# IT AND COMMUNICATIONS SYSTEMS POLICY

## 1. POLICY STATEMENT

1.1 Our IT and communications systems are intended to promote effective communication and working practices within our organisation. This policy outlines the standards you must observe when using these systems, the circumstances in which we will monitor their use, and the action we will take in respect of breaches of these standards.

1.2 In particular, remember that you are representatives of our organisation and all communication through our systems (whether by telephone, e- mail or otherwise), must be conducted in an appropriate manner.

1.3 This policy does not form part of any employee's contract of employment and may be amended at any time.

## 2. WHO IS COVERED BY THE POLICY?

2.1 This policy covers all individuals working at all levels and grades, including senior managers, officers, directors, employees, consultants, contractors, trainees, homeworkers, part-time and fixed-term employees, casual and agency staff and volunteers (collectively referred to as 'staff' or 'you' in this policy).

2.2 Third parties who have access to our IT and communication systems are also required to comply with this policy.

## 3. THE SCOPE AND PURPOSE OF THE POLICY

3.1 This policy deals mainly with the use (and misuse) of computer equipment, e-mail, the internet, telephones (including android and smartphones), laptops, other mobile devices, USB flash drives and voicemail. It also applies to the use of fax machines, copiers, scanners, CCTV and electronic key fobs and cards.

3.2 Misuse of IT and communications systems can damage the business and our reputation.

3.3 You must comply with this policy at all times to protect our IT and communications systems from unauthorised access, misuse, and harm. Breach of this policy will be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

3.4 We have a separate Social Media policy which you should also read and understand.

## 4. PERSONNEL RESPONSIBLE FOR IMPLEMENTATION OF THE POLICY

4.1 All managers have specific responsibility to operate within the boundaries of this policy, ensure that all staff understand the standards of behavior expected of them and to take action when behavior falls below its requirements.

4.2 You are responsible for supporting colleagues and ensuring the success of this policy. Staff should ensure that they take the time to read and understand it. If you are unsure about any of the content or the application of this policy, it is your responsibility to speak to your manager.

4.3 If you become aware of any misuse of our electronic communications systems or equipment, you should report it to your manager or a member of senior management.

## 5. EQUIPMENT SECURITY

5.1 You are responsible for the security of the equipment allocated to or used by you, and you must not allow it to be used by anyone else other than in accordance with this policy.

5.2 You are responsible for the security of any computer terminal used by you. You should lock your terminal or log off when leaving it unattended or on leaving the office, to prevent unauthorized users accessing the system in your absence. Anyone who is not authorised to access our network should only be allowed to use terminals under supervision. Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered without first consulting your manager.

5.3 Use of Personal Devices (BYOD)

The use of personal devices for accessing Europia systems or data is not permitted unless explicitly authorised and governed by a separate Bring Your Own Device (BYOD) agreement.

Approved personal devices must meet defined security standards. Europia reserves the right to remove company data from such devices where necessary to protect organisational or personal data.

## 6. REMOTE AND HYBRID WORKING

6.1 Staff who work remotely or in a hybrid arrangement must maintain the same standards of security and confidentiality as when working in the office.
Employees must:

(a) Use secure, password-protected Wi-Fi and, where available
(b) .Prevent third parties (including family members) from viewing or accessing confidential work information.
(c) Lock devices when not in use and store them securely.
(d) Ensure all software and security updates are installed promptly.

## 7. PASSWORDS

7.1 All hardware and services containing or being used to access Europia data must be password protected

7.2 All passwords should be reasonably complex and difficult for unauthorized people to guess. Employees should choose passwords that are at least twelve characters long.

7.3 As well as the password needing to be 12 characters long employees should also use common sense when choosing passwords. They must avoid basic combinations that are easy to crack. For instance, choices like “password12345,” “password11111” and “Pa$$w0rd0000” are equally bad from a security perspective.

7.4 A password should be unique, with meaning only to the employee who chooses it. That means dictionary words, common phrases and even names should be avoided. One recommended method to choosing a strong password that is still easy to remember: Pick a phrase, take its initials and replace some of those letters with numbers and other characters and mix up the capitalization. For example, the phrase “This may be one way to remember” can become “TmB0WTr!”.

7.5 Employees must choose unique passwords for all of their company accounts and may not use a password that they are already using for a

personal account.

7.6 If the security of a password is in doubt, for example, if it appears that an unauthorized person has logged in to the account, the password must be changed immediately.

7.7 Default passwords, such as those created for new employees when they start or those that protect new systems when they're initially set up, must be changed as quickly as possible.

