IT Acceptable Use Policy

POL-022

1. Policy Purpose and Scope

This policy defines the appropriate use of company information and systems. It is part of the overall Information Security Policy.

In order to ensure the security, confidentiality, integrity and availability of our systems, this policy outlines acceptable user behaviour. Effective security is a team effort requiring the participation and support of everyone using GRAHAM IT equipment and information systems.

This policy applies to employees, contractors, consultants, fixed term employees, and other workers at John Graham Construction Ltd. ("GRAHAM"), including all personnel affiliated with third parties given access to GRAHAM IT equipment or systems. This policy applies to all equipment that is owned or leased by GRAHAM. (The definition of equipment includes, but is not limited to, Personal Computers, Laptops, Mobile Phones, iPads/Tablets, USB & external storage devices, remote site communication equipment, printers, servers etc.)

It is the responsibility of every IT user to know these guidelines, and to conduct their activities accordingly.

GRAHAM are committed to being an inclusive workplace where all employees, customers and stakeholders can fully participate and contribute. We strive to ensure accessibility across all facets of our operations, including physical spaces, digital platforms, communication channels and services.

Our People polices are regularly audited against rigorous accessibility standards to ensure compliance and to support every employee.

Anyone who requires additional support or has any questions regarding accessibility can contact the HR team at HR-JGC@graham.co.uk

2. User Responsibility

Users must **not**:

- Access, or attempt to access, unauthorised information or resources.
- Share passwords or other access credentials with others.
- Impersonate someone else or attempt to disguise identity when using IT resources.
- Use their company credentials for personal applications.
- Leave laptops and other mobile devices overnight, or whilst on leave, in any office/site.
- Connect any Third-Party Site equipment such as CCTV DVR's, switches or wifi units to the GRAHAM network without the prior consent of GRAHAM IT.

- Connect any personal or non-GRAHAM issued device to the GRAHAM network or IT systems.
- Store GRAHAM data on any personal or non-authorised GRAHAM IT equipment
- Store personal information on GRAHAM IT equipment.
- Install any personal apps on GRAHAM devices.

Further details of what constitutes acceptable and unacceptable use is provided in the following sections of this policy.

2.1 User Login/Password Management

2.1.1. Users will be issued with individual login details which is for their sole use. Login details (ie User IDs, passwords, or passcodes) must **not** be shared with **anyone** else. This includes co-workers, family and other household members.

2.1.2. Authorised users are responsible for the security of their passwords and accounts. Passwords must be changed every 100 days; more complex passwords should be used, including mixed case letters, numbers and symbols, using a minimum of 12 characters. Passwords should not be easily associated with the company or the user, nor easily guessed, overly simple or common words. Passwords cannot be reused.

2.1.3. All activity performed under a User Login is the responsibility of the individual assigned to that User Login.

2.1.4. It is recommended that any information that users consider sensitive or vulnerable should be encrypted and password protected and stored in the appropriate designated folder.

2.1.5. Users are responsible for ensuring that all documents/information is handled and stored as applicable on the appropriate information store and according to their classification.

2.1.6. Multi-factor authentication prompts should only be accepted when the user is confident that it has been generated from their IT activity and not from another source (eg hacker).

2.1.7. Users are not to attempt to login to any accounts other than those allocated to them.

2.1.8. Users shall not attempt to access information for which they do not have a ‘need-to-know’.

2.2. Clear Desk/Screen

2.2.1. Users have a responsibility to keep devices and information secure, therefore individuals should take all necessary steps to prevent unauthorised access to company information whether in electronic or printed format.

2.2.2. All PCs, laptops and workstations should be secured with the forced password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by locking/logging-off when the device is unattended.

2.2.3. All PCs, laptops and workstations should be fully shut down at the end of each day to allow security updates to complete.

2.3. Remote Access Management (Remote Working)

See separate Remote Working Policy. All access from outside UK/Ireland is permanently blocked.

2.4. Internet Use

2.4.1. Internet access originating from Company devices must go through a Company-approved internet gateway. Use of commercial Internet service providers to access the Internet is prohibited.

2.4.2. Usernames and passwords associated with websites, portals and other cloud services used to store GRAHAM information should not be shared with anyone.

2.4.3. Accessing or distributing material that is obscene, defamatory, or constitutes a threat, including pornographic material, is prohibited.

2.5. Email and Teams Use

2.5.1. Individuals must prepare emails with the same care and attention as traditional written communications. Note: Electronic communications can be forwarded, intercepted or read by someone other than the person intended and may be disclosed to outside parties. Statements made through electronic communications may be legally binding.

