day basis. However, for Management and Executive staff, any time off in lieu for travel shall be agreed on a case by case basis with that individual's immediate Supervisor/Report.

Authorisation

- Authorisation will be as per the current distribution of authority 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 local company MD, with long haul travel notified to Business Managers.
- Urgent or out of hours new bookings require usual level of sign off or upward delegation of usual approval authority 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 CEO.
- Other Board members' requirements to be signed off by 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, including the use of non-preferred airline, requires prior Business Managers or CEO approval.
- Travellers requiring to have security clearance before making their trips are to ensure that this is secured from their security clearance officer.

Ticketing

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

Monitoring

- Contracts group (or equivalent group outside the UK) to provide details of exceptions to policy as they arise to Business Managers and Group Finance Director
- Contracts group to provide a monthly summary of major spends with preferred and non-preferred airlines by routeing/geography and equivalent arrangements outside the UK

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 inoculations are current before travel.
- Travellers should make enquiries of the Travel Co-ordinator for their insurance arrangements for the 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. An up to date inoculation record card should also 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.

Rob Smith
Chief Executive Officer
Filtronic plc
21 June 2017

Contents

1. Policy Statement

Filtronic plc, (including its subsidiary companies and business units) 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.

The Management of each Business Unit within the Filtronic Group shall ensure that relevant local legislative requirements are addressed and shall brief, train their employees on the existence and content of this Policy and shall and monitor compliance. Each Business Unit shall adapt this Policy where necessary to reflect the legal requirements of the territories within which they operate.

2. IT Policy Implementation

This section explains:

- how you may use email, telephones and the Internet using the Company's facilities;
- how you or the Company may be liable in law for misuse of email or the Internet;
- how your interests and the Company's interests can be protected; and
- the disciplinary action that may be taken against you if you fail to comply with the rules set out in this policy.

You must read this policy and apply it to your everyday work. If you have any questions as to the meaning or effect of this policy, you should contact your manager or a member of the HR or IT Departments.

This policy is not however a definitive statement of the purposes for which the Company's facilities must not be used. You must conduct yourself, at all times, in a trustworthy and appropriate manner so as not to discredit or harm the Company or its staff and in accordance with the spirit of this policy statement.

This policy applies to all telephone and computer users within the Company (including, without limit, all Directors, employees and third parties) who use email, bulletin boards, intranet, the worldwide web and the Internet through computers based at the Company's premises or through any computers located at other sites (including private 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.

Failure or refusal to comply with this policy is a disciplinary offence that may lead to disciplinary action, up to and including, dismissal without notice. For further details, please refer to the Company's Disciplinary Procedure.

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.

2.1 Telephone Use

Personal calls should not usually be made or received except in an emergency, when permission to make or take the call should be first obtained from your Line Manager. If a public payphone is not provided on Company premises for employees' private use the telephone at reception may be used. Calls to and from telephones will not be monitored. Private calls should be made during lunch and rest breaks where possible.

2.2 Email and Internet - Authorised Use

The Company encourages staff to use email as a prompt and effective method of communication. It will not always be appropriate to communicate by email and you should always consider whether there is a more suitable method (for example in circumstances where there is a need to preserve confidentiality or in the case of sensitive issues which should be communicated face to face).

Your use of email and the Internet is only authorised for bona fide purposes directly connected with your work or the Company's business. 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 as private or personal. As detailed below, the Company reserves the right to access such communications and information.

You 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. Remember that email sent via the Company's system may be legally regarded as bearing the Company letterhead and, should therefore, be treated the same way.

You may only set passwords and security codes for your computer, the system or any part of it or documentation held on it in accordance with Company policy from time to time. The use of someone else's identity and password to access the Internet or send email is strictly forbidden and will result in disciplinary action.

Internet access is provided for business purposes. You will need to be familiar with the type of information that the Company deems to be sensitive or secret and you must ensure that this is not made available to the public via the Company's email system. Employees who routinely work from home must use a Company supplied laptop computer or have a dedicated workstation supplied by the Company. Any other employees that need to use a home computer for work purposes on an occasional basis should only do so with the express permission of their line manager and must ensure they take all reasonable measures (which would involve liaising with the Company's IT department) to protect and maintain the integrity and confidentiality all Company information in doing so. Employees working offsite must use a Company provided e-mail system for Company business, and not a private or public e-mail account such as Hotmail, Yahoo, etc.

The amount of time spent browsing should be kept to a minimum by using search engines to locate what you are looking for.