7.8 **Protecting passwords**: Employees may never share their passwords with anyone else in the company, including co-workers, managers, administrative assistants, IT staff members, etc. Everyone who needs access to a system will be given their own unique password.

7.9 Employees may never share their passwords with any outside parties, including those claiming to be representatives of a business partner with a legitimate need to access a system.

7.10 Employees should take steps to avoid phishing scams and other attempts by hackers to steal passwords and other sensitive information.

7.11 Employees must refrain from writing passwords down and keeping them at their workstations. See above for advice on creating memorable but secure passwords.

7.12 Employees may use password managers as authorised by the Europia Senior Management Team

7.13 On the termination of employment (for any reason) you must provide details of your passwords to your manager and return any equipment, key fobs or cards.

7.14 Access on Termination of Employment:

(a) On termination of employment (for any reason), all access to Europia systems, accounts, and data will be disabled without delay by IT or authorised management.

(b) Employees must not retain, record, share, or attempt to use any access credentials following termination.

(c) Under no circumstances should passwords be shared with managers, colleagues, or third parties. Where continuity of access is required, IT will reset credentials or transfer ownership of systems, accounts, or data in a controlled and auditable manner.

## 8. SYSTEMS AND DATA SECURITY

8.1 You should not delete, destroy or modify existing systems, programs, information or data which could have the effect of harming our business or exposing it to risk.

8.2 Staff should not download or install software from external sources without authorisation from a member of senior management. This includes software programs, instant messaging programs, screensavers, photos, video clips and music files. Incoming files and data should always be virus-checked before they are downloaded. If in doubt, you should seek advice from your manager.

8.3 You must not attach any device or equipment to our systems without the prior approval of your manager. This includes any USB flash drive, MP3, tablet or smartphone or other similar device whether connected via bluetooth, USB port, infra-red connection port or in any other way.

8.4 We monitor all emails passing through our system for viruses. You should exercise particular caution when opening unsolicited emails from unknown sources. Inform your manager immediately if you suspect your computer may have a virus. We reserve the right to delete or block access to emails or attachments in the interests of security. We also reserve the right not to transmit any email message.

8.5 All employees must remain alert to cybersecurity risks, including phishing, malware, ransomware, and social engineering.

(a) Multi-Factor Authentication (MFA) must be used wherever supported.

(b) Company data must never be stored on personal or unapproved devices or cloud services.

(c) Any suspected cybersecurity incident, data breach, or phishing attempt must be reported to the IT Manager or Data Protection Officer immediately and no later than 24 hours after discovery.

(d) IT will maintain an Incident Response Procedure to ensure swift containment and investigation of any security incidents.

(e) Europia will provide annual cybersecurity training to all staff.

(f) During system outages or cyber incidents, employees must follow incident response procedures and avoid self-remediation.

8.6 Staff should not attempt to gain access to restricted areas of the network, or to any password-protected information, unless specifically authorised by your manager.

8.7 You must be particularly vigilant if you use our IT equipment outside the

workplace and take such precautions as we may require from time to time against importing viruses or compromising system security. The system contains information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our Data Protection Policy.

8.8 You should also be aware that when using equipment away from the workplace, documents may not be seen and/or read by third parties, for example, passengers on public transport.

8.9 You should avoid carrying any data via a USB flash drive but if there is absolutely no alternative and you have been authorised by your manager to do so, you should ensure that all data is encrypted and the individual files are password protected.

8.10 Data Classification and Handling

Europia classifies information to ensure it is protected and handled appropriately:

- **Public** – Information approved for public release.
- **Internal** – Information intended for internal business use only.
- **Confidential** – Sensitive business, client, or staff information requiring restricted access.
- **Highly Confidential / Special Category Data** – Personal data protected under UK GDPR.

Employees must handle information in accordance with its classification and must only store data on approved Europia systems and services.

8.11 Cloud Services and SaaS Platforms

Only cloud services and software-as-a-service (SaaS) platforms approved by Europia may be used for business purposes.

Uploading, storing, or processing company data on unapproved platforms or personal cloud services is strictly prohibited.

## 9. DATA PROTECTION AND PRIVACY

9.1 Europia is committed to protecting personal data in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

9.2 Personal data collected or processed using our IT and communication systems must only be used for legitimate business purposes and handled lawfully, fairly and transparently.

Employees must:

- Only access data that is necessary for their role.
- Ensure personal and confidential information is not shared with unauthorised individuals.
- Report any suspected data breach to their line manager or the Data Protection Officer immediately.

