IT Policy

Geason House |145 North Street
Glasgow |G3 7DA
www.geasontraining.co.uk | 0330 088 9596

Contents

Purpose

The purpose of this policy document is to ensure all Geason staff, students and guests understand the terms and conditions associated with the use of the company IT Infrastructure and their responsibilities therein. This policy document is introduced to staff and students at the point of induction.

Scope

The policies and procedures detailed in this document apply to all Geason employees, management, contractors, students, interns, volunteers and agents using Geason workstations, mobile devices or network infrastructure. The policy recognises and acknowledges the company's duties as laid out in the statutory Prevent Duty guidance for FE Colleges.

Responsibilities

It is the personal responsibility of all users of Geason information and IT assets to comply with the IT Policies.

Waid Network Solutions, are responsible for administering and maintaining the company's private network backbone and all connected parts of the network infrastructure

The responsibility for the management of this policy rests with the Managing Director who is granted management of information systems by Waid Network Solutions. They will be accountable for the security of those assets and protection of privacy in relation to information stored and transmitted through them. In situations where systems are managed by personnel who are not the designated System Administrator, such personnel have a responsibility to work with System Administrators in maintaining the security of systems they manage.

IT Infrastructure

Waid Network Solutions are responsible for:

1. Documenting security procedures governing connections between Geason's direct network and external networks as well as intra-company connections to the network. (Subsidiary links, e.g. Altrincham Training Academy)
2. Granting and denying access to Geason network.
3. Determining appropriate levels of authentication and access privileges for Geason's network.
4. Setting standards for the connection of devices to Geason's network.
5. Authorising gateway systems enabling remote access to Geason, detecting and reporting security violations or attempted security violations of Geason network.
6. Detecting and reporting security violations or attempted security violations of other networks from Geason.
7. In conjunction with the company security, an appropriate level of physical security Geason' hardware.
8. Disaster recovery procedures for hardware, software and information associated with the Geason networks.

Information transmitted and stored using IT infrastructure

System Administrators' responsibilities

System Administrators of information systems are responsible for the security of information stored on their systems and transmitted from their systems across Geason's network and beyond the Company.

1. System Administrators are responsible for:
    a. Developing local procedures aimed at maintaining the security of information;
    b. Ensuring staff members, contractors and third parties understand the importance of information security and are aware of local procedures and central policies;
    c. Disaster procedures for the recovery of information stored on information systems.

Connected systems

System Administrators' responsibilities:

The System Administrators of information systems connected to Geason network are responsible for security procedures governing those systems.

System Administrators of information systems are responsible for:

Where systems are not directly managed by Waid Network Solutions, System Administrators should:

1. Ensure that details of each system within their control are registered with Waid Network Solutions, including software.
2. Ensure that any software they install complies with the software suppliers licensing terms and conditions.
3. Document security procedures governing their information systems, including procedures to minimise the risk of computer virus infections.
4. Granting and denying access to their information systems.
5. Vigilance around security violations or attempted security violations of their information systems and/or other systems from their systems, and reporting to the Managing Director when incidents involve other systems on Geason's network.
6. Ensure that all gateway systems allowing connectivity from an external system require positive user identification and authentication and have a log that record:
    a. User access attempts
    b. Access completions
    c. Access violations
7. Ensure that Waid Network Solutions are aware of gateway systems connected directly to external systems and satisfied that such connections do not present an unacceptable risk to the security to the company's network.
8. Appropriate level of password management is maintained.
9. Appropriate level of physical security for systems hardware is maintained.
10. Implement disaster recovery procedures for hardware, software and information associated with the operation of their information systems.
11. Ensure that contractors or third parties are aware of and comply with local procedures and central policies.

Users' responsibilities

Staff, students and other users of Geason network are to act responsibly in their use of the company's private network and respect limitations placed on their access rights.

Users are responsible for:

1. Following authentication procedures and respecting access imitations stipulated by the Managing Director.
2. Not attempting to connect devices to Geason network without ensuring they meet connection standards.
3. Reporting all security violations or attempted security violations of Geason network to the Managing Director.
4. Reporting all security violations or attempted security violations of other networks from Geason network to the Managing Director.
5. Following security procedures, including safeguarding passwords and avoiding the risk of computer viruses, and respecting access limitations stipulated by the owner.
6. Reporting security violations or attempted security violations to the owner of the particular application or the person appointed by the owner to administer the systems.
7. Reporting instances of actual or suspected computer virus infections to the owner of a particular system or the person appointed by the owner to administer the system.
8. Ensure that any software they install conforms to the terms and conditions of the suppliers' license and that their use of software is in conformity with the supplier's terms and conditions for its use.
9. The company open culture encourages the free flow of information within the company and in pursuit of academic and administrative goals. However, all members of staff, contractors and business partners need to understand the importance of securely handling information entrusted to them.
10. Following local procedures and central policies governing the security of information:
    a. Protecting information appropriately, including that which is at an early stage of preparation or discussion and may not yet be formally recorded on an information system;
    b. Securely transmitting information in a way that minimises the risk of accidental or deliberate misuse outside the company;
    c. Within the parameters of local procedures and central policies, taking action to minimise physical access to information stored.

Enforcement

Any employee found to have violated these policies and procedures herein may be subject to disciplinary action, up to and including termination of employment and/or criminal charges.

1.0 IT Policy

Geason has a substantial investment in information and information technology. The co-operation of all staff and students is necessary to maintain the security of the company IT infrastructure and the information transmitted and stored within the environment and associated storage provision provided by partner-vendors.

