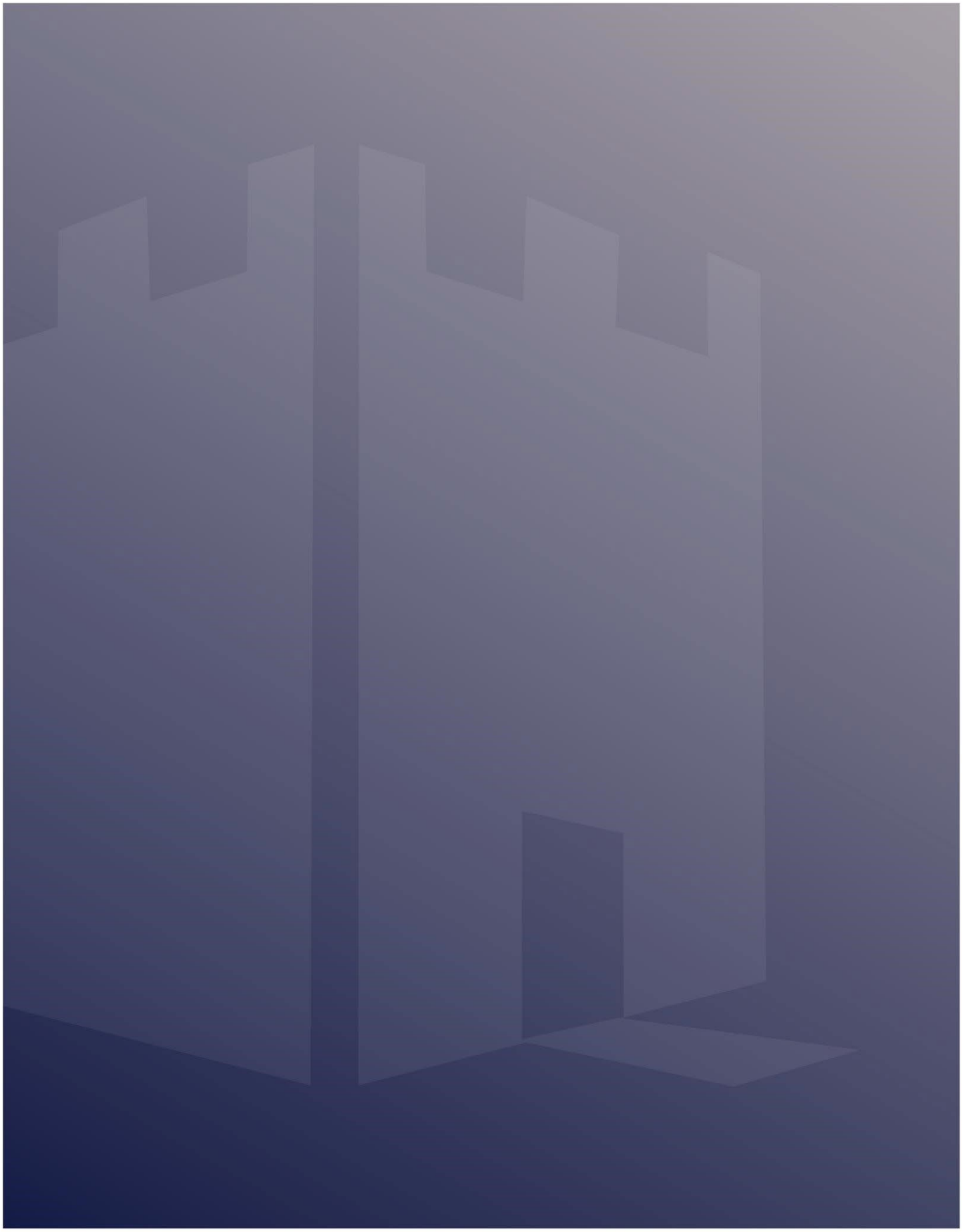
PONTEFRACT
ACADEMIES TRUST

Information Security



Summary:

The Information Security policy outlines Pontefract Academy Trust's organisational security processes and standards. The policy is based on the sixth principle of the UK GDPR which states organisations must protect personal data against unauthorised loss by implementing appropriate technical and organisational measures.

