User Policy for Information Security

Last Update: June 2024

Annington Limited
Hays Lane House
1 Hays Lane
SE1 2HB

The latest version of this document is maintained on the Policy Documents Drive. Please check you are using the correct version.

Annington Limited, together with its subsidiaries and affiliates ("Annington", the "Company", "we"), is committed to acting with collaboratively and integrity in all our business dealings.

1. INTRODUCTION

Information security can be defined as:

> "The collection of technologies, standards, policies, and management practices that are applied to information to keep it secure and safe from unauthorised access, disclosure, modification and inspection. "

Information Security is important to the Company because:

- The information the Company holds is valuable
- Failure to protect this information will result in financial punishment (please look at the Information Commissioner's Office (ICO) website for recent examples of organisations being subject to sanction for rules violations) The fine can be 4% of turnover or £17 million, whichever is higher
- It helps ensure information availability, confidentiality, and integrity
- Risks to information need to be identified and managed

It is essential that the Company maintains the integrity of their IT systems and associated processes. The Company therefore has an Information Security Policy ("the Policy") to help support this and which sets out the policies and procedures in respect of the use of its IT systems, together with your individual responsibilities as a user of those IT systems. This document should be read along with the Company's **Acceptable Use Policy**.

In relation to personal information, under Retained Regulation (EU) 2016/679, UK General Data Protection Regulation (UK GDPR), the Company must:

- use technical or organisational measures to ensure personal information is kept secure, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage
- implement appropriate technical and organisational measures to demonstrate that it has considered and integrated data compliance measures into the Company's data processing activities; and
- be able to demonstrate that it has used or implemented such measures.

The Policy applies to all employees, consultants, and contractors ("Staff") engaged by the Company and, for the avoidance of any doubt, covers the use of all equipment including, but not limited to, workstations, servers, netbooks, laptops, mobile devices/tablets, CCTV, security systems, telephones, mobile phones, voicemail, and other equipment provided to Staff during the course of their employment whether at work, home or elsewhere.

Staff are expected to always exercise their professional judgement and this Policy should be read in conjunction with the Company's other policies and procedures. Staff who fail to comply with the Policy may be subject to investigation under the Company's disciplinary procedure and, where appropriate, disciplinary action may be taken against the member of Staff.

The latest version of this document is maintained on the Policy Documents Drive. Please check you are using the correct version.

2. ROLES AND RESPONSIBILITIES

Information security is the responsibility of all Staff. The Company’s Data Protection Officer and Head of IT are jointly responsible for:

- monitoring and implementing this Policy
- monitoring potential and actual security breaches
- ensuring that Staff are aware of their responsibilities; and
- ensuring compliance with the requirements of Retained Regulation (EU) 2016/679, UK GDPR and other relevant legislation and guidance.

3. REPORTING AN INCIDENT

If you observe or suspect an incident of misuse or loss of personal data or confidential data (Information Security Incident), you must:

- Notify your Head of Department and the Head of IT **as soon as you are aware**;
- Provide a full description of the incident;
- Log the incident by emailing dataprotection@annington.co.uk;
- Conform with the **Personal Data Breach Policy**.

It is the responsibility of the Head of Department to oversee, in consultation with Head of IT investigations into suspected data misuse/loss incidents.

To help you understand and be aware of what an Information Security Event is it can best be defined as:

- an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.

An Information Security Incident is a single or a series of unwanted or unexpected Information Security Events that have a significant probability of compromising business operations and threatening information security.

A Serious Information Security Incident is one where an actual breach has occurred, and it is likely that the interests of the Company have been adversely affected.

If there is any doubt in the mind of the individual whether an occurrence amounts to an Information Security Event/Incident, the person must notify the Head of IT so that an appropriate decision can be reached.

4. IT SYSTEM SECURITY AND MAINTENANCE

All Staff are responsible for the security of the computer(s) and other IT equipment allocated to them during their employment and must not allow them to be used by another person unless permitted by this Policy. Passwords are unique to each user and employees must take appropriate steps to guard against unauthorised access to, alteration, accidental loss, disclosure, or destruction of data. Under no circumstances, should you divulge your password to anyone else nor should you gain access or attempt to gain access to information stored electronically which is beyond the scope of your authorised access level. Your password should never be written down. Writing down, printing and securing a username and password to anything, but especially a device which could be used to gain access to the Company's data is expressly forbidden. All PCs should be shut down by the user prior to leaving the office. Portable computing devices and mass storage devices are not to be left on the desk of any Staff member who is not in the office at that time.