Staff and students across the company have access to a networked IT infrastructure and, through the Internet, have access both internally and external to company. This complex open environment requires the company to adopt a policy on security.

Geason has a responsibility to take whatever measures are reasonable to ensure that the company Information and IT assets are protected. Security of the environment must not be unduly compromised and we have a duty of care to provide Geason students, staff and other approved users with access to accurate, relevant and timely information from convenient sources. Geason is also required under the PREVENT legislation to reduce the risk of online radicalisation either through accessing inflammatory material or through online grooming.

The IT Security Policy is approved by the Managing Director. Its operation is overseen by Waid Network Solutions.

Implementation of the IT Security Policy will be the responsibility of the Managing Director who will prepare guidelines to assist departments and support services to adopt good company IT system practices.

Enquiries in relation to this policy should be directed to the Managing Director.

Policy Statements

1. No information ‘system’ may be used within the company unless it has been registered with Waid Network Solutions.
2. The use of software on any Geason system is governed by suppliers’ terms and conditions of use.
3. Every fixed Geason network address will be allocated by the company and must be registered to include ownership details.
4. Users of company information systems must be identifiable and able to be authenticated for access rights and privileges.
    a. Access rights and privileges may be granted only to students, staff, visiting staff and other authorised persons by approved process that governs connecting to the company network.
    b. Access to Smart Assessor may be granted only to Geason students, employees and other authorised persons. Use of Smart Assessor is governed by the relevant Acceptable Use policies (JISC).
5. Subject to company policy, users' access rights and privileges may only be provided by a System Administrator.
6. The company will use its best endeavours to protect its IT systems from unauthorised access.
7. System Administrators must report all attempted, suspected and actual security violations to Waid Network Solutions.
8. Users will be informed of the "conditions of use" affecting access to company IT facilities.
9. A disaster recovery plan for Geason will be prepared and reviewed regularly.
10. Geason recognises and abides by its duties as laid out in the Prevent Duty under the Counter-Terrorism and security Act 2015.

Documents affecting security and privacy

References to guidelines, regulations and procedures that support this policy and references to other documentation and Acts of Parliament that relate to the use of IT equipment the management of security and privacy.

All employees, staff and students using Geason computing devices or accessing data records, should assume they do not have permission to view data or systems unless explicitly given permission to do so by their Line Manager. If access to data or a system is available but you do not believe you should have access, this should be reported to Waid Network Solutions immediately.

Security Principles

» Under no circumstances should anyone try to gain access to a system or device they are not expressly authorised for.

This includes but is not limited to;

- » Another persons' emails or files whether they are stored locally, network or in the cloud
- » Network resources / data folders
- » Geason Information Systems
- » Document folders not owned or the responsibility of the individual
- » Databases

» Any activities to gain access to information which you do not have permission to, to attempt to remove or take data for financial gain or distribution is explicitly forbidden.

» Sensitive data must only be stored on secure media – either within the Geason infrastructure or on an encrypted device.

» Mobile devices which are removed from Geason need to be kept secure at all times and protected by password access, and sensitive data stored upon them needs to be protected by encryption.

» No company information is to be stored on personal devices.

» Any device brought in to the Geason infrastructure can be subject to security checking for software licensing, anti-virus, security patches, illegally downloaded content – bit torrents for example, to protect the company network from inappropriate use.

» Any data transmitted over the Geason network can be monitored and appropriate action taken for misuse.

- » For example, downloading from Torrent sites,
- » Looking at Pornography, or any material associated with extremist views or any radicalisation agendas
- » Malicious emails, Malware, Phishing,
- » Gambling
- » Stalking, Bullying, Harassment behaviour

» Geason computing devices must not be used for illegal purposes

» Geason retains the right to remove services at any time if you are found to be in violation of any of the defined terms of use

» Monitoring of emails can be done at any time at the request of a Director.

- Monitoring / data records will be submitted as evidence by Waid Network Solutions if asked to do so
- The cost of an encrypted device is the individual areas responsibility
- Geason require the use of Bit Locker for laptop encryption on all new devices
- It is the responsibility of staff to report inappropriate content which is found to be available on the Geason network
- Staff must adhere to basic physical security
    - Ensure Rooms with IT equipment in are locked when not in use
    - No students to be left unattended in rooms with IT equipment
    - Only Authorised staff to enter network infrastructure rooms
    - Devices cannot be taken off site without permission from Waid Network Solutions, other than mobile devices specifically allocated to individual users
    - Loan devices – on site use only without prior approval
    - Lock desktops when not in use
    - Laptops to be secured to the desk or locked away when not in use
    - All desktop cases to be secured with padlock to prevent theft or damage of internal components

1.2 IT Security

1.2.1 Waid Network Solutions reports to the Managing Director.

1.2.2 It is the responsibility of the company IT Security Coordinator, together with the Geason Estate manager or deputy (who is responsible for physical security) to ensure that all methods required to adequately discharge their responsibilities are brought to the notice of administrators of information. The IT Security Coordinator is also responsible for maintaining a coordinated approach to IT security throughout Geason.

1.2.3 The IT Security Coordinator will devise and oversee an ongoing education program designed to educate System Administrators, staff and students about IT security.

1.2.4 On request, the IT Security Coordinator will review established security procedures with System Administrators to ensure that these maintain appropriate authentication processes, access privileges and access controls.

1.2.5 As part of monitoring compliance with the security policy, the IT Security Coordinator will also check that local security procedures, consistent with Geason's wider procedures, and that they are being followed. If necessary, alert the Managing Director to defective security practices.

