ICT Policy 2025

FREQUENCY OF REVIEW:	**Annually**
COMMITTEE:	**Audit & Risk Committee**
RATIFICATION DATE:	**2nd December 2025**
DATE OF NEXT REVIEW:	**Autumn 2027 unless there is a material change**

Signed…… Date …….

Chair of Audit & Risk

Signed …….. Date …….

CEO

Contents	Page
Aims	3
Delegation	3
Email/Teams/Other Communication	5
Social media	8
Personal Equipment	8
Physical and Environmental Security	9
Information Sharing	10
Information Security	10
Removable/External Media Device	11
Passwords	12
Data Security	13
Data Protection	13
Cyber Security	14
CCTV	15
IT Training	16
Network	16
Internet Access	18
Internet Monitoring	19
Acceptable Use of IT Policy (AUPs)	20
Information Sharing Policy – Appendix 1	26
School Information Security Policy – Appendix 2	32
Password Policy – Appendix 3	55
Cyber Security Policy – Appendix 4	60

1. Aims

The Trust recognises that staff and students have access to appropriate information and communication technology (ICT) infrastructure, equipment, training, tools and support which helps them to carry out their work efficiently and effectively.

This policy aims to provide TrustEd Schools Alliance with guidance in managing the infrastructure, resources and tools provided to staff and students, and to ensure that staff use of these resources is secure and appropriate.

This policy will help to deliver the following.

- Ensures consistency: Having a structured ICT policy in place ensures that all staff and students are on the same page in terms of technology usage.
- Protects data: Implementing a policy helps in safeguarding sensitive information and data within the school network.
- Promotes responsible technology use: By outlining guidelines, students are guided on how to responsibly use technology for educational purposes.
- Addresses cybersecurity concerns: With the increasing threat of cyber-attacks, an ICT policy helps in establishing preventive measures to protect school assets.

By adhering to this policy, we can maintain a secure and efficient work environment. Please take some time to review the policy and make sure you are familiar with it.

2. Delegation

Trustees and Central team	• Endorse and review overarching ICT Policy • Contribute to the 5 Year ICT Strategy • Familiar with legislative requirements regarding storage and data protection • Understand policies and procedures related to social media, communication, data protection and internet safety for all stakeholders • Approve ICT budget • Ensure systems are in place across the Trust to communicate appropriately • Ensure systems are in place that mean access to network is appropriately managed by having access in place. • Review Trust level systems, budgets and contacts for ICT
Headteacher (and CEO for Trust central)	• Ensure access to network is appropriately managed by having access in place. • Review and adjust the ICT Policy for school use. • Draw up and review any 5-year ICT strategy for school • Deliver an annual refresher programme • Review and implement effective school level systems, budgets and contracts for ICT

	• Understand and ensure the school complies with legislative requirements regarding storage and data protection • Ensure school processes align with security and training requirements.
LGB	• Review and adopt the ICT Policy for school use. • Adopt a 5-year ICT strategy for school • Review any annual ICT refresh programme • Familiar with legislative requirements regarding storage and data protection
ICT Provider (eg SLA)	• Comply and align with ICT Policy • Supports effective systems across all the schools • Aligns with and ensures legislative requirements regarding storage and data protection • Ensures secure systems are in place to protect privacy and personal information • Review devices and equipment whether they need updating or disposing • Work with the Trust to advice on systems, devices and software upgrades
Technical Support	• Ensure effective day to day running of ICT across the school • Advises Heads on local solutions and puts them into practice. • Comply with ICT Policy and any SLA Expert in legislative requirements regarding storage and data protection • Reviews and implements systems across all the schools and ensure systems are backed up and secure • Maintain equipment and access person for staff and students. • Maintain and review infrastructure across the site • Update the asset register • Troubleshoot issues with network/devices and printers
External Contractors	• Comply with ICT Policy • Familiar with legislative requirements regarding storage and data protection • Permission required to access data and systems through a user level agreement.
Staff	• Implement and follow policy • Ensure pupils in their charge follow ICT expectations as outlined in the policy and • Keep up to date with training, including an annual refresher on cyber security. • Sign and comply with the user agreement.

3. Use of Email/Teams/Other Communication/Video Conferencing Technologies

Email/Microsoft Teams and other communication technologies are a valuable business tool. However, staff must be aware that emails, saved Teams conversations and other electronic messages have the same legal status as other documents and in particular email attachments may be shared very quickly to readers across the world. Remember that contents of emails and/or any saved conversations using Teams or other communication technologies can be disclosed when requested under the Freedom of Information Act 2000.

Good management of staff mailboxes is essential for proper records management. It is also important as size of files and storage can easily get out of control, costing the school time and money. The school reserves the right to impose mailbox quotas on any or all staff if storage becomes an issue.