2.5.2. Individuals must use extreme caution when opening e-mails from externals and unknown senders as attachments may contain viruses or malware and links may be unsafe. Users should not enter their GRAHAM user credentials into a link prompt. If a virus is suspected on a user's machine it should be reported as a matter of urgency to the IT Helpdesk.

2.5.3. If an email is received in error, the recipient should notify the sender and delete the message.

2.5.4. There is an accepted risk around the content of incoming emails, attachments or internet sites. It is the recipient's responsibility to delete such inappropriate material and not forward it. Contact the GRAHAM IT Helpdesk if there appears to be an ongoing issue and they will endeavour to block future transmission from that source.

2.5.5. The sending of unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam), is prohibited.

2.5.6. Email, Teams, instant messaging, text or telephone, should not be used to harass or offend other employees or members of the public, whether through language, frequency, or size of messages.

2.5.7. Users should not forward GRAHAM emails/files to their personal email accounts.

2.5.8. Users should not setup forwarding rules on their company email account.

2.6. Device Security/ Damages

2.6.1. All devices used by an individual that are connected to the GRAHAM Internet/ Intranet/Extranet/Cloud storage, must have up to date antivirus software installed and operating.

2.6.2. It is prohibited to deliberately introduce malicious programs onto any GRAHAM computer, network or server.

2.6.3. It is the responsibility of all Employees or Third Parties engaged by GRAHAM, to care for and safeguard GRAHAM property and equipment allocated to them at all times no matter the location, keeping it in as pristine condition as possible. GRAHAM may charge the employee/Third party, the replacement cost of lost/damaged equipment if the employee was negligently responsible. Examples, but not an exhaustive list, of negligent behaviour include:

- Eating/drinking food/liquids in close proximity of the Laptop/iPad/Phone
- Working with Phones, iPads and/or other personal devices without appropriate protective covers
- Working with IT equipment on an unstable surface (e.g. balancing a laptop on knees or edge of a desk/table)
- Leaving Laptops, Phones, iPads etc. unattended and/or unsecured
- Leaving Laptops, Phone, iPads etc. behind on public transport, taxis, airport security, airplanes or any other location
- Carrying a phone/personal device in a shallow/unsecured pocket
- Damage, whether accidental or on purpose, caused by other people.

2.6.4. Because information contained on portable computers is especially vulnerable, special care should be exercised around their physical security especially when unattended.

2.6.5. Portable computers and electronic devices left in unattended vehicles during the day must be locked in the boot and out of sight. Under no circumstances should any sensitive files, documents and/or information be left in an unattended vehicle at any time.

2.6.6. Portable computers and electronic devices must not be left in vehicles after 9.00 pm or overnight, nor should they be left overnight in any office, under any circumstances.

2.6.7. Use encryption of information to reduce the risk of unauthorised access to information, especially when stored on mobile devices. The use of external storage devices is not allowed.

2.6.8. It is the responsibility of all individuals to notify the GRAHAM IT Helpdesk of the loss/damage/theft of IT item(s) as soon as practically possible.

2.6.9. If the item(s) have been stolen, the company also requires the individual to report the crime to their nearest Police Station within 48 hours from the estimated time of theft and receive a crime reference.

2.6.10. Designated staff living in Company provided accommodation are responsible for any comms equipment provided by either the company or third party including the return of same at the end of any contract.

2.6.11. Port scanning or security scanning is expressly prohibited.

2.6.12. Executing any form of network monitoring which will intercept data not intended for the user's device is prohibited.

2.6.13. Circumventing user authentication or security of any device, network or account is prohibited. This includes attempting to circumvent controls and gain access to blocked internet sites.

2.6.14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, access information or disable, a user's screen session, via any means, locally or via the Internet/Intranet/Extranet or on Cloud storage is prohibited.

Consequences of Lost/Damaged IT Equipment

2.6.15. In the case of damaged or lost equipment, the Director of IT Services will assess if the damage/loss is as a result of the individual failing to take proper care and will align with the respective Division/Function Director.

2.6.16. If negligence is determined, the individual may be responsible for the full cost of repair or replacement if equipment is beyond repair or lost.

NB: Individuals will not be permitted to claim any IT equipment purchase, repair and/or replacement via company expenses.

Equipment replacement in the event of loss/irreparable damage

2.6.17. If equipment is lost or irreparable, an alternative will be provided, however, this will be based on availability and may not be an exact replacement of the lost/damaged item. All replaced equipment remains the property of GRAHAM.

2.7. IT Asset Management

2.7.1. It is the user's responsibility to ensure that all software and application updates are applied as soon as they are released to mitigate security vulnerabilities.

2.7.2. All IT assets are the property of GRAHAM and must be returned to GRAHAM IT Helpdesk within 14 days when a replacement device has been issued, when leaving the company or during periods of prolonged absence such as a career break, maternity leave, long term sickness. All associated company data must not be deliberately or maliciously removed.