Author	Lead Governance Officer		
Applies to: (please check as appropriate)	Staff ✓	Pupil	Community
Ratifying Committee(s):	Audit and Risk Committee		
Available on:	Compliance Library ✓	Website ✓	
Date of Approval:	04/07/2025		
Date of Next Formal Review: (ensure this is aligned to committee meeting dates)	02/07/2027		
Review Period:	Every 2 years		
Status:	Non-statutory		
Owner:	**Pontefract Academies Trust**		
Version:	1.0		

Document Control

Date	Version	Action	Amendments
February 2025	01	New Policy	New policy based on Veritau's model Information Security policy, with reference to Cyber retained. Data protection content, including SAR/FOI process transferred to Data Protection & Data Breach Recovery Policy
September 2025	1.1	Reviewed by North East Business (and Cyber) Resilience Centre	i) New sections added: Purpose and objectives, roles and responsibilities, policy review, security of information, intellectual property, data security and email ii) Risks associated with users failing to comply with the policy added to roles and responsibilities and data breaches sections. iii) Software downloads section updated to specify (a) the Trust will ensure all software is properly licenced, recorded in an inventory and scanned with virus detection software. (b) Users must not use unauthorised/un-logged software, software must not be modified or pirated and users must not introduce or knowingly transmit vulnerabilities, malware etc.

Contents

1. Introduction

The Information Security policy outlines Pontefract Academy Trust's organisational security processes and standards. The policy is based on the sixth principle of the UK GDPR which states organisations must protect personal data against unauthorised loss by implementing appropriate technical and organisational measures.

To ensure we meet our legal obligations, personal data should be protected by the security model known as the 'CIA' triad. These are three key elements of information security:

- **Confidentiality** – only authorised people should have access to information.
- **Integrity** – information should be accurate and trustworthy.
- **Availability** – authorised people should have access to the information and systems they need to carry out their job.

The Information Security policy applies to all personal data, regardless of whether it is in paper or electronic format. It should be read alongside the other policies within our information governance policy framework, including data protection, records management, and acceptable use of systems.

Where this policy refers to the Trust it will be referring to information held and processed all Trust schools in addition to that of the central team.

2. Purpose and Objectives

The purpose and objective of the Information Security policy is to:

- Protect and preserve the confidentiality, integrity and availability of all client confidential data.
- Maintain demonstrable Information Security competence in order to achieve the objectives of the security management system.
- Protect information in line with the results of the latest risk assessment through regular review of the perceived organisational threats, vulnerabilities and impacts.
- Ensure all risk that exceeds the identified organisational risk appetite is accepted, treated or transferred in accordance with the organisational risk

3. Roles and Responsibilities

This policy and its appendices apply to our entire workforce. This includes employees, governors or trustees, contractors, agents and representatives, volunteers and temporary staff working for, or on behalf of, the school. Individuals who are found to knowingly or recklessly infringe this policy may face disciplinary action.

Overall responsibility for ensuring that we meet the statutory requirements of any legislation lies with the Board of Trustees. The following roles will have day-to-day responsibility for information security management and providing the necessary assurance to the Board.

Executive Leadership Team

The Executive Leadership Team is responsible for ensuring compliance with this policy and ensuring that effective information security practices are in place across the organisation. The Executive Leadership Team also responsible for risk management and will ensure that staff are appropriately trained in information security.

Headteachers

Headteachers are responsible for the security and maintenance of the data/information in their school and for ensuring that other staff members use the information safely and responsibly.

All staff

All staff, including governors or trustees, contractors, agents and representatives, volunteers, and temporary staff working for or on our behalf, will be responsible for information security in accordance with this policy.

Failure to comply with this policy could result in breaches of information security laws. All users can be held individually liable for their actions, as Pontefract Academies Trust could be held liable for actions carried out by authorised users.

4. Related Policies

The Information Security policy should be read in conjunction with the following:

- Data Protection and Data Breach Recovery Policy
- Data and Cyber Security Breach Prevention and Management Plan.
- Acceptable Use Policy – Pupils, Parents and Carers
- Acceptable Use Policy – Workforce.
- Records Management Policy.

5. Access Control

We will maintain control over access to the personal data that we process. These controls will differ depending on the format of the data and the status of the individual accessing the data.

Manual Filing Systems

Access to manual filing systems (i.e. non-electronic systems) will be controlled by a key management system. All files that contain personal data will be locked away in lockable storage units, such as a filing cabinet or a document safe, when not in use.

Keys to storage units will be stored securely. Access will only be given to individuals who require it to carry out legitimate business functions.