Do not subscribe to any bulletin boards, newsgroups or any other Internet services or download software without the prior written permission of the IT Systems Manager who may seek approval of Senior Management (if appropriate).

Incidental personal use of the Internet and the Company's email may be permitted but should be kept to a minimum and extended use for personal or non-company business, use for the operation of a personal business or activity intended to achieve personal financial gain, or use that could bring the Company's name into disrepute or be commercially damaging to the Company, is inappropriate and unacceptable.

You must not deliberately visit, view or download any of the following material and you are strictly prohibited from sending any material, whether downloaded from the Internet or otherwise which contains or refers to 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.

You are also 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 "delegate" arrangements, which retain individual accountability.

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

Unauthorised use of email and/or the Internet may expose both you personally and/or the Company to Court proceedings attracting both criminal and civil liability. You 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 your unauthorised use of email and/or the Internet.

2.3 Software

The Company licenses computer software from a variety of outside sources. The Company does not own this software or related documentation and, unless authorised by the software developer, does not have the right to reproduce it. The software used on the local area network or multiple/individual machines should have the appropriate licence(s).

You should notify your departmental manager or the IT Department of any misuse of software or associated documentation.

The use of software packages other than those licensed by the Company requires the approval of the IT department and the purchase of appropriate licences. Installation of software and modification of PC's must be performed by a member of the IT department, unless otherwise authorised by IT, your departmental manager or 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.

2.4 Third Parties

Do not give information to third parties unless authorised to do so and do not disclose security information or other details relating to the Company's computing resources, data, information or processes unless it is necessary for the third party to fulfil its role and the third party has entered into a confidentiality agreement. Any contract entered into by the Company that contracts a third party for services (e.g. contractors, partners, customers) should contain clear and comprehensive security conditions in respect of the access by the third party to 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.

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

2.5 Security and Viruses

The accessibility of the Internet is both an advantage and disadvantage of the system. Whilst you can access a huge amount of information via the Internet, information and emails sent across the Internet may be read by persons unknown to the sender. Potentially anyone could read private and confidential information transmitted on the Internet. Even if some information has been deleted from your screen it may not necessarily be deleted from the Internet system which provides backup saving mechanisms. Any message or information requiring security or confidentiality should be distributed by an alternative means of communication.

It is your responsibility to log off from email or close down active sessions when away from the office or from your computer to avoid inadvertent security breaches. You should update your security password regularly, not store it with your workstation and not disclose this detail unless your job requires it. You must not forward to third parties emails that contain information which is confidential or commercially sensitive and should not include anything sensitive or private in email messages

unless protected with approved encryption software, which can be obtained from the IT department. Also, be aware that email messages may be forwarded, distributed or read by others without your knowledge.

You must not send via or put on the Internet any material, 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. Accordingly, employees must not exchange executable programs using Internet email and must discard any documents or attachments which employees receive unsolicited. You must not introduce new software onto the Company's system without written authorisation from the IT department and you must always ensure that the appropriate virus checking procedures have been followed. If in doubt, take all floppy disks, CD-ROMs or other media originating from external sources to the IT department for virus scanning before inserting into your PC.

Sensitive documents should not be saved to public file shares and you should also physically protect floppy disks, laptops etc. by e.g., locking them up when leaving them unattended and protect sensitive information on documents by, e.g., disposing of sensitive documents in a secure manner.

2.6 Intellectual Property

The Company's intellectual property represents one of its most valuable assets. 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, which may be accessed by unauthorised individuals.

Further, 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. You should not, therefore, make careless publications on the Internet or send careless unencrypted emails that might lead someone to deduce the Company's ideas.

2.7 Courtesy

As emails can easily be misconstrued, you must therefore, consider very carefully whether email is the appropriate form of communication in particular circumstances. If you decide that it is, you should carefully consider the content of all emails and who the appropriate recipients should be. It is inappropriate to send emails and/or attachments to people (whether they are other employees of the Company or third parties) if the email does not relate to them or if the attachment should not be read by them. Pay particular attention to style and content of all emails when sending emails externally, treating them in the same way as letters on the Company's headed notepaper.

2.8 Defamation

Emails and the Internet are considered to be a form of publication and therefore the use of the Internet and email may result in communication constituting a libel contrary to the provisions of the Defamation Act. Both words and pictures produced on the Internet are capable of being libellous if they are untrue, ridicule a person and as a result damage that person's reputation. For these purposes, as well as any individuals, a "person" may include the Company or another company. You must not put any defamatory statement onto the Internet or on the Company's computer system whether in emails or otherwise. As well as you being personally exposed to potential legal action for defamation, the Company can also be exposed both for the actions of you as its employee and also as an on-line provider.