You must always use unique passwords (do not just append a character) and you should never use the same passwords across work and personal accounts.

The password complexity at Annington is such that your password needs to be a minimum of 16 characters, there are no other additional complexity requirements and Azure/Active Directory will enforce this. Mobile devices are secured by a 6-character PIN and further protected by Intune, failure to enrol a device in Intune will lead to the SIM being disabled and the device being withdrawn from use.

Staff who grant authorised access to other users (such as their PA or other appropriate persons) should ensure the level of access is appropriate to that position. Staff who are granted authorised access by another user are reminded that access is given for work related reasons only and should not gain access or attempt to gain access to information stored electronically which is not relevant to their role, beyond their scope or their authorised access level. For the avoidance of doubt, this includes browsing through diaries, emails and other electronic formats for information which is not relevant to their role.

If you lose any IT equipment allocated to you, you should immediately inform the IT Service desk. For the avoidance of doubt, the Company will generally provide one replacement device in the event of loss or accidental damage and individual Staff may be expected to bear the cost of any additional replacements resulting from loss or accidental damage. No non portable computer equipment should be removed from the premises without the express permission of the Head of IT.

5. INDIVIDUAL USAGE AND CONDUCT

The Company recognises that from time to time it is necessary for Staff to use the Company's IT systems for personal use and this is acceptable provided that the use:

- is minimal and does not interfere with the proper performance of your duties; and
- Complies with this Policy and the Company's other policies in force from time to time.

The Policy on personal use is designed to be liberal and its continuance is dependent upon all Staff acting in the spirit of use Policy set out above. The Company reserves the right to withdraw or amend the Policy on personal use.

2. Monitoring and surveillance

Whilst the Company will not actively monitor the actions of Staff save in the circumstances set out below, it is recommended that users work on the basis that all activity can be retrieved and viewed by IT Staff and other duly authorised Staff members if deemed necessary.

In accordance with your terms and conditions of employment and subject to its rights and obligations in law, the Company reserves the right to conduct monitoring (overt or covert) or cause such surveillance to be conducted of your correspondence, phone calls, e-mails, any documents or other material held on the network or your desktop or laptop PC, internet usage and of you by CCTV and by tracking the use of your security card. The purposes for which such surveillance may be carried out include (but are not limited to) the following:

- prevention and detection of crime;
- protection of the Company's property;
- enforcement of the Company's policies with which you are required to comply.

6. EMAILS

Staff are reminded that they should take extra care in the composition of emails as:

- email messages are documents which must be disclosed in legal proceedings if relevant to the issues (unless protected by privilege)
- email messages may be forwarded by the recipient to other email users
- emails are stored in Mimecast for 99 years
- email messages may seem to be an informal method of communication but comments can easily be misinterpreted, leading to offence; and
- Improper statements can give rise to personal or Company liability.

It is therefore recommended that Staff work on the assumption that their emails may be read by people other than the intended recipient and should ensure there is nothing in the email which is likely to cause offence or embarrassment to an individual or the Company, particularly if it found its way into the public domain. Staff should never:

- send Company-wide emails, save where the content is related to the business of the Company
- send offensive, abusive, obscene, sexist, racist, discriminatory or defamatory messages or material which might be construed as harassment
- send messages from another member of the Company’s computer or under a name other than your own name (although PAs and other authorised users are permitted to send emails in their own name on behalf of other persons if permitted or instructed to do so)
- open an email attachment from an unexpected or untrustworthy source or if, for any reason, it appears 'suspicious' (for example, if it ends in .exe, .com or .bat)
- send or forward private emails at work which you would not want a third party to read
- send or forward chain emails at work; and
- Agree to terms or enter into contractual commitments or make representations by email without having obtained proper authority, bearing in mind that when you type your name at the end of an email this act is just as much a signature as if you had signed it personally.

It is also recognised good practice to ensure that when sending:

- important information by email you obtain confirmation of receipt (by either a reply to your email or following up with a telephone call); and/or
- Confidential information by email it is marked as such and you obtain the recipient’s agreement prior to sending it.

Staff are also reminded that if you:

- send offensive, abusive, obscene, sexist, discriminatory, racist or defamatory material or material which could be construed as harassment then this will be subject to investigation under the

Company's disciplinary procedure and, where appropriate, disciplinary action may be taken against the member of the Company

- receive an email, or indeed any electronic correspondence, that you consider to be offensive or which contains abusive, obscene, sexist, racist, discriminatory or defamatory material or material which could be construed as harassment then you should immediately report this to your Head of Department and Head of IT and under no circumstances should you forward this material either internally or externally; and

- Suspect you have been sent a virus then you should immediately report this to the IT Helpdesk and under no circumstances should you open or forward this material either internally or externally.