9.3 Monitoring activities are carried out only where necessary for legitimate business or legal reasons and always in a proportionate manner consistent with UK GDPR principles.

9.4 Data Retention and Secure Disposal: Data will be retained only for as long as necessary for legitimate business or legal purposes and in accordance with Europia's Data Retention Schedule.

Secure deletion, anonymisation, or destruction of data will be carried out where data is no longer required.

## 10. ADMINISTRATOR ACCOUNTS

10.1 Administrator accounts inherently carry more risk to Europia and therefore require additional protections and working practices. Administrator accounts must use Multi-Factor Authentication, be logged, reviewed, and never used for email or internet browsing.

Emergency access accounts will be monitored and reviewed after use.

10.2 Administrator access can only be granted in exceptional circumstances, for a specific purpose and not without the written consent of the senior management team. A log must be kept of all individuals with administrator access and the log reviewed every 6 months. Service accounts or shared accounts are not permitted to have administrator access.

10.3 Where staff have local admin rights to their device (including BYOD) or to a cloud service, they should not log into the local administrator account except for when performing essential and authorised administrative activities such as making configuration changes or downloading software.

10.4 Under no circumstances are administrator accounts to be used for accessing email or for browsing the internet.

## 11. PROHIBITED USE OF OUR EQUIPMENT AND SYSTEMS

11.1 Misuse or excessive personal use of our telephone or email system or

inappropriate internet use will be dealt with under our Disciplinary Procedure. Misuse of the internet can in some circumstances be a criminal offence. In particular, it will usually amount to gross misconduct to misuse our systems by participating in online gambling, forwarding chain letters, or by creating, viewing accessing, transmitting or downloading any of the following material (this list is not exhaustive):

(a) Pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature). Offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or to our clients or customers.

(b) A false and defamatory statement about any person or organisation.

(c) Material which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches our Equal Opportunities Policy or our Anti-harassment and Bullying Policy).

(d) Confidential information about us, our business, or any of our staff, clients or customers (except as authorised in the proper performance of your duties).

(e) Any other statement which is likely to create any criminal or civil liability (for you or us).

(f) Music or video files or other material in breach of copyright.

11.2 Any such action will be treated very seriously and is likely to result in summary dismissal.

11.3 Where evidence of misuse is found, we may undertake a more detailed investigation in accordance with our Disciplinary Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the Disciplinary Procedure. If necessary, such information may be handed to the police in connection with a criminal investigation.

## 12. MESSAGES ETIQUETTE AND CONTENT

12.1 Although email is a vital business tool, you should always consider if it is the appropriate method for a particular communication. Correspondence with third parties by email should be written as professionally as a letter. Messages should be concise and directed only to relevant individuals. Our standard disclaimer should always be included.

12.2 We may use instant messaging as a business tool and the rules relating

to email messages also relate to instant messages.

12.3 You must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate emails. If you feel that you are being or have been harassed or bullied, or are offended by material received from an email, you should inform your manager.

12.4 You should take care with the content of all messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Remember that you have no control over where your message may be forwarded by the recipient. Do not say anything which would cause offence or embarrassment if it was forwarded to colleagues or third parties, or found its way into the public domain.

12.5 Messages are required to be disclosed and used as evidence in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an email cannot be recovered and used as evidence. All email messages should be treated as potentially retrievable, either from the main server or using specialist software

12.6 In general, you should not:

(a) send or forward private emails at work which you would not want a third party to read;

(b) send or forward chain mail, junk mail, cartoons, jokes or gossip;

(c) contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding emails to those who do not have a real need to receive them;

(d) sell or advertise using our communication systems;

(e) agree to terms, enter into contractual commitments or make representations by e-mail unless appropriate authority has been obtained. A name typed at the end of an e-mail is a signature in the same way as a name written at the end of a letter;

(f) download or email anything subject to copyright protection, unless it is clear that the owner of such works allows this;

(g) send messages from another person's computer or under an assumed name; or

(h) send confidential messages via e-mail or the internet, or by other means of external communication which are known not to be secure.

12.7 If you receive a wrongly-delivered e-mail you should return it to the sender.

12.8 Do not use your own personal email account to send or receive email for the purposes of our business. Only use the email account we have provided for you.

12.9 We do not permit access to web-based personal email such as Gmail or Hotmail on our computer systems at any time due to additional security risks.

## 13. USE OF THE INTERNET

13.1 When a website is visited, devices such as cookies, tags or web beacons may be employed to enable the site owner to identify and monitor visitors. If the website is of a kind described below, such a marker could be a source of embarrassment to the visitor and us, especially if inappropriate material has been accessed, downloaded, stored or forwarded from the website. Such actions may also, in certain circumstances, amount to a criminal offence if, for example, the material is pornographic in nature.