1.2.6 Mechanisms for detecting potential, attempted and actual access violations of Geason will be monitored by Waid Network Solutions and investigated, particularly those emanating from outside the company communication network.

1.2.7 Waid Network Solutions, on the recommendation of the Managing Director, are authorised to disconnect systems Geason network if a perceived threat to company IT security exists.

1.3 Access Control

1.3.1 Access to Geason information must be based on each individual's role and responsibilities. Users must only be provided with access to applications and services that they have been specifically authorised to use by the relevant Line Manager, as dictated by business needs.

1.3.2 An Acceptable Use Policy is signed as part of the enrolment process for Students. A warning banner advising that access to the system is for authorised individuals only is shown prior to logging onto all systems. The warning banner reflects relevant legislation with regard to penalties for unauthorised access.

1.3.3 Formal user account management procedures control the secure creation, amendment and deletion of user accounts. Staff with privileged accounts must use a separate, non-privileged account for performing normal business functions.

1.3.4 All user accounts are protected by passwords. Passwords are required to be changed at least once every 90 days.

1.3.5 User accounts must be attributable to a single individual. Under no circumstances must staff user accounts be shared or password information divulged. Staff must be provided with security training on this matter and be advised of the policy when issued with their user account.

1.3.6 All personal computers require a password to be entered when awakening from sleep mode. This configuration is enforced via Windows Group Policy Objects and other regular configuration checks.

1.4 Business Continuity Management

Business Continuity and disaster recovery plans must be made available in order to ensure operational continuity in the event of a loss of service or disaster.

- Geason has formalised its business continuity planning process. Business continuity planning comes under the overall control of the Managing Director.
- A formal risk assessment has been undertaken across the company in order to determine all essential and critical business activities to be included in the business continuity plan.

1.5 Data Security

Communications and Operations Management

The following security controls are applied within Geason data centres;

1.5.1 Roles and responsibilities are defined and include appropriate segregation of duties to prevent both fraud and potential malicious or accidental misuse of the system, or have other compensating controls.

1.5.2 A mandatory, locked down installation of leading anti-virus software is applied to all shared and personal computer systems. A robust mechanism for timely distribution of updates to the anti-virus software, operating system and other key software is in place. This allows for centralised “push” distribution of updates and monitoring of successful uptake.

1.5.3 Information must not be stored, processed or transmitted by Geason staff on equipment neither managed nor owned by Geason. This includes personal home computers and other mobile computing devices such as smartphones and tablets. However, information may be stored in the cloud service provided by Geason via the Microsoft Agreement, OneDrive for Business.

1.5.4 Only authorised and appropriately licensed software may be installed within the Geason environment.

1.5.5 Data is backed up throughout the day. Operational procedures verify the successful completion of backups. Backed-up data is stored in secure locations on site and externally. Backup failures are recorded via Waid Network Solutions.

1.5.6 Appropriate patch management systems encompassing controls relating to monitoring vulnerabilities, vendor patches and fixes, are in place for the centrally managed Microsoft systems. Should a business need arise to not implement one of more identified patches, then such decisions are risk-assessed, acknowledged and documented.

1.5.7 External network perimeters are hardened and configured to protect against unauthorised traffic. Inbound and outbound points must be protected by means of firewalls and intrusion detection systems.

1.5.8 All PCs are equipped with personal firewall software. It is automatically enabled and uses a standard configuration to protect against malicious network traffic, including Internet-based network threats, un-trusted networks or malicious software. Base configuration settings are secured against change, tampering or disablement by end users or malicious programs. This protects the host PC from incoming malicious activity, and potentially other networks to which the PC attaches by restricting outgoing network activity generated by virus or worm infections etc.

1.5.9 A Virtual Private Networking (VPN) device or equivalent must be used when PCs connect remotely to the internal Geason network, with the exception of Waid Network Solutions who can allocate access to authorised third parties, at their discretion. Remote access gateways connect to the company network via intrusion detection systems that identify and can block suspicious activity and known attack patterns.

1.5.10 All storage media (hard drives, back-up tapes etc.) are subject to audited, secure destruction, either using physical measures (such as drilling or crushing), or logical means using multiple random overwrites.

1.6 Asset Management

1.6.1 Information is an asset of Geason. The company is charged with the protection of information for its learners and staff. In order to secure the assets properly Geason applies controls that are appropriate to the requirements and sensitivity of that information – Laptops will be installed with encryption to protect the on-board data.

1.6.2 Information owners must ensure that data destruction, retention and backups comply with business, legal and regulatory requirements.

1.6.3 All central information systems (PICS database, File stream, finance database, human resources database and active directory database) are backed up centrally.

1.6.4 Geason recommends that data is not removed from site. If data is taken from site it should be encrypted using suitable methods (advice can be gained from Waid Network Solutions). The person taking the data from site takes personal responsibility for the security of the data once removed from Geason.

2.0 Secure Working Practice - Workstation Security

Appropriate measures must be taken when using devices to ensure the confidentiality, integrity and availability of sensitive information and that access to sensitive information is restricted to authorised users.

Staff using workstations or other devices shall consider the sensitivity of the information that may be accessed and minimise the possibility of unauthorised access.

Geason will implement physical and technical safeguards for all workstations that access electronic information to restrict access to authorised users.

Appropriate measures include:

1. Restricting physical access to devices to only authorised personnel.
2. Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorised access.
3. Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected
4. Complying with all applicable password policies and procedures.
5. Ensuring workstations are used for authorised business purposes only.
6. Never installing unauthorised software on workstations.
7. Storing all sensitive information on network servers
8. Keeping food and drink away from workstations in order to avoid accidental spills.
9. Securing laptops that contain sensitive information by using cable locks or locking laptops up in drawers or cabinets.
10. Ensuring that monitors are positioned away from public view. If necessary, install privacy screen filters or other physical barriers to public viewing.