2.9 Obscenity

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. The accessing or sending of obscene or indecent material using the Company's system is strictly forbidden.

2.10 Discrimination and Harassment

The Company does not tolerate discrimination or harassment in any form whatsoever. This principle extends to any information distributed on the Company's system or via the Internet. You may not put on either system any material which discriminates or encourages discrimination or harassment on racial or ethnic grounds or on grounds of gender, sexual orientation, marital status, age, ethnic origin, colour, nationality, race, religion, belief or disability. Please also bear in mind the Company's policy on discrimination and harassment.

Breaches of this policy will lead to disciplinary action. In the event you receive or become aware of obscene, indecent, offensive, inflammatory, discriminatory or socially offensive material you should notify your manager immediately so that appropriate action may be taken.

2.11 Data Protection

Only designated employees within the HR and IT departments may place staff information (including photographs) onto the Company's system. In all cases, the individual to whom the personal data relates should have been made aware that this information would be placed on the system. Photographs should not be placed on the system without an individual's consent. If you are in any doubt you should check with a member of the HR Department/your Manager.

2.12 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
- to check voice mail systems when you are on holiday or on sick leave.

The Company also logs all Internet activity and reserves the right to 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.

Rob Smith
Chief Executive Officer
Filtronic plc
21 June 2017

Filtronic plc
Anti-Bribery and Corruption Policy

1 Definition

This Policy should be read as an adjunct to the Company's Management Policy and Code of Ethics. For the purpose of this policy, bribery and corruption is defined as giving someone a financial or another advantage to encourage that person to perform their functions or activities improperly or to reward them for having already done so.

2 Filtronic's Stance on Bribery and Corruption

Filtronic will not engage in bribery or corruption.
This policy applies to all employees of Filtronic and its subsidiaries ("the Group"). All managers in the Group shall at all times comply with the law and they 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.

3 Reporting 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.

4 Procedure

This policy should be read and implemented by reference to the Company's Anti-Bribery and Corruption Procedure (details of which follow)**.**

Rob Smith
Chief Executive Officer
Filtronic plc
21 June 2017

Filtronic plc
Anti-Bribery and Corruption Procedure

Procedures that should be followed during business transactions

Filtronic's policy on Bribery and Corruption applies to all employees (of Filtronic plc including its subsidiary companies) 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 Some due diligence on suppliers and agents should be considered particularly before engaging them to represent the Company in business dealings.
5 Employees (and agents) 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 not 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 "Facilitisation 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.

Rob Smith
Chief Executive Officer
Filtronic plc
21 June 2017

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, information about the Group which you have and which is not public.

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

Filtronic plc (Group Wide) Dealing Code - Adopted on 3rd July 2016

Introduction

The purpose of this code is to ensure that the directors of Filtronic plc (the '**Company**'), and certain employees of the Company and its subsidiaries, do not abuse, and do not place themselves under suspicion of abusing, Inside Information and comply with their obligations under the Market Abuse Regulation.

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

1 Clearance to Deal

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

1.2 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.

1.3 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).

1.4 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.

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

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

1.7 Programme under which Company Securities may be purchased or sold unless clearance has been given to do so.

1.8 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.

1.9 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.

1.10 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.

NOTE:

2 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

3 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.

4 Notification of transactions

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

(A) 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.

(B) 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.

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

5 PCAs and investment managers

5.1 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.

5.2 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.

5.3 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.

5.4 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:

(A) 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);

(B) 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).

'**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, (maura.moynihan@filtronic.com) and in Maura's absence, please send it to either the CEO (rob.smith@filtronic.com) or the Finance Director (michael.tyerman@filtronic.com). 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 Maura, Rob or Michael.

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 Code	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 Flu Policy

Introduction

Influenza is a highly infectious viral illness that has the capacity to spread rapidly. A pandemic is likely to occur when a new influenza 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 flu pandemic, Filtronic's overall aim will be to encourage our staff 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.

In terms of business continuity, this means that we will seek to sustain our core business and services as far as is practicable during an influenza 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.

During a Pandemic

During a recognised influenza 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.

Additional Hygiene Arrangements:
- The company will provide antibacterial 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) and to wash/sanitise their hands regularly.

Flu Vaccination
- The company may identify certain key staff and arrange for those staff to be given a flu 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 flu-like symptoms before being allowed into company premises.
- 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.

Face to Face Meetings

- Travel should largely be avoided unless absolutely essential and in particular if it involves the use of public transport.
- 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 provided and will be cleaned daily.