The following conditions must be followed:

Acceptable – Staff must

- Use of encrypted email to exchange personal and sensitive data to external parties
- Ensure that a generic/team email account is only used in appropriate circumstances such as information which is relevant to each staff member and not using the account to send confidential information which should only be shared with certain staff members
- Ensure they send an email to the correct person, always double check the recipient. They must also limit the number of recipients of the email to people who require it to do their job or are bona fide recipients
- Limit the amount of personal data in the body of the email or in attachments to only that which is needed and/or anonymise where possible
- Where possible provide a link to documents in an email to reduce the number of copies held of a document
- Remind the recipient, if any sensitive/confidential data, of their responsibility for the security and confidentiality of that data
- When confidential/sensitive data is received by email it should be deleted from the email system as soon as possible and filed/secured appropriately, either electronically or on paper.
- When “forwarding” emails or using the “reply all” facility consider whether the content is suitable for everyone on the list of recipients, as confidential/sensitive data could be sent in error
- Use a dedicated room when using Teams video meetings
- Always use the BCC field when you are emailing a group of external email addresses
- Accessing emails on personal devices will use of MFA (Multi Factor Authentication) for staff and privileges accounts.

Unacceptable – Staff must not

- Use their school email address for personal use, e.g. register it on a non-work website
- Respond to suspicious (spam) emails, if they have any doubts about who has sent the email then the email should not be opened or replied to
- Click on any untrusted web links detailed in a suspicious email or open any attachment as they may contain viruses

- Use email/Teams/other communication tools to send personal messages in work time and/or that are inappropriate, abusive and malicious
- Access an email/Teams/other communication tool for which they are not authorised
- Use email/Teams/other communication tools for any private gain including running a business or associated advertising
- Keep received, sent or deleted sensitive/confidential data on the email/Teams/other communication tools longer than necessary
- Send or forward confidential information outside the school without appropriate security in place including strong passwords and encryption
- Forward School emails to their own personal email address
- Use the Schools email/ Teams/other communication tools in any way that could damage the reputation of the school and/or its staff
- Represent their own opinions as those of the school
- Send emails that infer that they are an official document when that is clearly not the case
- Click on any links or follow any instruction in an email received from an unknown source. Emails of this nature can contain malicious content
- Use their personal email for school business

Use of SMS (text)
For school business, staff should be aware that any communications with colleagues and/or customers are business records and therefore they should be managed accordingly.

Please note SMS is **NOT** a secure means of communication and therefore should:

- Only be used where there are no other viable alternatives
- Not be used to communicate personally identifiable information

Use of Video Conferencing Technology (VCT)
School staff are increasingly using video conferencing technologies to meet and/or collaborate with third parties. The school preferred choice of VCT should be Microsoft Teams and should always be used, unless they are joining third party meeting, and there is no alternative.

If transcription services are required, then staff must use MS Teams by default. If other solutions are being considered, these need to be checked and the ICT Technical team or the school SBM.

Security & Monitoring

Email Security
Private, confidential, personal or sensitive information should not be revealed. When unsure whether content is suitable for sending by external email ask yourself "*if this information was about me, my family or my company would I want the information available for anyone to see?*"

- Secure email systems such as TLS enabled mail to exist for the secure transfer of personal / sensitive information to external bodies and therefore should be used.

- Before sending emails, staff must consider whether it is essential to include full names in external emails where abbreviations or reference numbers could be used, so that individuals cannot be identified.

An email should be treated in the same way as a paper record regarding retention or deletion.

Email Monitoring

- The school reserves the right to access, read and monitor emails/Teams messages or other electronic communications that are transmitted over School networks or stored on School equipment.
- Monitoring of activity will take place, in line with Lawful Business Practice Regulations 2000 and only when it is appropriate to do so.
- Misuse of email/Teams/other electronic communication technologies could result in temporary or permanent withdrawal of access and may be dealt with under the disciplinary process of the school. Separate legal proceedings may be necessary including seeking prosecution under the Computer Misuse Act 1990.
- Email/saved Teams or other work electronic messages may need to be accessed by management when staff are absent from work, and signing this policy will constitute acceptance of this.

Staff should also note:

- **Out of office** - 'Out of Office' assistant should always be used for planned absence. All out of office messages should contain as a minimum the statement *"If this is a request under the Freedom of Information Act or similar legislation, please send your request to the school office*. Where absence is unplanned employees should activate their out of office message via a works mobile device or by Web Mail. If this is unachievable managers will ask ICT Technician to activate the 'Out of Office' message.
- **Outlook calendar** - With the move to Office 365 employees should not save personally identifiable data in the subject of their outlook calendars.

Key Messages to Staff

- All emails sent and received using the school's system will be automatically scanned and filtered
- Employees emails/Teams messages and other electronic communications will be monitored if it is deemed appropriate to do so. This will include any private emails
- Misuse of email/Teams/other communication technologies can lead to disciplinary or criminal proceedings
- All emails/Teams and other messages communicated electronically on School systems remain the property of the school and may need to be disclosed under the Freedom of Information Act 2000
- Staff should minimise the amount of personally identifiable data in emails

- When sending an email to many recipients' personal email addresses, these email addresses must be put in the BCC field

4. Social Media

Members of staff should make sure their use of social media, either for work or personal purposes, should always be appropriate. See staff Code of Conduct for additional information.