2.1 Workstation Security Offsite

Device security offsite

1. Only view confidential documents, on paper or on screen, if you are sure they cannot be read by other people nearby.
2. Only leave your device temporarily unattended e.g. whilst working at another site or train/plane, etc. if:
    a. It is being looked after by a known and trusted individual and
    b. The screen is locked.
3. Only move your laptop if it is either
    a. switched off - this is the safest and preferred method or
    b. in standby mode as a minimum e.g. for very short journeys during the day

    This will protect the hard drive from damage and provide password security if the laptop/device is inadvertently left unattended, lost or stolen.
4. When outside of the office you must keep your laptop/device bag either in sight, within reach or inaccessible to others, e.g.:
    a. If you must take your bag with you to a public place, put it between you and a corner/wall so that no one else can reach it and never let it out of your sight.
    b. If on public transport keep your laptop/device bag either on your lap or safely behind your legs.
    c. If on a plane keep your laptop/device under the seat in front of you.
    d. If you are transporting your laptop/device in a vehicle and might need to leave it unattended temporarily, always lock it in the boot and out of sight at the start of your journey or take it with you when leaving your vehicle.

3.0 Device Allocation

3.1 Computers

Staff required to use a computer for the majority of their working day will be entitled to receive a company device, this could be a desktop computer if you are a member of support staff or a laptop if you are a member of Curriculum staff. Geason does not have sufficient funds to provide staff with multiple devices.

Waid Network Solutions must approve all IT hardware purchases; devices purchased without their prior approval will not be supported or connected to the Geason network. This is to ensure full compliance with company systems and management/monitoring software.

Members of staff who are allocated a desktop will not generally be able to have a company laptop as well or vice versa. Those members of staff who currently have more than one device, (i.e. a laptop and a desktop) will be asked to choose which one they would like to keep and return the second device to ensure a more even allocation of resources across the company. Anyone allocated a Geason portable computing device is required to take reasonable care of it and ensure its safe keeping. Loss, theft or significant damage of any device will be charged back to the department at full cost price to enable the purchase of a replacement. Loss or theft should be reported to the police by the member of staff who has been allocated with that device then also communicated to Waid Network Solutions.

3.2 Network Connection

Device allocation and connection to the company network is dependent on availability of network points or a resilient wireless connection.

3.3 Device Ownership

All company devices are the property of Geason and their allocation and management is the responsibility of Waid Network Solutions, regardless of which departmental budget was used to purchase the device.

Included within this policy are all Geason tablet devices. All company iMacs will be centrally managed and imaged, any machines too old to support the company image will be removed from the network and not supported by Waid Network Solutions. All unlicensed software will therefore also be removed.

3.4 Account Privileges

Only Waid Network Solutions staff will have Admin rights on any device, or are authorised to move Geason computing devices or change the configuration of Geason computing devices. Computers relocated without the prior knowledge and consent of Waid Network Solutions will be assumed stolen and reported to the police. Disciplinary action may be taken against the member of staff found responsible for moving the device without permission.

3.5 User Accounts

All staff and students will be provided with a Geason computer user account. This account will be created on the basis of details provided to us by the students. This information will also be used to create email addresses, so please ensure that the information you provide is accurate. It is important to note that we cannot change usernames once the account has been setup with Microsoft Office 365. If your circumstances change and you would like your username and email address to be changed to reflect a change of name, we will have to delete the existing account and create a new one with the new details. During this process we cannot guarantee that all data from one account will be successfully migrated to the new account although we will use our best endeavours.

3.6 Device Requests.

If staff would like a mobile device instead of a desktop computer, this needs to be specified and approved by Waid Network Solutions and their Line Manager. The device will be a laptop which can be provided with a separate monitor, mouse and keyboard if required. The device will be purchased from the Line Manager's area budget. Any other device allocated to the member of staff will be returned to Waid Network Solutions for re-distribution. All staff, including Line Manager's, under normal circumstances, are to have one computing device only provided by the company to ensure fair and even distribution of IT resources across Geason.

4.0 Acceptable Use

4.1 Prohibited Use

The Geason email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair colour, disabilities, age, sexual orientation, pornography, radicalisation and/or extremist views, religious beliefs and practices, political beliefs, or national origin. Employees who receive any emails with this content from any Geason employee should report the matter to their manager and then Waid Network Solutions immediately. Students who receive any such emails should report the matter to their tutor or another member of staff immediately.

4.2 Personal Use

Using a reasonable amount of Geason resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a Geason email account is prohibited. Virus or other malware warnings and mass mailings from Geason shall be approved by Geason senior management before sending. These restrictions also apply to the forwarding of mail received by a Geason employee.

4.3 Monitoring

Geason employees shall have no expectation of privacy in anything they store, send or receive on the company's email system. Geason may monitor messages without prior notice. Geason is not obliged to monitor email messages.

An email sent to all staff or all students can only be sent from a member of the Geason Management Team, Senior Management Team or nominated representatives authorised by Managing Director.

4.4 General Use and Ownership

While Geason network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of Geason. Because of the need to protect Geason's network, management cannot guarantee the confidentiality of information stored on any network device belonging to Geason.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their Supervisor or Manager.

Geason recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see Geason Secure Working Practice and Device Security procedures.