Electronic Systems

Access to electronic systems will be controlled through a system of user authentication. Individuals will be given access to electronic filing systems if required to carry out legitimate functions. All electronic systems require authentication by username and unique password.

Individuals will be required to regularly change their password and Headteachers will be required to inform the IT provider if any user name requires suspending when an individual is on long term absence or when an individual leaves our employment.

Individuals should ensure they use different passwords for different systems to ensure if one system is compromised, that does not lead to other systems being accessed.

Software and Systems Audit Logs
We will ensure that all major software and systems have inbuilt audit logs, wherever possible, so that we can ensure it can monitor what users have accessed and what changes may have been made. Although this is not a preventative measure it does ensure that the integrity of the data can be assured and deters individuals from accessing records without authorisation.

External Access
On occasions we will need to allow individuals who are not part of our workforce to have access to systems. This could be, for example, for audit purposes, to fulfil an inspection, when agency staff have been brought in, or because of a partnership arrangement with another educational establishment. Headteachers, or if unavailable an appropriately senior member of staff, is required to authorise all instances of third parties having access to systems. The Executive Leadership Team can authorise access to central or Trust wide systems.

We will maintain an access log, detailing who has been given access to what systems and who authorised the access.

6. Security of Information

All records, especially those containing personal data, will be stored securely to maintain confidentiality, whilst also keeping information accessible to those authorised to see it. Electronic records will have appropriate security and access controls in place, and systems will have robust audit functions in place wherever possible. Permission to access data will be granted by the Information Asset Owner.

Should paper records need to be kept, they will be stored in secure, lockable storage areas with restricted access.

When sharing or transferring records containing personal information, we will ensure appropriate transmission security controls are in place.

Employees should note that attempts to access unauthorised information is a Computer Misuse Act offence.

For further information regarding how the Trust will comply with Data Protection principles, please see the Data Protection and Breach Policy.

7. Physical Security

We will maintain high standards of physical security to prevent unauthorised access to personal data. We will maintain the following controls:

Clear Desk and Screen Policy
Individuals will not leave personal data on desks, or any other working areas, unattended and will use the lockable storage units provided to secure personal data when not in use.

Unattended computer terminals must be turned off or locked when unattended.

Alarm System
All Trust premises will maintain a security alarm system in our premises so that, when the premises are not occupied, an adequate level of security is still in operation.

Building Access
External doors to the premises will be locked when the premises are not occupied. Only authorised individuals will be key holders for the building premises. Headteachers will be responsible for authorising key distribution and will maintain a log of key holders.
Internal Access
Internal areas which have restricted access will be kept locked and only accessed through pin pads, fobs or keys.

Visitor Control
Visitors to each school will be required to sign the visitor book or on the visitor management system. They may also be asked to provide information to help provide support in the event of an emergency. This may be either in paper or electronic format. Visitors will be escorted throughout the school and will not be allowed to access restricted areas without appropriate supervision.

Secure Disposal
We will ensure that all personal data is securely disposed of in line with our Records Management Policy and retention schedule. Hard copy information will be securely destroyed by shredder or a confidential waste provider. Electronically held information will be deleted automatically with retention periods built into the system wherever possible. Otherwise, manual review and deletion will take place at least annually.

Redundant computer equipment will be disposed of in accordance with the Waste Electrical and Electronic Equipment (WEEE) Regulations and through secure and auditable means.

8. Environmental Security

As well as maintaining high standards of physical security to protect against unauthorised access to personal data, we must also protect data against environmental and natural hazards such as power loss, fire, and floods.

It is accepted that these hazards may be beyond our control, but we will implement the following mitigating controls:

Back Ups
We will regularly back up our electronic data and systems and carry out tests to ensure that they restore correctly. These backups will be held in a different location to the main server or held off-site by an external provider. This arrangement will be governed by a data processing agreement. Should our electronic systems be compromised by an environmental or natural hazard then we will be able to reinstate the data from the backup with minimal destruction.

Fire-proof Cabinets
We will aim to only purchase lockable data storage cabinets that can withstand exposure to fires for a short period of time. This will protect paper records held in the cabinets from any minor fires that break out on the building premises.

Fire Doors
Areas of the premises which contain paper records or core electronic equipment such as server boxes, will be fitted with fire doors so that data contained within those areas will be protected, for a period of time, against any fires that break out on the premises. Fire doors must not be propped open unless automatic door releases are installed.