You should exercise caution when using social networks. You should not communicate with pupils over social network sites. You must block unwanted communications from pupils. You are personally responsible for what you communicate on social media.

As we continue to enhance our online presence, it is crucial to maintain professional conduct across social networks. To ensure that we represent ourselves and our schools in the best light, please adhere to the following guidelines:

- Confidential Information: Never share sensitive school information, employee details, or school data.
- Professionalism: Always maintain a professional tone. Avoid posting inappropriate content or engaging in online disputes.
- Personal Views: Clearly differentiate personal opinions from professional statements, especially when it relates to place of work.
- Respect: Be respectful of colleagues and other individuals. Online harassment or disrespectful comments will not be tolerated.
- Network Security: Beware of phishing scams and insecure networks when accessing your accounts.

Note: It is a requirement for all schools to complete Social Media searches for any shortlisted candidate. The schools in TrustEd all comply with this requirement.

5. Personal Equipment

It is prohibited to bring in personal equipment (eg laptops / iPad) in schools (excluding mobile phones). Personal equipment would raise

- Safety concerns: Bringing in personal equipment may pose safety risks to students and staff members.
- Distraction: Personal devices can distract students from focusing on their studies
- Cybersecurity: Personal devices may expose the school network to cybersecurity threats and compromise sensitive information.
- Would not be tested as part of Portable Appliance Testing (PAT) and therefore not electrical compliant.

Please note mobile phones are prohibited in schools for pupil use, and any use by staff must be used discretely and away from any pupils. See Code of Conduct and Safeguarding Policies for additional regulations / requirements for mobile phone use.

6. Physical & Environmental Security

- All employees have a responsibility for the physical security of School's assets (including information) including securing their laptops, locking away sensitive information, etc.
- The school will be responsible for the provision of suitable physical, technical, procedural and environmental security controls in line with best practice such as ITIL (Information Technology Infrastructure Library – standard for IT service management) to prevent unauthorised access to, interference with, or damage to information.

Access Control

The management team have responsibility for authorising their staff to access information including IT networks, offices, secure filing cabinets etc. No School employee may access or attempt to access any information for which they have not been given authorisation.

The management team may remove access to information during periods of extended leave or sickness of more than 3 months. A review of employee's level of access to School information must be undertaken by their manager during supervision.

Additional security measures shall be implemented by data owners to control access to especially personal/sensitive School data.

To control access to information, care must be taken (within the constraints of new ways of working) as to the physical positioning of desks and equipment used to view key personal, sensitive or confidential data. Desks used to process or view such data must be positioned away from doors/windows and public areas.

Managers must ensure appropriate access controls are in place for information processed in open plan offices. Adequate clear desk arrangements should be adhered to as outlined in this policy.

Physical security (equipment)

Desktop machines in public areas must be secured to protect against theft and/or unauthorised access.

Multi-functional devices (MFD) machines must be sited appropriately in areas where sensitive information can be handled.

Backup equipment and media must be sited at a safe distance to avoid damage from a disaster at the main site(s) and must be subject to the same environmental and physical protection as the main system.

Leaving procedure

When staff leave the school, as part of the school's leavers procedure their manager is required to:

- Ensure that any information held in the leaver's One Drive, that is of importance to the school, is moved to a relevant network folder
- Request accounts to access systems to be deleted/disabled
- Ensure email accounts/contacts and membership of email group accounts are removed and, if appropriate, emails will be auto responded to providing alternative contact details
- Ensure leaver returns all work ICT equipment/data

Disposal of equipment

ICT equipment for disposal must be disposed of securely either by T&WC ICT or other reputable disposal company. ICT equipment no longer required must not be used by staff for personal use.

Third party access to systems

It is the responsibility of SBM/Headteacher in conjunction with ICT Technician to authorise third party access to resources and systems. User accounts and passwords will have to be created and where necessary relevant policies will have to be signed by the school and the third party prior to allow access.

It is the responsibility of the SBM/Headteacher to advise the ICT Technician as soon as the third-party access is no longer required.

7. Information Sharing

This policy is based on the requirements of the latest Information Commissioners Office (ICO) Data Sharing Code of Practice. The policy will help ensure any sharing is fair, transparent and in line with the UK Data Protection Act/UK GDPR 2018 and the rights and expectations of the people whose information is being shared.

Information sharing is the disclosure of data from one or more organisations to a third-party organisation(s), or the sharing of information between different parts of the school.

This policy covers the sharing of personal information on a systematic and exceptional basis.

Systematic Information Sharing – this involves the routine sharing of the same or similar information for the same person between a set number of organisations. Sharing ordinarily takes place under the conditions of an agreed information sharing agreement.