For security and network maintenance purposes, authorised individuals within Geason may monitor equipment, systems and network traffic at any time.

Geason reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.5 Security and Proprietary Information

The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential. Examples of confidential information include but are not limited to: learner data, staff data, company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Staff should take all necessary steps to prevent unauthorised access to this information.

Keep passwords secure and do not share accounts. Authorised users are responsible for the security of their passwords and accounts. System level passwords should be changed every 90 days, user level passwords should be changed every 90 days.

All PCs, laptops and workstations should be secured when not in use either by logging-off or locking the screen when the host will be unattended.

As information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the Secure Working Practice and Device Security policy.

Postings by employees from a Geason email address to newsgroups or forums should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Geason, unless posting is in the course of business duties.

All hosts used by the employee that are connected to the Geason Internet/Intranet/Extranet, whether owned by the employee or Geason, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.

Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.6 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is any user of Geason computing infrastructure authorised to engage in any activity that is illegal under law while utilising Geason-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

The following activities are strictly prohibited, with no exceptions:

- 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 Geason.
- Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Geason or the end user does not have an active license is strictly prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using a Geason computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or other laws in the user's local jurisdiction.
- Using a Geason computing device to undertake online radicalisation activity either through accessing inflammatory material or through online grooming.
- Making fraudulent offers of products, items, or services originating from any Geason account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the employee is not expressly authorised 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.
- Port scanning or security scanning is expressly prohibited unless prior notification to and approval from Waid Network Solutions is achieved.
- Executing any form of network monitoring which will intercept data not intended for the user’s host, unless this activity is a part of an employee's normal job/duty.
- Circumventing user authentication or security of any host, network or account.
- Interfering with or denying service to any user other than the user's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, Geason students and/or employees to parties outside Geason.

4.7 Unacceptable Email and Communications Activities

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorised use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within Geason networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Geason or connected via Geason's network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

4.9 Blogging

- Blogging by employees, whether using Geason's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Geason systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Geason policy, is not detrimental to Geason best interests, and does not interfere with an employee's regular work duties. Blogging from Geason systems is also subject to monitoring.
- Geason Secure Working Practice and Device Security policy also applies to blogging. As such, Employees are prohibited from revealing any Geason confidential or proprietary information, trade secrets or any other material covered by Geason Secure Working Practice and Device Security policy when engaged in blogging.
- Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Geason and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by Geason Equality & Diversity policy.
- Employees may also not attribute personal statements, opinions or beliefs to Geason when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Geason. Employees assume any and all risk associated with blogging.
- Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Geason trademarks, logos and any other Geason intellectual property may also not be used in connection with any blogging activity

5.0 Internet Use And Monitoring

5.1 Internet Service Provider

Geason aims to provide a secure network environment that controls access to the internet for staff, students and other people who use company devices and our guest wireless network to access the internet. The purpose of this secure environment is to restrict access to inappropriate websites for staff and students and to minimise exposure to web content which could potentially lead to the radicalisation of staff and / or students.

Our primary internet connection is provided by Waid Network Solutions.

Waid Network Solutions provide continual monitoring and protection against cyber threats and unwanted intrusion attacks, restricting access to various web locations through security and acceptable use policies.

For all traffic the monitoring system must record the source IP Address, the date, the time, the protocol, and the destination site or server. Where possible, the system should record the User ID of the person or account initiating the traffic.

There are a number of mechanisms in place which offer protection from unwanted access to potentially damaging and influential websites being accessed from Geason computers or publicly owned devices connecting to the internet via our company wireless network, in line with Government Prevent strategies as expressed in the Counter-Terrorism Security Act 2015.

5.2 Access Controls

In addition to the security and parameters set out by Waid Network Solutions, our internal company network is protected from the outside world by an enterprise level firewall, Cisco 800, TP-Link Jetstream Managed PoE Switches.

The firewall works by blocking access to certain communication ports, for example, we block the ports which are known to host peer to peer networks and file sharing websites, amongst other things. The only ports we have open for external access are client access ports 80 and 43 – these provide internet access only.

While the firewall blocks access to specific ports, the web filter allows us to block specific websites and categories, as defined by our own requirements. All Geason desktop computers connect to the internet via this proxy, through the web filter. The only machines with a direct route out are servers providing web services or requiring external communications, such as Finance and MIS systems, even so, access to these servers is restricted at user level via group policy in active directory.

The Geason website is hosted on an off-site server with a direct route out, however access back in to the company is severely restricted by channel blocking and permission based access level control.

The web filter is designed to block access to specific sites, based on policies set by Geason. In addition to adhering to policy criteria, it is also possible to block specific domains and individual websites, allowing access to certain elements of a website.

It is entirely user configurable and can restrict access by a number of different methods which can be linked together to provide an all-encompassing secure browsing solution.

Scope of parameters:

- Filtering is done by course code
- Age range
- Subject matter
- Categories
- Key words – gambling, porn, violence, hate, ISIL, ISIS etc.

The structure is such that we can restrict access by age and course code. Wireless access is set to the highest possible security level as all ages can connect to the Geason wireless network.

In addition to restricting internet access and exposure to unwanted subject areas, all Geason desktop computers are locked down to prevent installation of software, access to peer to peer networking, unauthorised IM, (yahoo etc.) via Group Policy. Waid Network Solutions can also see, via security logs on the web filter, where staff and students have tried to access an unauthorised page.

Our policy towards social media is to allow access to main sites, such as Facebook.com, but restrict the applications available from within. As social media represents a very powerful marketing and communication tool, we are not in a position to block it completely, although in the past, we have restricted access to it on classroom computers, only allowing access in common areas.