2.7.3. Devices are issued to users for their sole use, users should not allow others to use them.

2.7.4. In general IT devices are replaced at end of equipment life; outside of this is at the discretion of the Director of IT Services.

2.7.5. It is the responsibility of GRAHAM IT to decide if/when replaced/returned IT devices are reallocated or disposed of. Proper management and disposal of IT devices is required from both an environmental and legal perspective. GRAHAM IT has a legal obligation to ensure IT Assets are disposed of securely. If a device is being disposed of, GRAHAM will use

an appropriate third party who will ensure all devices are securely wiped and disposed of under the WEEE Directive.

2.7.6. Equipment provided may not always be in accordance with personal preferences but will be sufficient for an individual to carry out their role.

2.7.7. To comply with ISO 27001, all IT devices have to be securely erased and as such NO IT devices will be available for purchase or gifting.

2.7.8. Replacement Device

- Users will be given as much notice as possible prior to being issued with a new device.
- It is the user's responsibility to remove any personal information off their device and ensure all business information is saved to the network prior to the changeover date.
- When a replacement device has been issued, the old device MUST be returned to GRAHAM IT within 14 days, after which time the device will be disabled.
- If old IT devices are NOT returned within 4 weeks of the handover of the new device, the Director of IT Services will contact the relevant Managing Director to advise that there is an issue and the full cost of replacing the item new will be taken via payroll if the device is not returned. This shall not constitute an unlawful deduction from wages.

2.7.9. Leavers/prolonged period of absence

- All GRAHAM equipment must be returned to GRAHAM IT on the individual's leaving date or last day prior to commencing prolonged period of absence such as a career break, maternity leave, long term sickness.
- If IT devices are not returned by the date of leaving, the individual will be invoiced for the full replacement cost.

2.7.10. Non-GRAHAM employees

- All GRAHAM equipment must be returned to GRAHAM IT when no longer being used on a GRAHAM contract.
- It is the responsibility of GRAHAM management to advise IT when contractors leave.
- If IT devices are not returned by the contractor they will be invoiced for the full replacement cost.

2.8. Business Use/ Personal Use

2.8.1. GRAHAM IT Assets are provided to conduct Company business. Occasional personal use is permitted as long as it does not:

- interfere with job performance
- consume significant resources, cost or time
- violate this Acceptable Use Policy, other company policies or any applicable laws.

2.8.2. All phone usage is monitored and where personal calls are considered excessive, the company reserves the right to make an appropriate charge.

2.8.3. As a matter of professional courtesy it is advisable to either turn off the mobile device, divert it or set to silent mode when working in open plan offices and during meetings, interviews, training courses, etc. Misuse of a mobile device can be an annoying distraction to others and, at worst, unsafe.

2.8.4. GRAHAM IT assets should not be used by employees or others to operate their own business or trade.

2.8.5. Personal information should not be stored and personal applications should not be installed on GRAHAM devices (including desktops, laptops, iPads and phones).

2.8.6. Data created on the corporate systems remains the property of GRAHAM. Because of the need to protect GRAHAM's network, management cannot guarantee the confidentiality of information stored on any device, networked or not, belonging to GRAHAM.

2.8.7. Users should ensure they are aware of the appropriate procedures for handling any Sensitive, Confidential or Highly Confidential company information to which they have access.

2.8.8. The company does not allow the transfer of the GRAHAM issued SIM card from the supplied handset to a personal device, or vice versa.

2.8.9. All smartphones/tablets have a passcode applied; this should not be removed as it is an additional security measure to protect the information held on the device.

2.8.10. Privileged access or position should not be used to facilitate the use of personal devices.

2.8.11. Under no circumstances is an employee of GRAHAM authorised to engage in any activity that is illegal under local, national or international law while utilising GRAHAM-owned resources. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, GRAHAM's trademarks, logos and any other GRAHAM intellectual property may not be used in connection with any unauthorised activity.

2.8.12. It is unlawful and unsafe to use a handheld mobile device whilst driving. It is GRAHAM policy that those using a mobile device to make or receive calls whilst driving a company vehicle must stop their vehicle at a safe location and switch off the engine before using the phone. Hands-free equipment is fitted for the driver's convenience and is not supplied to enable calls to be made or received whilst in transit. The illegal use of a mobile device may invalidate insurance cover.

2.8.13. Installation of software by the user is prohibited. A list of company authorised and licenced software is in place and must be installed by GRAHAM IT. Users must adhere to the licencing conditions of all installed software.

2.8.14. All Users are required to undertake the Company's Security Awareness training courses. These are issued monthly via email.

2.8.15. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by GRAHAM is strictly prohibited.

