IT Acceptable Use Policy

1. Introduction

In order to ensure the security and integrity of our systems, this policy outlines acceptable user behaviour. Effective security is a team effort involving the participation and support of every GRAHAM employee contractor, consultant, temporary, and other workers at GRAHAM, including all personnel affiliated with third parties who deal with information and/or information systems. 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-GFM@graham.co.uk

2. Purpose

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

3. Scope

This policy applies to employees, contractors, consultants, fixed term employees, and other workers at GRAHAM, including all personnel affiliated with third parties given access to GRAHAM equipment or systems.

This policy applies to all equipment that is owned or leased by GRAHAM. Additionally, this applies to all personal devices where an employee uses GRAHAM systems and/or uses proprietary systems to represent 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.)

4. User Responsibility

Users must **not**:

- 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.

User responsibility is defined within the following sub-sections.

4.1. Internet Use

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

4.1.2. Usernames and passwords associated with websites should not be shared with anyone.

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

4.2. Email and Teams Etiquette

4.2.1. 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.

4.2.2. 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.

4.2.3. 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.

4.2.4. 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.

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

4.2.6. The company expectations in relation to communication and collaboration using the Teams platform is detailed in the GRAHAM Teams Guidelines document.

4.3. Password Management

4.3.1. Authorized users are responsible for the security of their passwords and accounts. Passwords should be changed every 100 days; more complex passwords should be used, including mixed case letters, numbers and symbols, using a minimum of 10 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.

4.3.2. All activity performed under a User ID is the responsibility of the individual assigned to that User ID. Do not share User IDs or passwords with anyone.

4.3.3. Do not reveal your account password to others or allow the use of your account by others. This includes co-workers, family and other household members.

4.3.4. It is recommended that any information that users consider sensitive or vulnerable should be encrypted and password protected.

4.3.5. 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).

4.4. Clear Desk/Screen

4.4.1. Users have a responsibility to keep devices and information secure, therefore individuals should take all necessary steps to prevent unauthorized access to company information.

4.4.2. 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 logging-off when the device is unattended.

4.5. Physical Security/ Damages

4.5.1. It is the responsibility of all Employees or 3rd 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/3rd 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.

4.5.2. Because information contained on portable computers is especially vulnerable, special care should be exercised around their physical security especially when unattended. Security locks should be used for portable devices.

4.5.3. 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.

4.5.4. 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.

4.5.5. Use encryption of information to reduce the risk of unauthorized access to information, especially when stored on mobile devices. The use of external storage devices is not allowed, except in exceptional circumstances with director approval. Encrypted devices must be obtained via IT.

4.5.6. 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.

4.5.7. 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.

4.5.8. Designated staff living in Company provided accommodation are responsible for company owned equipment such as Broadband Routers and wireless units.

4.5.9. Port scanning or security scanning is expressly prohibited unless prior notification to the Group IT department is made.

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

4.5.11. 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.

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

Consequences of Lost/Damaged IT Equipment

4.5.13. 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.

4.5.14. 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

4.5.15. 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.

4.6. IT Asset Management

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

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

4.6.3. 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 3rd party who will ensure all devices are wiped and disposed of under the WEEE Directive.

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

4.6.5. 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.
- 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.

4.6.6. 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.
- If IT devices are not returned by the date of leaving, the individual will be invoiced for the full replacement cost.

4.6.7. 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.

4.7. Business Use/ Personal Use

4.7.1. 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.

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

4.7.3. 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.

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

4.7.5. Personal information and applications should not be stored on GRAHAM infrastructure (including desktops, laptops, ipads and phones).

4.7.6. 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.

4.7.7. Under no circumstances is an employee of GRAHAM authorized to engage in any activity that is illegal under local, national or international law while utilizing 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.

4.7.8. 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.

4.7.9. 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.

4.7.10. Unauthorized copying of copyrighted material including, but not limited to, copyrighted music, games or movies, digitization 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.

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

4.7.12. 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.

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

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

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

4.8. Social Media

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

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

4.9.1. 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.

4.9.2. 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.

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

4.10. Remote Access Management (Remote Working)

4.10.1. Particular care should be taken when accessing company systems in non-company locations or from third party devices to avoid accidental disclosure of information to third parties including family members.

4.10.2. Only secure wifi connections should be used when accessing company systems, this includes home wifi.

4.10.3. GRAHAM IT assets (such as laptops, iPads, mobile phones, etc) should not be used by other people.

4.10.4. All IT devices should be logged off and securely stored when unattended.

4.10.5. Only company approved secure online meeting platforms should be used. Particular care should be taken when using online meeting systems to avoid the disclosure of business information either to others in the vicinity of your location or, when allowing the use of shared screens, of information outside the scope of the meeting to other meeting participants.

4.10.6. Hard copies of business information should be securely stored when working remotely until it can be safely returned to the office environment, or confidentially shredded where it is not required to be retained. All company information should be returned or confidentially disposed of at the termination of employment.

4.11. Virus Control

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

4.11.2. Individuals must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses or malware. If a virus is suspected on a user's machine it should be reported as a matter of urgency to the IT Helpdesk.

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

4.12. Reporting Security Incidents

4.12.1. Individuals shall not effect 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 or logging into a server or account that the individual is not expressly authorized to access, unless these duties are within the scope of regular duties. 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.

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

4.12.3. 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.

5. Monitoring

- For security and network maintenance purposes, authorized individuals within GRAHAM IT will monitor equipment, systems and network traffic at any time. 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;
- We also reserve 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): interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of social media;
- 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;
- 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. These may include but are not limited to during sickness absence and holiday periods. All such access requests have to be authorised by Human Resources.
- Additionally when an employee leaves the business a relevant manager may be permitted access to the employee's email account to facilitate business needs. The length of this period is determined by the Leaver Policy.

6. 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.

7. Definitions

Term Definition

Social Networking sites

Sites such as Facebook, LinkedIn, Twitter.

Spam

Unauthorized and/or unsolicited electronic mass mailings.