Access to Geason computers is controlled through user authentication, only authorised staff and students can access Geason computers. These accounts are unique to each user which enables tracking. There are no generic accounts available for security reasons.

It should be noted however, that whilst access to the internet is controlled through the wired and wireless networks at Geason using both company and guest devices, anyone accessing the internet on their own personal device through a 3/4G connection (not using Geason WIFI), will have full and unrestricted to any website whilst on the company premises and unfortunately, this cannot be prevented.

5.3 Access to Web Site Monitoring Reports

General trending and activity reports will be made available to any employee as needed upon request to Waid Network Solutions. Computer Services staff may access all reports and data if necessary to respond to a security incident. Internet Use reports that identify specific users, sites, teams, or devices will only be made available to associates outside the Computer Services team upon written or email request to Waid Network Solutions from a member of Senior Management or a Human Resources Representative.

6.0 Password Security

6.1 General Password Construction Guidelines

Geason requires that all staff & employees use strong passwords.

Passwords will have the following characteristics:

- Contain lower case characters
- Upper case characters
- Numbers
- At least one “Special” character (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc.)
- Contain at least 10 characters in total.

Guidance on choosing a password:

Passwords should avoid a word in common usage such as:

- Names of family, pets, friends, co-workers, fantasy characters, etc.
- Computer terms and names, commands, sites, companies, hardware, software.
- The words "Geason", or any derivation.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)
- Should not contain your name or username

Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R" or "Tmb1W>r~" or some other variation.

(NOTE: Do not use either of these examples as passwords!)

6.2 Password Protection Standards

» Always use different passwords for Geason accounts from other non-Geason access (e.g., personal ISP account, personal banking, etc.).

» Always use different passwords for various Geason access needs whenever possible. For example, select one password for systems that use directory services (i.e. LDAP, Active Directory, etc.) for authentication and another for locally authenticated access.

» Do not share Geason passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential Geason information.

» Passwords should never be written down or stored on-line without encryption.

» Do not reveal a password in email, chat, or other electronic communication.

» Do not speak about a password in front of others.

» Do not hint at the format of a password (e.g., "my family name")

» Do not reveal a password on questionnaires or security forms

» If someone demands a password, refer them to this document and direct them to Waid Network Solutions.

If an account or password compromise is suspected, report the incident immediately to Waid Network Solutions.

6.3 Application Development Standards

Application developers must ensure their programs contain the following security precautions.

Applications:

- Shall support authentication of individual users, not groups.
- Shall not store passwords in clear text or in any easily reversible form.
- Shall provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- Shall support TACACS+ (older authentication commonly used with Linux systems), RADIUS and/or X.509 with LDAP (Active Directory authentication) security retrieval wherever possible.

7.0 Printing Policy

Geason has a managed service to operate Ricoh Copiers on site which are Multi-Function Devices and allow secure printing, copying, scanning and emailing of documents, printing to A4 and A3, single and double sided. They also collate printed documents and certain models offer stapling and hole-punching.

The costs associated with the use of these copiers are considerably less than printing on laser jet printers and they are covered by a maintenance contract which provides onsite support within 4 hours of logging a call.

8.0 Software Purchasing And Installation Policy

Staff and Students are not authorised to install software on Geason computing devices operated within the Geason network. Software requests must first be approved by the requester's Manager and then be made to Waid Network Solutions. Software must be selected from an approved software list, maintained by the Waid Network Solutions, unless no selection on the list meets the requester's need, Waid Network Solutions will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation, under the direction of the Departmental Software Specialist / owner.

8.1 Software Installation / purchase request form

All requests for software need to be submitted to Waid Network Solutions in advance.

Any software purchased without the prior knowledge and consent of Waid Network Solutions will not be supported or installed on Geason computers, as per the Finance Regulations.

8.2 Departmental Specialists / Owners

Waid Network Solutions require one dedicated departmental specialist / owner (and a backup) to take responsibility for the specialist software used in their area. This person will liaise directly with Waid Network Solutions to provide installation locations and configuration options for the software. No changes will be made to the configuration, or installations in alternative locations, without the prior authorisation of the department specialist / owner.

8.3 Computer Ownership

Geason computers are owned by Geason, a business, not an individual, therefore all software installed on them has to be licensed to Geason, the company and not an individual. This also means that software available free for home use (freeware), is not always available under the same licensing conditions for use on corporate computers. In such cases a valid license agreement will need to be produced before software can be installed.

All Software Installed Must Be Covered By A Current, Valid License Agreement

8.4 Hardware Specification

The hardware specification of the computers across the company varies, sometimes due to age, but in other cases, certain computers have been custom built to serve a specific purpose, therefore it is crucial that all requests for software are made to Waid Network Solutions so that they can ensure the proposed purchase will be compliant with our network and Computer systems. Software also has to be SCCM compliant for packaging and deployment.

8.5 Permissions

All software installed on Geason computers must be able to run without any special account permissions, under no circumstances will staff or students be granted admin rights to use software other than specified personnel in MIS.

8.6 Time scale for software installation;

New software will require testing in a secure environment before deploying on the company network. This can take up to a month. All new software required for September start of term needs to be requested by the 30th May to allow sufficient time to investigate the optimum purchase options, install, configure, test and deploy the software. If new software must be installed during term time, we require one month's notice to test and package the software ready for installation and will then deploy at the next available time slot if manual installation is required – packages which can be deployed over the network can be done so when they are ready, software which requires an installation at the desktop will usually have to be scheduled for a holiday period.