2.8.16. Unauthorised copying of copyrighted material including, but not limited to, copyrighted music, games or movies, digitisation and distribution of photographs from magazines, books or other copyrighted sources, and the installation of any copyrighted software for which GRAHAM or the end user does not have an active license is strictly prohibited.

2.8.17. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is prohibited.

2.8.18. It is prohibited to use a GRAHAM IT asset to actively engage in procuring or transmitting material that may be construed as harassment, disparagement or offensive to others based on sex, race, colour, religion, age, nationality, disability, marital status or sexual orientation or is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction. This also covers transmissions that violate the GRAHAM values and professional conduct.

2.8.19. Making fraudulent offers of products, items, or services originating from any GRAHAM account is prohibited.

2.8.20. Making statements about warranty, expressly or implied, unless it is a part of normal job duties is prohibited.

2.8.21. Providing information about, or lists of, GRAHAM employees, suppliers or customers to parties outside GRAHAM without authorisation is prohibited.

2.9. Social Media

2.9.1. The company has a separate policy covering acceptable use of social media. This applies to employees, partners and the supply chain.

2.10. Social Engineering (manipulation of individuals to divulge confidential/ personal information)

2.10.1. Individuals must be alert to possible social engineering attacks and respond appropriately. Social engineers are fraudsters, tricksters and scammers who seek to mislead individuals into revealing or granting unauthorised access to confidential or restricted corporate or personal information, bypassing physical and/or technical security controls.

2.10.2. If an individual recognises that a social engineering-type attack may be in progress, they should:

- Avoid disclosing any (further) information to the suspected social engineer
- Refer the suspected social engineer to Management who will, in turn, try to gather further information in order to authenticate the suspected social engineer's identity (e.g. name, telephone number, employer's name, etc.)

- Report the suspected attack as soon as possible to IT.

2.10.3. Employees must not use social engineering techniques to gain unauthorised access to company information systems.

2.11. Reporting Security Incidents

2.11.1. If an individual is party to or becomes aware of an IT security incident or breach, it is their responsibility to report it **immediately** to the GRAHAM IT Helpdesk. This includes the loss/theft of IT equipment.

2.11.2. Individuals shall not cause security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the individual is not an intended recipient, issuing confidential/sensitive information to internal or externals which they are not authorised to receive, or logging into a server or account that the individual is not expressly authorised to access. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

2.11.3. Where an individual has instigated or facilitated an IT security incident, they will be required to undertake additional IT security awareness training. Failure to do so may result in disciplinary action being taken.

3. Monitoring

- For security and network maintenance purposes, authorised individuals within GRAHAM IT will monitor equipment, systems and network traffic at any time, and where appropriate the device or user account may be disabled. The contents of GRAHAM IT resources and communications systems are the property of GRAHAM.

- GRAHAM reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy. IT administration staff may have a need to disable the network access of a device if that device is disrupting production services or being used in contravention of this policy.

- While GRAHAM will take steps to ensure privacy, all IT system traffic is monitored and devices are audited. Breach of the Acceptable Use policy will result in disciplinary action being taken.

- Logging, auditing, monitoring and recording:
  - Ensure the effective operation of our telecommunications systems and to maintain system security, including the retrieval of lost messages.
  - Investigate and detect unauthorised use of the systems in breach of this policy.
  - Investigate allegations of misconduct, breach of contract, a criminal offence or fraud by the user or a third party.
  - Pursue any other legitimate reason relating to the operation of the business.
  - The company also reserves the right to monitor and record staff use of, and activity on, social media whether or not the use/activity takes place during working hours or using GRAHAM IT equipment or otherwise.

- Monitoring may include (without limitation): location tracking, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, logins, recordings and other uses of social media.
- The company 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.
- The information gathered will only be given to those who need to see it in accordance with these purposes. If information gathered is relevant to any disciplinary action taken, it will be made available to those who are involved in the disciplinary procedure.
- To ensure appropriate business continuity, GRAHAM reserves the right to access and to allow a relevant manager to have access, to an employee's GRAHAM email account in certain exceptional circumstances. All such access requests have to be authorised by the Head of Human Resources.
- Additionally, when an employee leaves the business a relevant manager may be permitted access to the employee's email and OneDrive accounts to facilitate business needs. The length of this period is determined by the Leaver Policy.

4. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. In situations where non–employees violate this policy, GRAHAM reserves the right to take steps as warranted by the situation, including legal action.

5. Definitions

Term Definition

Social Networking sites

Sites such as Facebook, LinkedIn, X (Formerly known as Twitter).

Spam

Unauthorised and/or unsolicited electronic mass mailings.

6. Associated Policies and Records

GRAHAM Information Security Policy

Remote Working Policy

GRAHAM Social Media Policy