Staff Identified as Potentially At-risk

- Staff at risk of developing influenza-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 until it is deemed safe to return to the workplace.

Staff with Flu symptoms (the most significant symptoms are the sudden onset of:
fever, cough or shortness of breath; other symptoms may include: headache, tiredness, chills, aching muscles, sore throat, runny nose, sneezing, loss of appetite)

1. Whilst at Work
If a member of staff feels ill with symptoms consistent with flu, 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 influenza, they will be sent home, advised to contact their GP and told not to return to work until the symptoms have cleared.

2. 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 and their GP has confirmed 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 flu. This is really a private matter for the individual, but allowing colleagues to know about it will allow them to 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.

Staff Who Have Difficulty Attending Work (where they themselves do not have flu)
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 flu 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.

c) The employee reports that their child or other dependant has flu 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 Special 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 asks not to attend work because of fear of contracting flu:
The employee is contractually bound to attend work, and not doing so in these circumstances may be dealt with through the company disciplinary procedures. However, if the company is convinced that the individual has psychological or physical reasons whereby they should not attend, then it may decide to agree to a period of annual/unpaid leave, or working from home arrangements with the employee concerned.

e) The employee has school-age children and the school is closed due to the influenza 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.

Rob Smith
Chief Executive Officer
Filtronic plc
21 June 2017

Filtronic plc
Policy on Employment of Connected Persons

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.

Rob Smith
Chief Executive Officer
Filtronic plc
21 June 2017

Filtronic plc
Policy on Counterfeit/Grey Goods

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.

Rob Smith
Chief Executive Officer
Filtronic plc
21 June 2017

Filtronic plc
Code of Ethics

(Filtronic plc and its subsidiaries expect its suppliers and subcontractors to support the principles of this code (as if the Company referred to below was their organisation) and to implement policies that reflect the principles of this code throughout their respective organisations)

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

Good Stewardship: All employees shall 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 or financial data, company policies, procedures, letters, plans, drawings and computer programs, product developments, price and cost data and personal data and

(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 should be prepared accurately and honestly.

Procurement Ethics: Business shall be awarded solely on the merits of the offered product or service; employees should not engage in any activity or allow any relationships to impair their judgment. *(Please see separate policy on Anti-Bribery and Corruption).* No Gifts, Gratuities or Favours of significant value shall be given/accepted by employees to/from Customers or Suppliers except where they are publicly presented for noteworthy service or when explicitly authorised by Filtronic's Board of Directors. (*Please see separate policy on Anti-Bribery and Corruption*).

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.

Customer Care:
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.

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.

Rob Smith
Chief Executive Officer
Filtronic plc
21 June 2017

Filtronic plc
Social Media Policy

Aims and objectives

The Company aims:

- to establish clear rules on personal usage of social media at work
- to remind you that monitoring is taking place
- to advise you that what you say on social media sites, even outside of your working time, is not private and that the Company will not tolerate comments which bring the company, its employees or its customers into disrepute or which infringe the company bullying and harassment policy
- to explain the possible consequences of policy breaches

What the Company means by social media

Social media means:

- social networking sites such as Facebook, Google+, Twitter, Snapchat and MySpace
- professional networking sites such as LinkedIn
- online chat rooms and forums
- blogs
- other social media such as YouTube, Instagram and Flickr.

Use of company equipment for personal social media activities
You may use company equipment, including PCs, laptops and smartphones to access social media outside your working hours or during breaks. 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 set out below.

Monitoring
The Company logs and audits the use of company computers, laptops and PDAs, 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.

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. Any usage should be restricted to breaks.

Posting responsible content on social media sites
When using social media sites such as Facebook, MySpace, Google+, 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.

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:

- Remember that conversations between 'friends' on Facebook are not truly private and can still have the potential to cause damage.
- State that the views you are expressing are your personal ones, not those of the company, in any situation where you disclose that you are an employee of the company or where this could be inferred.

- Report to HR 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.
- Use social media to insult, embarrass or offend a colleague, customer or supplier.
- Use social media to bully or harass or discriminate against any colleague in a way which contravenes the company bullying and harassment policy.
- Comment on business-related topics.
- Post comments or pictures which are inconsistent with the requirements of your role or the image it requires you to project.
- Use a company e-mail address to register on social media sites
- Divulge confidential information about the business or its customers or suppliers

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.

You must remove any material posted in breach of this policy upon our request.

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.