To ensure we protect against loss of emails, misdirection and interception, all emails which contain sensitive or personal data must be properly secured and protected.

7. THE INTERNET

Save for reasons related to personal use as set out below, Staff should only use the internet for work related reasons.

Staff should not access from the Company's IT systems any web page or electronic file (whether documents, images or other) which, in the widest meaning of those terms, could be regarded as illegal, offensive, in bad taste or immoral. Generally, if any person within the Company (whether intending to view the page or not) might be offended by the contents of a web page or electronic file, or if the fact that the Company's software has accessed the page might cause embarrassment to the Company if made public, then Staff should not view it or attempt to view it. This definition is intended to be interpreted very broadly.

If a member of the Company believes they need to gain access to a website which falls into one of the categories set out above for work related reasons then they should seek the permission of the Head of IT prior to doing so.

Staff may access the internet for personal use, and this includes access to social network sites.

Staff are also reminded that:

Web sites can "know" who has visited them and you may well leave a "calling card" which will enable the site owner to work out who has visited.

Text, music and other content on the internet may be subject to copyright and, where this is the case, should never be downloaded or its content forwarded to other users.

8. SOCIAL MEDIA

The Company realises that social media and networking websites are a part of everyday life. However, we are also aware that these sites can become a negative forum for complaining or gossiping and care must be taken not to breach our confidentiality Policy or offend anyone when using these services. The Policy has been designed to give staff clear guidelines as to what is expected when accessing these sites. The absence of, or lack of, explicit reference to a specific website or service does not limit the extent of the application of this Policy. Where no Policy or guidelines exist, employees should use their professional judgment and take the most prudent action possible. Consult with your manager or supervisor if you are uncertain.

If you have your own personal profile on a social media website, you should make sure that others cannot access any content, media or information from that profile that (a) you are not happy them to have access to; and (b) which would undermine your position as a professional, trusted and responsible person. As a basic rule, if you are not happy for others you work with to see comments, media or information simply do not post it in a public forum online.

When using social media sites, Staff members should consider the following:

- Changing the privacy settings on your profile so that only people you have accepted as friends can see your content
- Never use a work email for social media logins/accounts
- Reviewing who is on your 'friends list' on your personal profile.
- Ensuring personal blogs have clear disclaimers that the views expressed by the author are theirs alone and do not represent the views of the Company.
- Ensuring information published on the Internet complies with the Company's confidentiality and data protection policies. Do not disclose confidential or personal information.
- Breach of confidentiality will result in disciplinary action and may result in termination of your contract.

This Policy does not seek to regulate how Staff use social media in a purely private capacity, if use has no bearing on the Company or its activities. This Policy is intended to ensure that Staff understand the rules governing their use of social media in relation to their work for the Company, or when referencing the Company, or where use of social media may affect the Company or its activities media. This Policy therefore applies where:

- your use of social media relates to the Company or its activities;
- your use of social media relates to, or is otherwise connected with, your work, whether the intended use is personal or professional; and/or
- you represent yourself, or are otherwise identifiable, as someone employed by, or otherwise associated with, the Company.

Bear in mind that, even if you are using social media in a personal capacity, other users who are aware of your association with the Company might reasonably think that you speak on behalf of the Company. You should always take account of any adverse impact your content might have on the Company's reputation.

The latest version of this document is maintained on the Policy Documents Drive. Please check you are using the correct version.

When creating or exchanging content on a social media platform, you must always comply with your contract of employment (or other contractual arrangements) with the Company, the Company's disciplinary rules and any of the Company's policies that may be relevant. You must:

- not harass or bully other members of;
- not discriminate against other members of Staff or third parties;
- not post any content likely to bring the company into disrepute.

9. ARTIFICIAL INTELLIGENCE (A.I.) USAGE

What is A.I. and how could it be used?

Users of an AI tool at Annington are likely to use it to assist in the production of a report or document where the tool may enhance and improve the original content suggested to it. Typically, an AI tool receives preliminary text or content which is then edited and amended to produce a coherent document.

Policy:

- Annington Staff are only permitted to use the Microsoft Co-Pilot A.I. tool. All other tools, such as Chat GPT, will be blocked for use on Annington's systems.
- Please note, no confidential, personal, private or sensitive data should be shared on Co-Pilot, please only use generic examples.
- All Staff should familiarise themselves with the Confidentiality Provisions within the rest of this document (the Annington User Policy for Information Security) and the Annington User Acceptance Policy.
- Staff remain responsible for the output generated and all documents should be proof-read before being sent outside of Annington.