Exceptional Information Sharing – these are one off ad hoc decisions to share information
It is important to remember that data protection principles also apply to information shared **within** the school as well as sharing with external organisations.

Schools must comply with the Trust's Information Sharing Policy as attached as appendix 1

8. Information Security

Information can exist in many forms. It can be printed, written, stored electronically, transmitted by post, email, and fax or even spoken in conversations. The purpose of information security is to ensure that all information (including personal information) and associated processing systems are protected to an adequate level.

This policy sets out minimum standards and common acceptable use for confidentiality, integrity and availability of information to meet internal and legal requirements.

Confidently

Ensuring that information is accessible only to those authorised to have access.

Availability

Ensuring that authorised employees have access to information when required.

Integrity

The policy has been written to conform, where possible, to standards such as ISO 27001 (Information Security Management standard), HMG Data Handling Guidelines, Government Functional Standard (GovS 007: Security) and PCI-DSS (Payment Card Industry – Data Security Standard).

Schools must comply with the Trust's Information Sharing Policy as attached as appendix 2

9. Removable/External Media Use

Removable media (or storage) (eg USB stick) includes but is not necessarily limited to:

- The introduction of Office 365 has significantly reduced the need for removable media such as USB sticks, CD's and removable drives. Before staff use any removable media, they should contact their ICT Technician to investigate whether there are more secure alternatives to using these types of devices.
- High profile data losses highlight the importance of understanding how removable media should and should not be used.

Where staff have no other alternative but to use removable media they **must do/do not** do the following.

Acceptable

- Use for the shortest time and erase information after use.
- Only use encrypted removable/external media provided through authorised channels.
- Encrypt AND password protect ALL confidential information being transferred by these media
- Contact ICT Technician if there is any doubt as to the integrity of any removable media

- In the event of theft or loss of such media, it must be reported immediately in line with the schools Information Security Breach Procedure.

Unacceptable

- Never keep personal/sensitive data on removable media
- Never transfer confidential information from removable/external media to personal/private equipment
- Never leave these media in unsecure locations or lend the media to others
- Never use removable media as an archive in place of corporate backups
- Never use School removable media for personal files
- Never store files that can be considered inappropriate, e.g. sexually explicit images

If in exceptional circumstances removable media is required, then this should be approved by the SBM and/or Headteacher.

10.Passwords

Password management is an integral part of the school's information governance arrangements. This policy outlines the requirements associated with the use and management of passwords and complies with guidance from the National Cyber Security Centre (NCSC). This policy should be read in conjunction with the Schools Information Security Policy (SISP).

We all require passwords to access information held on a number of IT systems, mobile apps and websites. Using your passwords securely, in adherence to this policy, will help ensure adequate protection for the data you are accessing. The following areas need to be considered:

- How to choose a good password
- Password Protection
- Multiple Passwords
- Password Storage

Where there is an opportunity to use multi-factor authentication (MFA), to support password use, this functionality should be used.

How to choose a good password

Password requirements should follow the '12 x 4 Rule' and be/contain:

12 = 12 characters minimum length
4 = 1 lower case + 1 upper case + 1 number + 1 special character*

*A special character is a non-numeric or alpha character such as '£' or '!'

The National Cyber Security Centre (NCSC) suggests that passwords should include 3 random words to make it difficult to guess. This is in addition to incorporating the 12 x 4 rule. Examples here could be:

Rot2Big!dot75
4New8£ran9ear

There are a number of things to **avoid** when choosing a password, in the main these include (but not limited to) **not**:

- Using your user ID as part of your password
- Using the name of a family member, friend or pet
- Using personal information about you that can be easily obtained such as date of birth, phone number, vehicle registration number, etc.
- Use sequences, i.e. consecutive alpha/numeric characters, e.g. qwertym, 12345, etc
- Use words with just one number substitution, e.g. Passw0rd
- Using the same base word for your password and then changing one character to create a new one, e.g. old password – Miranda1! changed new password to Miranda2!
- Using common names such as days or months
- Using common place names particularly those near where you live/work, e.g. Telford, school name, etc

Schools must comply with the Trust's Password Policy as attached as appendix 3

11.Data Security

Data security is crucial in protecting sensitive information and preventing unauthorised access. The school should:

- Implement Multi-Factor Authentication: Require users to provide multiple forms of verification before accessing sensitive data, such as passwords, security questions, and biometric authentication.
- Regular Data Backups: Ensure that all data is regularly backed up and stored securely to prevent loss in case of a security breach or data corruption.
- Employee Training Programs: Conduct regular training sessions to educate employees on best practices for data security, such as recognizing phishing attempts and securely handling sensitive information.
- Regular Security Audits: Conduct regular security audits and assessments to identify potential vulnerabilities and weaknesses in the data security system, allowing for timely action to strengthen security measures.
- When sharing data work with 3rd party companies to plan data audits to review where the data is stored and who has access to it.