Fire Alarm System
We will maintain a fire alarm system at our premises to alert individuals of potential fires and so the necessary fire protocols can be followed.

9. Systems and Cyber Security

We will protect against hazards to our IT network and electronic systems. It is recognised that the loss of, or damage to, IT systems could affect our ability to operate and could potentially endanger the safety of our pupils and workforce.

We will implement the following security controls to mitigate risks to electronic systems:

Software Download Restrictions
Employees do not have administration rights to enable them to install software. Our IT provider will vet software to confirm its security certificate and ensure software is not malicious and will ensure all software is properly licenced, recorded in an inventory and scanned with virus detection software. Our IT provider will retain a list of trusted software so that this can be downloaded on to individual desktops without disruption.

Users must not use unauthorised/un-logged software, software must not be modified or pirated and users must not introduce or knowingly transmit vulnerabilities, malware etc.

Firewalls and Anti-Virus Software
Our IT provider will ensure that firewalls and anti-virus software are installed on electronic devices and routers. Staff will update firewalls and anti-virus software when updates are available and when advised to do so by our IT provider. Our IT provider will review our firewalls and anti-virus software on an annual basis and decide if they are still fit for purpose.

Cloud Computing
The Trust currently operates its email communications on Office365. Employees will not save any other records on cloud storage unless authorised to do so by their Headteacher. This should be in limited or exceptional circumstances (i.e. google drive or one drive). Employees can access email communications on their personal or work mobile telephone only if it has a pin code or bio recognition and adheres and adheres to the Office365 security policy.

Shared Drives
The Trust maintains a shared drive on our servers. Whilst users are encouraged not to store personal data on the shared drive it is recognised that on occasion there will be a genuine business requirement to do so.

The shared drive will have restricted areas that only authorised users can access. Information held within shared drives will still be subject to our retention schedule.

Phishing Emails
To avoid our computer systems from being compromised through phishing emails, users are encouraged not to click on links sent to them in emails when the source of that email is unverified. Employees will also take care when clicking on links from trusted sources in case those email accounts have been compromised. Users will check with our IT provider if they are unsure about the validity of an email and must immediately inform our IT provider if they have clicked on a suspicious link. We will ensure staff have received adequate training to be able to recognise such emails.

For further information regarding cyber security, please see the Data and Cyber Security Breach Prevention and Management Plan.

10. Communications Security

The transmission of personal data is a key business need and, when operated securely is a benefit to us and pupils alike. However, data transmission is extremely susceptible to unauthorised and/or malicious loss or corruption. We have implemented the following transmission security controls to mitigate these risks:

Sending personal data by post
When sending special category data by post we will use Royal Mail's 1st Class Recorded postal service. Envelopes should be marked "Private and Confidential, to be opened by the addressee only".

Individuals will double check addresses before sending and will ensure that the sending envelope does not contain any data which is not intended for the data subject.

If the envelope contains information that is thought to be particularly sensitive, individuals are advised to have the envelope double checked by a colleague.

Sending special category data by post
When sending special category data by post we will use Royal Mail's 1st Class Recorded postal service. Individuals will double check addresses before sending and will ensure that the sending envelope does not contain any data which is not intended for the data subject. If the envelope contains information that is thought to be particularly sensitive, individuals are advised to have the envelope double checked by a colleague.

Sending personal data by email
Where personal data is emailed external to the Trust the subject header should start with [Encrypted] to secure it from interception. The email requires authentication at the recipients end regardless of their system.

Individuals will always double check the recipient's email address to ensure that the email is being sent to the intended individual(s). Use of autocomplete should be strongly discouraged.

Files shared as email attachments must be password protected. Passwords may be shared with recipients via a separate text, phone call or email.

Where special category data is being shared, employees should be extra vigilant.

When sending emails to a large number of recipients, such as a mail shot, or when it would not be appropriate for recipients to know each other's email addresses then we will utilise the Blind Copy (BCC) function.

Exceptional Circumstances
In exceptional circumstances we may wish to hand deliver, or use a direct courier, to ensure safe transmission of personal data. This could be because the personal data is so sensitive that the usual transmission methods would not be considered secure, or because the volume of the data that needs to be transmitted is too big for usual transmission methods.

Data Security and Email

All incoming and outgoing emails will be automatically scanned for viruses and malware to prevent the transmission of malicious content. Users must not bypass or disable these virus scanning measures, nor send or receive copyrighted material via email unless they have the appropriate permissions or licences. This includes documents, software, images, and other digital content.