Installations on Curriculum machines can only realistically be done during holiday periods as access to classrooms is severely restricted during term time.

Installations on staff machines can be organised for a mutually agreeable time at any point in the year, subject to the appropriate testing having been completed successfully.

9.0 Support Desk Service Standards

9.1 Creating a Support Ticket

Staff and students can log support requests via one of two routes;

1. Directly on to the Support Desk system at http://helpdesk.waid.co.uk/ this is the preferred method as it automatically generates a support call and includes all the information required by Waid Network Solutions to start work resolving the issue raised.
2. Via Telephone to Waid Network Solutions on Lync, or 0141 530 9790.

Information required

When logging a support call with Waid Network Solutions, please include as much information as possible. Valuable time can be lost chasing for information that could be better spent resolving the issue at hand.

Please always include;

- Full description of the issue
- Username of the person experiencing the problem
- Computer name and location if it is specific to one machine
- Contact details
- Convenient time for the remedial work to be carried out
- As much detail as possible to enable us to begin remedial works.

9.2 Service Level Agreements (SLA's)

All calls logged to a technician are to be acknowledge within 4 hours of the technician being made responsible for the call.

- URGENT priority: Must have had an attempted resolution within 1 Hour (24/7x365) – details to be recorded on the ticket.
- HIGH priority: Must have had an attempted resolution within 8 Hours (24/7) and details of this recorded against the call for reference
- NORMAL priority: Must have had an attempted resolution within 3 working days and details logged on the ticket.

The following should provide a guideline as to the definition of priority levels:

Urgent – A companywide Issue – The internet or Email is unavailable. Authentication has failed. Network switch has failed. Virtual Machine / Host has failed.

High – Affecting a Classroom or an individual with a business critical process which has to be completed to a deadline. Inter Active White Board not working – unable to teach. Finance document has to be submitted and the process is failing. Student reports have to be uploaded and the process is failing.

Normal – affecting one person or a small group of people but does not stop them working on other items, for example, a printer has failed.

10.0 Tablet Devices / App Purchasing Policy

10.1 Purchasing Tablet devices

Any member of staff who requires a tablet device for company purposes should first obtain approval from their Line Manager supported by a written justification.

The request should include an explanation of how the tablet device will benefit the department and/or the learners.

Once authorised by your Line Manager, the request has to be forwarded to and signed off by Finance Department.

The authorised request should be sent to Waid Network Solutions who will then place the order on the Finance system and cross charge it to the relevant department.

As the company is predominantly a Microsoft Campus, Waid Network Solutions would prefer to only purchase Windows based tablets for staff. These will allow better compatibility with company systems and provide staff with access to resources which would otherwise not be available on other tablet devices (Apple). Therefore, only in exceptional circumstances, which need to be approved by one of the Directors, will any other device be purchased.

Once purchased, the tablet remains the property of Geason. We reserve the right to re-allocate it at any time and request a return to Waid Network Solutions for upgrades and service checks.

10.2 Purchasing Apps for mobile devices

Geason App Purchasing policy:

Option 1: The tablet device is configured with the Geason image. Geason will purchase all apps on your behalf through a central purchasing program in conjunction with the Finance team. Restricting App purchases and access to App stores. Only centrally purchased apps can be installed on the device.

All requests for Apps should be made to Waid Network Solutions in writing. These will then be assessed and if approved, the app will be purchased and installed.

- This also applies to free apps.

Option 2: For legacy Apple iPad devices: The tablet can be set up and configured by the individual staff member, however, you agree to make all your own purchases at your own cost. No claim can be made against your department, Geason or to petty cash for recompense.

- This option allows access to the App stores and all purchases are the individual's responsibility.
- At no time will Geason refund the cost of these purchases.
- The tablet device remains the property of Geason, although you would own the apps installed on it. This means you would be able to transfer those apps to another device.

Only Windows based tablets are purchased and supported by Waid Network Solutions to ensure optimum compatibility, they will also be centrally managed by Waid, negating the requirement to make individual app purchases at personal cost.

Apple iPads are currently supported in the Curriculum, but must all be configured with the Geason image and all App purchases must be made through the authorised Geason account using Apple Configurator. Purchases made by individuals are not licensed for use on company devices. When the time comes to replace / upgrade the Apple devices, a decision will be made regarding their replacement on the basis of ease of support / benefits to teaching and learning / management and scalability.

11.0 UNIFIED COMMUNICATIONS

Geason has invested in a Unified Communications System – it differs from a traditional telephony system by offering additional modes of communications.

The system currently deployed across the company is Microsoft Lync Unified Communications, which is to be rebranded as Skype for Business by Microsoft.

The system offers the following functionality;

- SIP (Session Initiation Protocol) trunk connectivity (A Voice over Internet Protocol for streaming media and unified communications)
- Voice over LAN (Local Area Network instead of requiring a traditional telephone line)
- Extension number for every member of staff
- Instant Messaging
- Video Conferencing
- Call Conferencing
- Desktop sharing / collaboration
- Extension Mobility
- Presence Status
- Voicemail
- Call groups

Staff have access to the full set of features, Students are not allocated Voice features.

11.1 Telephone Profile / Devices

All members of staff will have a unique Lync Communications profile - this will enable them to access the company's communications system and use MS Lync (Skype for Business) for instant messaging, video conferencing (web cam dependent), desktop sharing, collaboration, presence, call conferencing. All staff will have their own telephone extension number instead of several members of staff sharing one number.

Office based staff will be given an appropriate device to suit their needs in line with the company's supported devices, any device requested other than these must have a supported business case and any additional costs compared to standard equipment, will be cross charged to the appropriate department.