12.Data Protection

All personal information managed by the school is covered by the UK Data Protection Act 2018. This provides legislation as to how personal information may be used, stored, processed and shared. It contains seven principles that the school should conform to and also governs how information needs to be handled under certain circumstances.

- Lawfulness, fairness and transparency.
- Purpose limitation.
- Data minimisation.
- Accuracy.
- Storage limitation.
- Integrity and confidentiality (security)
- Accountability.

Staff must notify the school in case of a data breach. Please refer to the **Trusted Schools Alliance Data Protection Policy.**

Training – All staff must ensure they complete relevant data protection training and keep up to date with information governance related policies and guidance.

13.Cyber Security

The protection of information and communication technologies (ICT) within a school environment is paramount. This Cyber Security Policy aims to establish a framework for maintaining the security and integrity of digital resources, protecting personal data, and ensuring a safe digital environment for students, staff, and stakeholders. Schools must comply with the Trust's Cyber Security Policy as attached as appendix 4.

In the event of a cyber security incident:

- The IT department will initiate an immediate investigation.
- Containment measures will be implemented to prevent further damage.
- Affected individuals will be informed promptly.
- A report detailing the incident and response actions will be documented.
- Preventative measures will be revised to avoid future occurrences.

School Administration

The administration is responsible for:

- Ensuring the development and implementation of the cyber security policy.
- Ensuring adequate resources are allocated for cyber security measures.
- Overseeing cyber security training and awareness programs.
- Reviewing and updating the policy periodically.

IT Support

IT support is tasked with:

- Maintaining and securing the school's IT infrastructure.
- Implementing technical measures to protect against cyber threats including:
  - Use of anti-malware and firewalls
  - Regular patching and software updates
  - Secure configuration of devices and networks
  - Use of **Multi-Factor Authentication (MFA)** for staff and privileged accounts
  - Controls over user accounts and access privileges including a review of accounts and prompt removal of leavers
- Monitoring network activity for potential security breaches.
- Responding to and mitigating the effects of cyber security incidents.
- Back-ups are periodically tested with at least one back up kept offline
- Provide web filtering and monitoring of internet access to prevent access to malicious sites

Staff

All staff members must:

- Adhere to the cyber security policy and procedures.
- Participate in cyber security training and awareness programs.
- Report any suspicious activities or security incidents.
- Safeguard their login password.
- Use MFA where possible

Students

Students have the responsibility to:

- Follow the school's cyber security guidelines and rules.
- Respect the privacy and security of others.
- Report any cyber security concerns to a teacher or other school staff.

Anti-Virus

ICT Technician Responsibility

- It is the responsibility of ICT Technician to ensure appropriate anti-virus software is installed on all work desktop computers, laptops and tablets that connect to the school's network.
- ICT Technician is also responsible for sending updates to the anti-virus software.

Staff Responsibility

Staff must not:

- Not disable the anti-virus software, or software of a similar function or any automatic update facilities on school PC
- Inform ICT Technician if their anti-virus software appears to not be working or updating correctly
- Virus checks any media being used to transfer data from a laptop to another piece of school equipment
- Not knowingly distribute or otherwise be involved in virus, trojans, malware

Anti-virus software monitors staff internet use when at work, e.g. the software is checking for malicious websites.

14.CCTV

The use of CCTV in schools can help enhance security measures to ensure the safety of students and staff. When accessing CCTV footage, the school must

- Set Password Protection. Passwords must be unique and changing password regularly.
- Restricted Access. Limiting access to authorised personnel only
- Implementing multi-factor authentication. Implementing multi-factor authentication
- Regular Maintenance. Periodic system checks and updates
- Prompt response to system vulnerabilities
- Placement of visible signage indicating CCTV surveillance

15.IT Training

As part of our ongoing commitment to staff development, the school provide IT training sessions designed to enhance staff technical skills and improve overall efficiency in their workflows.

Benefits of IT training for staff to:

- Enhancing Staff Skills
- Improving Operational Efficiency
- Ensuring Policy Compliance

IT Managers and technicians have ongoing training updates in

- Software Applications
- Network Security
- Data Management

16.Network

Computer networks include:

- virtual private networks (VPN), e.g. AOVPN, Meraki/SD WAN
- local area networks (LAN)
- wide area networks (WAN)
- wireless networks
- network storage

Virtual private networks

A VPN is a secure network that will allow staff to access the school's network if a direct link to the school's network is not available.

Local area network, wide area networks and wireless networks

Access to the school's networks is given to staff that have a need to use it.

This service can be revoked at any time by the school if there is unacceptable use of the networks.

The networks are the infrastructure of the school's systems and as such are used via equipment that staff will have access to. Information travelling the network may be monitored in line with the Lawful Business Practices Regulations 2000.

Wireless network access to the school's networks is available to a wireless enabled device. Third party access is also available on the schools Guest Network.