Status of this policy and new instructions

This policy does not give contractual rights to individual employees. The company reserves the right to alter any of its terms at any time although we will notify you in writing of any changes.

This policy may be supplemented by additional instructions from the IT department about how to use the company's telecommunications equipment.

Rob Smith
Chief Executive Officer
Filtronic plc
21 June 2017

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.

1. 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.

2. 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.

3. 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.

4. 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 the HR Department (UK, or International where appropriate) or use the Filtronic grievance procedure.

Rob Smith
Chief Executive Officer
Filtronic plc
21 June 2017

Filtronic plc
Conflict Minerals Policy

Filtronic plc ("the Company") together with its subsidiary companies (herein "Filtronic") Policy Statement on Conflict Minerals:

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.

Rob Smith
Chief Executive Officer
Filtronic plc
21 June 2017

Filtronic plc
Policy on Modern Slavery

1. Policy Statement

1.1 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.

1.2 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.

1.3 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.

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

2. Responsibility for the Policy

2.1 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.

2.2 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.

2.3 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.

2.4 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.

3. Compliance with the Policy

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

3.2 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.

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

3.4 You are encouraged to raise concerns about any issue or suspicion of modern slavery in any parts of our business or supply chains of any supplier tier at the earliest possible stage.

3.5 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.

3.6 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 chains constitutes any of the various forms of modern slavery, raise it with your manager or any plc Director or Company Secretary.

3.7 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.

4. Communication and Awareness of this Policy

4.1 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.

4.2 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.

5. Breaches of this Policy

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

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

Rob Smith
Chief Executive Officer
Filtronic plc
21 June 2017

Filtronic Group
Sanctions Policy Statement

Filtronic plc ("the Company") together with its subsidiary companies (herein "Filtronic") are committed to complying with the sanctions laws and regulations of the United Nations (UN), the United Kingdom ("UK") and the European Union ("EU") as well as applicable sanctions laws and regulations in the jurisdictions in which Filtronic operates.

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

(i) Screening customers and transactions globally against the sanctions lists issued by the United Kingdom, as well as the UN and the EU. (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 comply with the Export Control Act of 2002 and applying for an export licence if necessary. (For information on applying for an export licence and export controls in general refer 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 Filtronic's Global Sanctions Policy. This includes individuals or entities named on an applicable sanctions list or directly or indirectly involving countries or territories subject to comprehensive sanctions. As at 21 June 2017, these countries and territories include Cuba, Iran, North Korea, Sudan, Syria and the Crimea region. (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 (that follows).

Rob Smith
Chief Executive Officer
Filtronic plc
21 June 2017

Annex 1
(to Filtronic Group Sanctions Policy Statement)
Additional Insurance Requirements

As a term of its business arrangements with Willis Towers Watson ("Willis") and our insurers, Filtronic (and subsidiary companies) Filtronic has undertaken to notify Willis 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
6. Require cover for goods that are subject to Export Control Legislation

Below is the current EU, UK, UN and US sanctioned territories list; the blue territories have far wider reaching sanctions against them:

SANCTIONED TERRITORIES LIST	
Afghanistan	**North Korea (Democratic People's Republic of Korea)**
Belarus	Republic of Guinea-Bissau
Burma/Myanmar	Republic of Guinea (Guinea-Conakry)
Burundi	**Russian Federation (incl. Crimea)**
Central African Republic	Serbia
Cote d'Ivoire (Ivory Coast)	Somalia
Cuba	South Sudan
Democratic Republic of Congo (DRC)	**Sudan**
Egypt	**Syria**
Eritrea	Ukraine
Iran	Tunisia
Iraq	Venezuela
Lebanon	Yemen
Libya	Zimbabwe

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, Willis 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 Willis Towers Watson / insurers.

The below lists are not exhaustive and if you have any doubts at all about the goods being exported you must inform us.

Military Goods are defined under Schedule 2 of the Export Control Order 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 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 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
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.

We will establish Quality Management objectives which are relevant to the conformity of our products and enhance customer satisfaction.

The effectiveness of our Quality Management systems is maintained through a process of monitoring and continual improvement versus measurable objectives at all levels of the organisation.

Rob Smith
Chief Executive Officer
Filtronic plc
21 June 2017

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: HR Manager, Filtronic, NETPark, Thomas Wright Way, Sedgefield, Co Durham TS21 3FD, UK with a copy to General Counsel & Co Secretary, Filtronic plc, Filtronic House, Unit 3 Airport West, Lancaster Way, Yeadon, LS19 7ZA

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

Rob Smith
Chief Executive Officer
Filtronic plc
25 March 2018