1. Bias and Discrimination: AI systems must not perpetuate biases present in the original data. Staff must ensure that AI outputs do not result in discriminatory outcomes.
2. Explainability and Transparency: AI decision-making processes should be understandable to maintain accountability.
3. Security and Privacy: The use of AI must not compromise security or privacy. Staff must take measures to prevent breaches and protect individual privacy in accordance with Annington's standards and policies.
4. Human Oversight: Staff must maintain control and involvement throughout, particularly in decision-making processes, to ensure the ethical application of AI and address unforeseen issues.
5. Data Governance: All data-related activities, including collection, storage, usage, and security, must comply with applicable data privacy regulations and Annington's ethical standards and policies.

Usage Guidelines:

- Co-pilot is the only approved AI tool for staff to enhance draft documents or emails securely within Annington's Microsoft estate.
- Staff wishing to use alternative AI tools must contact the IT helpdesk for a data privacy assessment.
- Staff are responsible for reviewing AI-generated content for factual accuracy, correctness, and alignment with Annington's brand voice and tone.

Compliance and Enforcement:

- Any data breaches or Policy violations associated with AI use will be addressed following established procedures outlined in the Annington Employee Handbook.

The latest version of this document is maintained on the Policy Documents Drive. Please check you are using the correct version.

10. PROVISION AND USAGE OF MOBILE DEVICES OWNED BY THE COMPANY

In accepting the provision of a mobile device owned by the Company users are reminded that:

- the device is the property of the Company, the provision of which can be withdrawn, permanently or temporarily, at any time
- you should never remove any certificates or profiles installed on the phone
- you should always use appropriate passwords/pass codes to secure the device
- you should not disclose your passwords/pass codes to anyone other than a member of the IT team
- in accepting a device you acknowledge that the Company takes no responsibility for the loss of any non-work-related media or files saved on the device
- in the event of a loss or suspected loss of the device it is the individual's responsibility to report this to a member of the IT team immediately so that the device can be erased remotely
- It is your responsibility to install updates as soon as possible
- We reserve the right to disable the device without any notice
- if you lose or damage the device the Company reserves the right to ask you to reimburse all of part of the cost of replacing or fixing the device
- you are responsible for returning the device if it is no longer needed or when your employment with the Company ends, failure to do so may result in you being charged the appropriate amount to replace the device
- the Company will issue you with the appropriate equipment and accessories to meet the business requirements of the Company
- in particular you should never purchase replica chargers from unauthorised dealers and which have been proven to be a genuine fire hazard

11. PERSONAL USAGE

Personal use is acceptable provided that the use:

- is minimal and does not interfere with the proper performance of your duties; and
- complies with this Policy and the Company's other policies in force from time to time.

Each device allocated to you will have more than sufficient data allowance to enable you to browse the web and generally use a smart phone as intended. If you go over the data allowance by downloading and streaming media, the Company may pass on the excess charges to you.

12. LAPTOP, NETBOOK AND OTHER PORTABLE DEVICES

Laptop computers taken outside secured environments are subject to special security risks: they may be lost or stolen and may be exposed to unauthorised access or tampering. Laptops taken abroad may also be at risk, for example confiscated by police or customs officials.

Laptop loss will mean not only the loss of availability of the device and its data but may also lead to the disclosure of sensitive information. This loss of confidentiality, and potentially integrity, will often be considered more serious than the loss of the physical asset. Therefore, all Laptops issued by the Company will have their disk drive encrypted by Bit Locker prior to being issued to the Staff member.

Under no circumstances should you use a non-Annington supplied portable device to store or work on any sensitive data. You should avoid connecting to Wi-Fi where you have no assurances around the security of said Wi-Fi. Your home network is fine, “free Wi-Fi” is not!

If you have any doubt, queries or concerns speak to Head of IT in the first instance.

13. BRING YOUR OWN DEVICE (BYOD)

The company will issue you with the device(s) that enable you to perform your role. It is therefore not acceptable to use BYOD devices to access work systems and data without the express consent of the IT department. Any BYOD devices must be registered with the IT department.

14. REMOVABLE MEDIA

Information should always be stored centrally on the firms` system and to mitigate the risk of data on USB sticks being lost or stolen it is not possible to save data to USB sticks from our network. There is a Group/Intune Policy in place to make all USB storage read only.