Network storage

The network drives are the locations of information stored on the school network. The C drive, the drive physically inside a PC or laptop is not a network drive and will not be backed up.

No personal information of any kind must be stored on any computer drives, networked or otherwise, including video, pictures or music that are non-work related.

Shared drives are networked drives that must be used to store, manage and share information with colleagues. Restricted areas can be set up on shared drives or Sharepoint sites to keep information confidential to teams. Contact the ICT Technician if this facility is required.

Storage of any information and files that can be considered obscene, pornographic or fall within any of the other unacceptable uses is not allowed and will result in disciplinary action and where appropriate, police action.

Managers take responsibility within their areas for where and how information is stored (in any format).

The security of the school's information is of paramount importance, to protect the ability of the school to provide services, and in the case of personal data to protect the privacy of the individual. When saving

confidential information to network drives consideration must be given to who has access to that area and whether it is appropriate to store the information there.

File retention and destruction rules exist for all information within the school that govern how long information must be held. Access the school Information Retention Schedule (SIRS) via the school office or contact Data Protection Officer for more information on good records management including retention and destruction.

Backups

Why IT backups are crucial:

- Protecting data: IT backups ensure that important data is safeguarded from loss or corruption.
- Disaster recovery: Having backups in place allows for quicker restoration of systems in case of a disaster.
- Compliance requirements: Many industries have regulations that mandate regular backups to maintain compliance.
- Peace of mind: Knowing that data is securely backed up provides peace of mind for organisations and individuals.

  The school should

  1. Implement automated backups to ensure regular and consistent data protection without manual intervention.
  2. Use a combination of on-site and off-site backup solutions to mitigate the risk of data loss in various scenarios.
  3. Conduct regular testing of backup systems to ensure that data can be successfully restored when needed.
  4. Utilise encryption and access controls to maintain the security of backup data and prevent unauthorised access.

17. Internet Access

Use of Internet

The use of the internet is a valuable business tool, but employees must be aware that the internet should be used responsibly.

Key Messages

- All internet use via the school's equipment/systems/mobiles will be monitored.
- Officers can only use the school's internet facility for personal use in non-work time and in compliance with the usage set out in this document.

- Misuse of the internet can lead to disciplinary or criminal proceedings

For internet use staff must abide by the information below

Acceptable

- Only access the internet for personal reasons in non-works time with access complying with the requirements of this policy.
- Ensure personal use of the internet complies with the requirements of this document.
- Consult with ICT Technician before downloading software from the internet
- Report any information found on the internet that may be inaccurate or defamatory to the school or its officers to the SBM/Headteacher
- Report accidental unauthorised internet access, i.e. when they received an 'Access Denied' system message, to their line manager

Unacceptable

- Breach the confidentiality of individuals or the school
- Run a business of profit-making activity including auction site
- Access websites for personal use during work hours
- View websites that are not allowed by the school-on-school equipment/using school infrastructure, including but not limited to:
    - Video and audio files
    - Photo searches
    - Sexually explicit/pornographic
    - Intolerance/hate
    - Criminal action
    - Chat groups/rooms
    - Violence/weapons
    - Illegal drugs
    - Hacking
    - Spyware
    - Proxies and translators
    - Sex education
    - Fraud
    - Phishing (fraudulently obtaining sensitive information such as passwords, bank details, etc, by pretending to be a trustworthy source)
- Download software or utilities to school equipment without authorisation
- Publish or make available confidential or personal data via websites, newsgroups, forums, social networking/media sites or any similar facility.
- Represent their own opinions as those of the school on any websites
- Knowingly distribute or otherwise be involved in virus, Trojans or other malware use
- Post school information on personal social media sites

18.Internet Monitoring

The school reserves the right to monitor the use of the Internet and web in line with the Lawful Business Practice Regulations (2000) for the purposes of:

- gaining routine access to business communications
- monitoring standards of service and training
- prevention or detection of crime
- detecting unauthorised use of the internet.

Staff must be aware that the school cannot guarantee privacy of private information if they use webmail or Internet banking and supply passwords and other security details to gain access to these facilities.

The school reserves the right to block access to any website deemed inappropriate and to report access of inappropriate material to the Headteacher if this type of activity is logged. Misuse of the internet can lead to disciplinary action being taken.

19.Governors, Members and Trustees

Governors, Members and Trustees should comply with this policy with the following variations:

- Personal equipment is encouraged to be brought to governors' meetings. This is to allow individuals to see papers electronically.
- All papers (except for agendas) must be kept ONLY on the Governors SharePoint area. For security and confidentiality, and to ensure all papers are held as a record, no papers should be circulated by email.
- Headteachers must ensure that their governors can access the SharePoint area, and that they put on training and troubleshooting sessions with technicians to overcome any technical issues.
- Full details are available in the Governors Handbook.

20.Acceptable use of IT

Acceptable use policy for pupils

Acceptable Use Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

• I understand that the school will monitor my use of the systems, devices and digital communications.