Emails sent or received on Trust systems may be monitored and stored in compliance with data retention policies and relevant legislation. The Trust reserves the right to review emails for security purposes, compliance with policy, or in response to legal requests.

All outgoing emails should include the Trust's legal disclaimer, outlining confidentiality and legal obligations. The disclaimer should automatically be appended to all emails sent via Trust email systems.

The Trust employs spam filtering software to identify and block unsolicited, irrelevant, or harmful emails. Users are advised not to interact with suspicious emails and should report them to IT.

Sending or receiving inappropriate, offensive, or illegal content via email is strictly prohibited. This includes but is not limited to content that is discriminatory, defamatory, harassing, or in violation of UK law. Violations may lead to disciplinary action and legal action.

11. Intellectual Property and Software Use

The Trust and users must comply with relevant IP laws, including copyright and trademark protections, and avoid any illegal use or distribution of software.

The Trust acknowledges that third-party software and IP remain the exclusive property of their creators or licensors, unless the Trust has acquired ownership or developed the IP in-house.

All software used within the Trust must be properly licensed. Users must ensure that software is used in accordance with its licence agreement and must not exceed the scope of granted permissions. Users are prohibited from downloading, modifying, or distributing software without the owner's consent. Reverse-engineering or circumventing licence terms is also forbidden.

The Trust may retain ownership of internally developed IP, or take ownership of commissioned work, as specified in contracts.

The Trust will monitor software usage to ensure compliance with this policy.

12. Data Breaches

All actual and suspected breaches of security or confidentiality are to be reported in accordance with the Data Breach Procedure set out in the Trust's **Data Protection and Data Breach Recovery Policy**.

Article 33 of the UK GDPR requires data controllers to report breaches of personal data to the Information Commissioner's Officer; and sometimes the affected data subject(s), within 72 hours of discovery if the incident is likely to result in a risk to the rights and freedoms of the data subject(s).

Failure to comply with this policy could result in breaches of information security laws. All users can be held individually liable for their actions, as Pontefract Academies Trust could be held liable for actions carried out by authorised users.

13. Business Continuity

We will ensure that we have business continuity plans in place to ensure we can continue normal business in the event of a security incident or disaster.

14. Policy Review

The **Lead Governance Officer** is responsible for ensuring this policy is kept up to date.

The **Executive Leadership Team** will review this policy **every two years**. It will be re-presented to the **Audit and Risk Committee** for approval, in the event of any material changes.

Pontefract Academies Trust reserves the right to amend the policy at any time.

If you have any comments or questions regarding this policy, or spot any errors, please email clerk@patrust.org.uk.

Appendix A: Remote Working Policy

Introduction

On some occasions our workforce may need to work at home or remotely. Where this is the case, the workforce will adhere to the following controls:

Lockable Storage

Individuals will ensure they have lockable storage to keep personal data and our equipment safe from loss or theft.

Individuals must not keep personal data or our equipment unsupervised at home for extended periods of time (during periods of annual leave).

Individuals must not keep personal data or our equipment in cars if unsupervised.

Private Working Area

Individuals must not work with personal data in areas where other individuals could potentially view or even copy the personal data (for example on public transport).

Individuals should also take care to ensure that other household members do not have access to personal data and do not use our equipment for their own personal use.

Trusted Wi-Fi Connections

Individuals will only connect their devices to trusted Wi-Fi connections and will not use 'free public Wi-Fi' or 'Guest Wi-Fi'. This is because such connections are susceptible to malicious intrusion.

When using home Wi-Fi networks individuals should ensure that they have appropriate anti-virus software and firewalls installed to safeguard against malicious intrusion. If in doubt, assistance should be sought from our IT provider.

Encrypted Devices and Email Accounts

Individuals will only use encrypted devices issued by ourselves to access school data, unless authorised by the SIRO in accordance with the acceptable use policies.

Individuals will not use personal email accounts to access or transmit school related personal data. Individuals must only use school issued, or school authorised, email accounts.

Data Removal and Return

Individuals will only take personal data away from our premises if this is required for a genuine business need. Individuals will take care to limit the amount of data taken away from the premises and will ensure that all data is returned to our premises either for re-filing or for safe destruction. Individuals will not destroy data away from the premises as safe destruction cannot be guaranteed.