It is not acceptable to have or use any USB or portable drive without the express permission of IT and any such drive (if used) must be encrypted.

15. REMOTE (HYBRID) WORKING

Recognising the change in working patterns since the Pandemic and the hybrid working approach that the firm has embraced there are several Information Security risks that need to be highlighted when working out of the office:

- Confidential or Sensitive documents should be kept securely when not in the office
- Documents should be returned to the office to be filed or securely destroyed
- IT equipment should be returned when your employment ends
- If using non work issued equipment you must ensure the Anti-Virus software is installed and up to date
- You must ensure your operating system is up to date, if you are unclear what this means please contact the IT team
- Please take extra care with the firms' data and devices when working remotely

In addition to the above, please note that:

- If you are using your laptop or any device to work when travelling or in public places do not access confidential or sensitive data unless you are certain you have privacy.

Physical IT security measures

- Ensure that laptops are not left unattended when working remotely
- When travelling and not in use, ensure that laptops are stored securely out of sight. For example, when travelling by car, ensure laptops are locked in the boot. Laptops left on display and unattended will inevitably attract attention and are likely to be stolen.
- Full disk encryption should be used (your laptops are encrypted, all other media you may use should be too, check with IT)
- Do not leave laptops unattended in insecure areas, for example meeting rooms next to areas of public access, and hotel rooms where others may have access. Make use of room locks and lockable storage facilities where available
- Be aware of the potential for opportunist or targeted theft of laptop bags in busy public places including airports, train stations, hotel lobbies, exhibition halls etc. and on public transport e.g. buses and trains
- Do not use laptops with removable media in places where that media could easily be left behind or misplaced
- When travelling, avoid placing laptops in locations where they could be easily forgotten or left behind e.g. overhead racks and taxi boots
- Be aware that the use of laptops in public places will likely draw the attention of those in the vicinity. It is possible that information viewed on a laptop screen could lead to the unauthorised disclosure of that information being processed.

3. Non-standard software

Staff are provided with a package of software appropriate for their role and for which the Company holds the relevant licences. The Company needs to ensure the integrity of the Company's IT systems are always protected, against computer viruses, and that the Company is protected against misuse of others' copyright material. It is therefore expressly prohibited to load onto any of the Company's IT systems any external programmes, software or files which have not been checked by the IT department for viruses and applicable licenses. In all circumstances these should be forwarded to the Head of IT for verification and, as a rule, approval will only be given for genuine work-related matters.

4. Clear Desk Policy

If you are going to be away from your desk for an extended period, ensure you have taken reasonable measures to prevent unauthorised access to confidential information. As a minimum you should:

- Lock your computer ([*ctrl-alt-delete*]) when you are away from your desk
- Shut your computer down completely when leaving the office for the day.
- Dispose of any confidential information in designated confidential waste facilities.
- Store confidential papers out of sight overnight or if you will be out of the office for any significant period in locked cabinets.

Do not:

- Leave papers on printers
- Leave phones, tablets, removable media, or valuable personal belongings unattended for any significant length of time.

5. Post and Courier Services

Care must be taken when sending any confidential, sensitive, or valuable information to ensure items are securely packaged and clearly labelled.

6. Variation

No policy can anticipate every circumstance or question which may arise in the workplace. It is impracticable to attempt to produce guidelines which can consistently be applied to all situations. Common sense and good judgment may dictate that exceptions should be approved in certain circumstances or that certain policies should be changed. For example, introduction of new legislation or codes of practice may require the Company to modify a Policy to comply with the law or code. The Company therefore reserves the right to interpret, modify, revise, supplement, or rescind this Policy or portion of this Policy from time to time as it deems appropriate and will monitor it periodically to review its effectiveness.

7. Queries

If you have any queries in relation to the above then you should raise these with Tim Bond, Head of IT or Sarah Jury, Head of Legal, as appropriate, in the first instance.

DOCUMENT HISTORY

Policy Number	ANN-POL-018	**Version No**	V.1.1
Effective Date	October 2022	**Last Reviewed**	April 2025
Policy Owner	Head of IT	**Policy Approved By**	Annington Ltd Board

Internal Compliance Version Only
VERSION HISTORY

VERSION	AUTHOR	REVISION DATE	CHANGES
V.1.0	Head of IT	October 2022	Policy creation
V.1.1	Head of IT	April 2025	Policy updates, including use of AI

The latest version of this document is maintained on the Policy Documents Drive. Please check you are using the correct version.