• I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it

. • I will be aware of “stranger danger”, when I am communicating on-line.

• I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)

• If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me

• I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line or any part of the school IT system

I understand that everyone has equal rights to use technology as a resource and:

• I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use.

• I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

• I will not use the school systems or devices for non-educational purposes.

• I will act as I expect others to act toward me:

• I will respect others’ work and property and will not access, copy, remove or otherwise alter any other user’s files, without the owner’s knowledge and permission.

• I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.

• I will not take or distribute images of anyone without their permission.

•I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school.

• I will only use my own personal devices (mobile phones/USB devices etc) in school if I have permission and I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.

• I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.

•I will immediately report any damage or faults involving equipment or software; however, this may have happened.

• I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)

• I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.

• I will not use social media sites within school. When using the internet for research or recreation, I recognise that:

• I should ensure that I have permission to use the original work of others in my own work.

• Where work is protected by copyright, I will not try to download copies (including music and videos).

• When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me. I understand that I am responsible for my actions, both in and out of school.

• I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be online-bullying, use of images or personal information whilst using the school ICT systems).

• I understand that if I fail to comply with this acceptable use agreement, I may be subject to disciplinary action. This could include loss of access to the school network/internet, detentions, suspensions, contact with parents and in the event of illegal activities, involvement of the police. Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems. I have read and understand the above and agree to follow these guidelines when:

• I use the school systems and devices (both in and out of school).

• I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.

• I use my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email.

• Office 365, Microsoft Teams website etc.

Name of Student/Pupil: ……

Group/Class: …….

Signed: Date: ……..

Staff (and Volunteer) Acceptable Use Policy Agreement

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students/pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

• I understand that the school will monitor my use of the school digital technology and communications systems.

• I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc) out of school, and to the transfer of personal data (digital or paper based) out of school.

• I understand that the school digital technology systems are primarily intended for educational use.

• I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.

• I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the relevant member of SLG.

•I will be professional in my communications and actions when using school/systems:

• I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

• I will communicate with others in a professional manner, I will not use aggressive or inappropriate language, and I appreciate that others may have different opinions.

• I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured. I will always check permissions as per the school records (SIMS)

• I will not use social networking sites in school. Only those staff with responsibility for marketing and as authorised by the Headteacher can use social networking sites in school in accordance with the school's policies.

• I will only communicate with students/pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.

• I will not share my personal home accounts/data (social media, email etc) with pupils.

• I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

• I will avoid using my mobile devices in front of students. When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will ensure that any such devices are protected by up-to-date antivirus software and are free from viruses.

• I will not use personal email addresses on the school ICT systems

• I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).

• I will ensure that my data is regularly backed up, in accordance with relevant school policies.

• I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.

• I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

• I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.

• I will not disable or cause any damage to school equipment, or the equipment belonging to others.

• I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School/LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in safe storage.

• I understand that data protection policy requires that any staff or student/pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

• I will immediately report any damage or faults involving equipment or software; however, this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

• I will ensure that I have permission to use the original work of others in my own work.

• Where work is protected by copyright, I will not download or distribute copies (including music and videos). I understand that I am responsible for my actions in and out of the school:

I understand that this acceptable use policy applies not only to my work and use of school digital technology equipment in school but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.

I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors/directors and/or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name:

Signed:

Date:

Appendix 1

Information Sharing Policy

v1

FREQUENCY OF REVIEW:	**Annually**
COMMITTEE:	**Audit & Risk Committee**
RATIFICATION DATE:	**2nd December 2025**
DATE OF NEXT REVIEW:	**Autumn 2027 unless there is a material change**

Signed…… Date ……
Chair of Audit & Risk Committee

Signed …… Date ……
CEO

1. Introduction & Scope of Policy

1.1 This policy is based on the requirements of the latest Information Commissioners Office (ICO) Data Sharing Code of Practice. The policy will help ensure any sharing is fair, transparent and in line with the UK Data Protection Act/UK GDPR 2018 and the rights and expectations of the people whose information is being shared.

2. What do we mean by data/information sharing

2.1 Information sharing is the disclosure of data from one or more organisations to a third party organisation(s), or the sharing of information between different parts of the school.

2.2. This policy covers the sharing of personal information on a systematic and exceptional basis.

2.2.1 **Systematic Information Sharing** – this involves the routine sharing of the same or similar information for the same person between a set number of organisations. Sharing ordinarily takes place under the conditions of an agreed information sharing agreement.

2.2.2 **Exceptional Information Sharing** – these are one off ad hoc decisions to share information

2.3 It is important to remember that data protection principles also apply to information shared **within** the school as well as sharing with external organisations.

3. Information Sharing and the Law

3.1 The school derives its powers to share information from either Acts of Parliament or other legislation that governs the school's activities.

3.2 The first point to consider before sharing information is what legal basis is there to share information. The legal basis will ordinarily fit into one of three categories.