13.2 You should not access any web page or download any image, document or other file from the internet which could be regarded as illegal, offensive, discriminatory, in bad taste or immoral. Even web content which is legal in the UK may be in sufficient bad taste to fall within this prohibition.

13.3 As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy. Except as authorised in the proper performance of your duties, you should not under any circumstances use our systems to participate in any internet chat room, post messages on any internet message board or set up or log text or information on a blog or wiki, even in your own time.

13.4 Personal social media use during working hours must be minimal and not interfere with business operations

13.5 Generative AI tools (such as ChatGPT, Copilot, or Gemini) may only be used with management approval.

Such tools must not be used to process personal data, confidential information, or client data without explicit authorisation.

Employees remain fully responsible for the accuracy, appropriateness, and lawful use of any AI-generated output.

13.6 Further information on the use of Social Media is given on our Social Media Policy.

## 14. PERSONAL USE OF SYSTEMS

14.1 We permit the incidental use of internet, e-mail and telephone systems to send personal email or messages, browse the internet and make personal telephone calls subject to certain conditions set out below. You are not permitted to use our systems or equipment to access personal social media accounts (see our Social Media policy for more information). Personal use is a privilege and not a right. It must not be abused or overused and we reserve the right to withdraw our permission for it at any time or restrict access at our discretion.

14.2 The following conditions must be met for personal usage to continue:

(a) use must be minimal and take place substantially out of normal working hours (that is, during lunch hours, before or after work);

(b) personal emails must be labelled "personal" in the subject header;

(c) use must not interfere with business or office commitments;

(d) use must not commit us to any marginal costs; and

(e) personal use must comply with this policy and our other related policies including the Social Media Policy, Equal Opportunities Policy, Anti-harassment and Bullying Policy, Data Protection Policy, Disciplinary Rules and Disciplinary Procedure.

14.3 You should be aware that personal use of our systems may be monitored (see below) and, where breaches of this policy are found, action may be taken under the disciplinary procedure. We reserve the right to restrict or prevent access to certain telephone numbers or internet sites if we consider personal use to be excessive.

## 15. MONITORING OF USE OF SYSTEMS

15.1 We may monitor telephone, e-mail, voicemail, internet and other communications.

15.2 Monitoring may include, without limitation, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the systems as well as keystroke

capturing and other network monitoring technologies. We may store copies of such data or communications for a period of time after they are created and may delete such copies from time to time without notice.

15.3 For business reasons, and in order to carry out legal obligations in our role as an employer, use of our systems, including the telephone and computer systems, and any personal use of them, is continually monitored. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

15.4 We reserve the right to retrieve the contents of messages, posts or details of activity or check searches which have been made on the internet for the following purposes (this list is not exhaustive):

(a) to monitor whether the use of the e-mail system or the internet is legitimate and in accordance with this policy;

(b) to find lost messages or to retrieve messages lost due to computer failure;

(c) to assist in the investigation or wrongful acts; or

(d) to comply with any legal obligation.

15.5 Do not use our IT resources and communications systems for any matter that you wish to be kept private or confidential from us.

15.6 If you access any personal web based email accounts such as Gmail or Hotmail (which is specifically prohibited) we cannot guarantee that those emails will not be caught in our monitoring systems including monitoring what your emails say.

15.7 If you access personal social media using our systems or devices (which is specifically prohibited) we cannot guarantee that the monitoring software will be able to differentiate between personal account use and business use.

15.8 Monitoring is carried out lawfully, proportionately, and in compliance with UK GDPR and the Data Protection Act 2018.

Monitoring is not used for routine performance management. Personal data is accessed only where necessary for legitimate business, security, or legal reasons.

## 16. ENVIRONMENTAL REPOSNABILITY

16.1 Employees are encouraged to use IT and communication systems responsibly to reduce energy use and environmental impact.

(a) Switch off devices and monitors when not in use.

(b) Avoid unnecessary printing and use digital alternatives where possible.

## 17. MONITORING AND REVIEW OF THIS POLICY

17.1 We will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives. If you have any suggestions please let your manager know.

17.2 All staff are required to read, understand, and formally acknowledge this policy on an annual basis.

| | |
|---|---|
| **Approving body** | Europia Trustees and CEO |
| **Last Reviewed:** | January 2026 |
| **Next review date:** | January 2028 |
| **Reviewer / Changes:** | Danail Georgiev |