Staff with a company issued smartphone will be able to have their work number associated with their mobile via the Lync app for smart phones.

The use of profiles will enable extension mobility for out of office working. All mobile company devices, (laptops and tablets) will be configured to allow off site working. Lync will have full functionality as long as you have sufficient internet connectivity. (Wireless, Ethernet or 4G).

12.0 USB Mass Storage Policy

USB memory sticks and External Hard Drives have become increasingly popular because of their small physical size and large storage capacity. This has made them very convenient devices for carrying files from one place to another. However, these very features have introduced new information security risks which Geason aims to mitigate through the controlled / restricted use of USB memory sticks.

USB and Mass storage devices are inherently vulnerable for a variety of reasons;

- Loss of information – a memory stick, like a computer, is susceptible to data loss or failure and less likely to be backed up on secure network storage facilities.
- Potential breach of confidentiality – if the memory stick is lost or stolen and is not encrypted, the data can be accessed by whoever gains access to the device.
- Physical loss – being so physically small the memory stick can easily be lost or damaged.
- Corruption of data - if the memory stick is not removed properly from a computer, corruption can occur, especially if moving between an Apple and a Windows device.
- Virus transmission – memory sticks can be used introduce viruses or harmful executable scripts onto a computer network.

12.1 Reducing the risk of data loss.

There are two main ways of preventing data loss associated with USB devices:

- Avoid physically carrying such information on highly portable devices, use Cloud services instead.
- Encrypt all portable devices containing confidential, sensitive & Person Identifiable Data.

Avoidance

Confidential, Sensitive and Person Identifiable Data must not be stored or carried on non-encrypted memory sticks. Staff should use other secure methods for carrying such information:

- Instead of USB devices, store information in secure network locations, i.e. the shared ‘H’ drive. Your departments ‘H’ drive folder can be access on any Geason networked computer.
  Use your personal Z drive storage space on the company network.
- Use the secure e-mail system either within the Geason network or via Office 365.
- Only work on encrypted Geason issued laptop computers outside of company.
- Use the company secure OneDrive cloud Storage solution.

Encryption

Where a need has been identified and agreed with a Line Manager that an encrypted memory stick is required to carry confidential, sensitive or PID, a request must be made via Waid Network Solutions Support desk for a Geason Computer Services approved encrypted device.

An encrypted memory stick allows information to be stored but renders the information undecipherable unless the correct password is entered. Encrypted memory sticks will be issued to specifically named members of staff for their professional use. They must not share the device with other persons as this would require sharing the encryption password. They must not share or disclose the password to other persons.

Confidential, sensitive or PID carried on encrypted memory sticks must not under any circumstance be placed on non-Geason issued computers.

Such information must always remain on the encrypted device and be immediately transferred onto user's departmental 'H' drive files and deleted from the encrypted memory stick once no longer required to be on the device.

An asset register will be maintained of all encrypted memory sticks issued. All issued encrypted memory sticks remain the property of Geason and must be returned when staff leave employment with Geason or no longer need to use such a device.

Student USB Devices

USB ports on Geason computers will be disabled for mass storage devices, any USB mass storage devices connected to a Geason computer will not be recognised.

It is highly recommended that Students save their work to their secure OneDrive rather than use USB devices. This will allow secure remote access via internet connection.

14. Backup Policy

Geason has a comprehensive backup solution which covers all shared network drives, staff home drives, student home drives, databases, systems and servers.

The backups are configured as follows:

- An image backup is performed of each server every week night (Monday through to Friday).
- We have 20 restore points which gives us a month (working days) of restore points.
- Backups are stored on a NAS storage array in another part of the company.
- A copy backup is created and this is continuous.
- For archival purposes a monthly, quarterly and yearly backup is stored.

Definitions

System Administrator

For the purposes of this policy, the System Administrator is the person with delegated management of information systems in any particular situation. System Administrators would normally have operational management responsibility within their department or be directly delegated by a person with operational management responsibility.

Guidelines

Devices / Workstations include:

Laptops, desktops, smartphones, tablets and authorised home workstations accessing the Geason network.

Geason members include:

Employees, students, volunteers, trainees, visitors and other persons under the direct control of Geason.

Information System

For the purposes of this policy Information System refers to all electronic systems for the management of information.

IT Security Coordinator

Nominated member of Computer Services Team – Primarily Systems and Servers Engineer, in the absence of him, the Computer Services Supervisor.

IT

For the purposes of this policy, IT products/services are defined as all types of technology and associated resources which relate to the capture, storage, retrieval, transfer, processing, communication or dissemination of information through the use of electronic media. It encompasses all resources required for the implementation of information technology, namely hardware, software, facilities and services.

License Agreement

These are the terms and conditions under which software vendors are prepared to provide software for use by Geason, it includes definitions of acceptable use and the number of concurrent installations we are entitled to, but does not necessarily imply ownership.

Security violation

A security violation includes one or more of the following acts;

- Unauthorised access to and/or disclosure of secure information.
- Unauthorised communication with or use of computing equipment, without necessarily causing damage.
- Enabling unauthorised access to computing equipment and IT systems.
- Distributing information that may encourage or lead others to attempt unauthorised access to computing equipment and IT systems.
- Damaging, contaminating, destroying, erasing or rendering meaningless data contained on computer equipment, including the introduction of computer viruses.
- Fraudulently obtaining a financial or other advantage or causing a detriment to another by the manipulation of data.

Standard

An essential requirement to the implementation of a specific policy. Compliance with standards is mandatory.