3.2.1 **Express obligations** – This is where there is an established legal requirement for the school to share information. An example of this would be legislation that requires the school to share information with Her Majesty's Revenues & Customs (HMRC) for taxation purposes.

3.2.2 **Express powers** – The school will be given legal powers to enable the sharing of information. An example of this is the Strengthening Families programme that allows the school to share information with the Department of Work & Pensions (DWP).

3.2.3 **Implied powers** – Certain legislation regulates how school services are run but does not give express powers to share information. However, to meet the requirements of the legislation there is implied power to share information. An example here would be the Children's Act which requires school's to protect children. To protect a child the school may have to share information with a number of organisations.

4. Deciding on Sharing Personal[1] Information

4.1 There are a number of factors to be considered before information sharing takes place. The following questions need to be considered before sharing.

4.1.1 **What is sharing meant to achieve?** A clear objective for sharing should be identified. This will assist in deciding on what elements of information need to be shared.

4.1.2 **What information needs to be shared?** Only the elements of information required to meet the objective identified should be shared. Where opinion is being shared it should be clearly denoted that this is an opinion being shared.

4.1.3 **Who requires access to the shared information?** 'Need to know' principles should be applied. Individuals should only be able to access shared information if they need to.

4.1.4 **When should it be shared?** It should be recorded whether the sharing was on an exception or systematic basis.

4.1.5 **How should it be shared?**
Externally - Information should only be shared securely, e.g. electronically using secure email or hand delivered to named individuals or sent by post (special delivery/secure courier) dependent on the level of sensitivity of the information being shared.

Internally- If sharing is electronic and to/from @telford.gov.uk or @taw.org.uk then this a secure method. However the correct recipients details should be checked before an email is sent. If hard copy information is being shared then hand delivery/collection should be considered for special category (very sensitive) personal information.

4.1.6 **What are the risks in sharing and not sharing the information?** A number of questions should be asked such as what is the potential benefit/harm/damage to an individual whose information may be shared, will an individual be likely to object, etc.

4.1.7 **Can the objective be met without sharing the information or by anonymising it?** If an objective can be met by sharing anonymised information or by not sharing personal information at all then the objective should be met in this alternative way.

4.1.8 **Record what you have shared**. Once you have decided there is adequate justification to share information then the actual sharing should be recorded including what information was shared, to who, when and by who.

4.2 Obtaining consent from individuals to share their personal information should also be factored into the decision making process for sharing information. Consent should be a positive action, specific, given freely, granular and provide an informed indication of the wishes of the individual that they agree to how their personal data will be processed.

4.3 It is not always appropriate to obtain consent from an individual (or in fact inform them that sharing is taking place) for sharing their information. Consent is not needed for all aspects of personal information sharing. An example of this is where the school is required to

[1] The term personal information is used to generically include personal and sensitive information

provide the police with information for the prevention and detection of crime or for the protection of children/vulnerable adults. However, a legal basis detailed in the UK Data Protection Act 2018 is **always** required before any sharing occurs.

5. Fairness and Transparency

5.1 To share information in a fair and transparent manner, individuals should be aware of which organisations are sharing their personal data, with whom and what it is being used for. Fairness also relates to how personal information is shared in that this should happen in a reasonable way that the individual would not reasonably object to. However, there are certain exceptions to this, see 4.3 above.

5.2 Fairness and transparency can be achieved by the use of privacy notices which, as a minimum, tells an individual from whom information is being collected why their information will be shared and who it is going to be shared with (either named organisations or types of organisation). See guidance note on privacy notices for further information.

6. Security When Sharing Information

6.1 The UK DPA 2018 requires the school to have adequate technical and organisational measures in place to protect personal information. This requirement also covers when the school shares information.

6.2 There are a number of security issues that should be considered in respect to shared / sharing the information.

6.2.1 Information must be shared in a secure manner, see paragraph 4.1.5 for further detail.
6.2.2 Information received from other organisations should be reviewed to ensure there are no conditions of use attached to it and it needs to be kept secure.
6.2.3 Information sent from the school to other organisations should be reviewed to ensure staff understand who will access it and for what purpose.
6.2.4 More sensitive information shared should be afforded additional security.
6.2.5 The level of impact of a data breach on both the individual(s) and the school

6.3 For more information on required security arrangements please read the Schools Information Security Policy.

7. Governance Arrangements

7.1 Responsibility for sharing information lies with the 'Information Asset Owner'. The Information Asset Owner is the Head Teacher.

7.2 The information owner should ensure there are appropriate arrangements in place to share information that comply with the requirements of this policy.

7.3 A further element of governance in respect to information sharing is the use of information sharing agreements (ISA's). An information sharing agreement sets out a number of common rules to be adopted by the various organisations involved in the data sharing operation.

7.4 It is good practice to have an ISA in place if information sharing is taking place on a large scale or on a regular basis.

8. Reporting Security Incidents

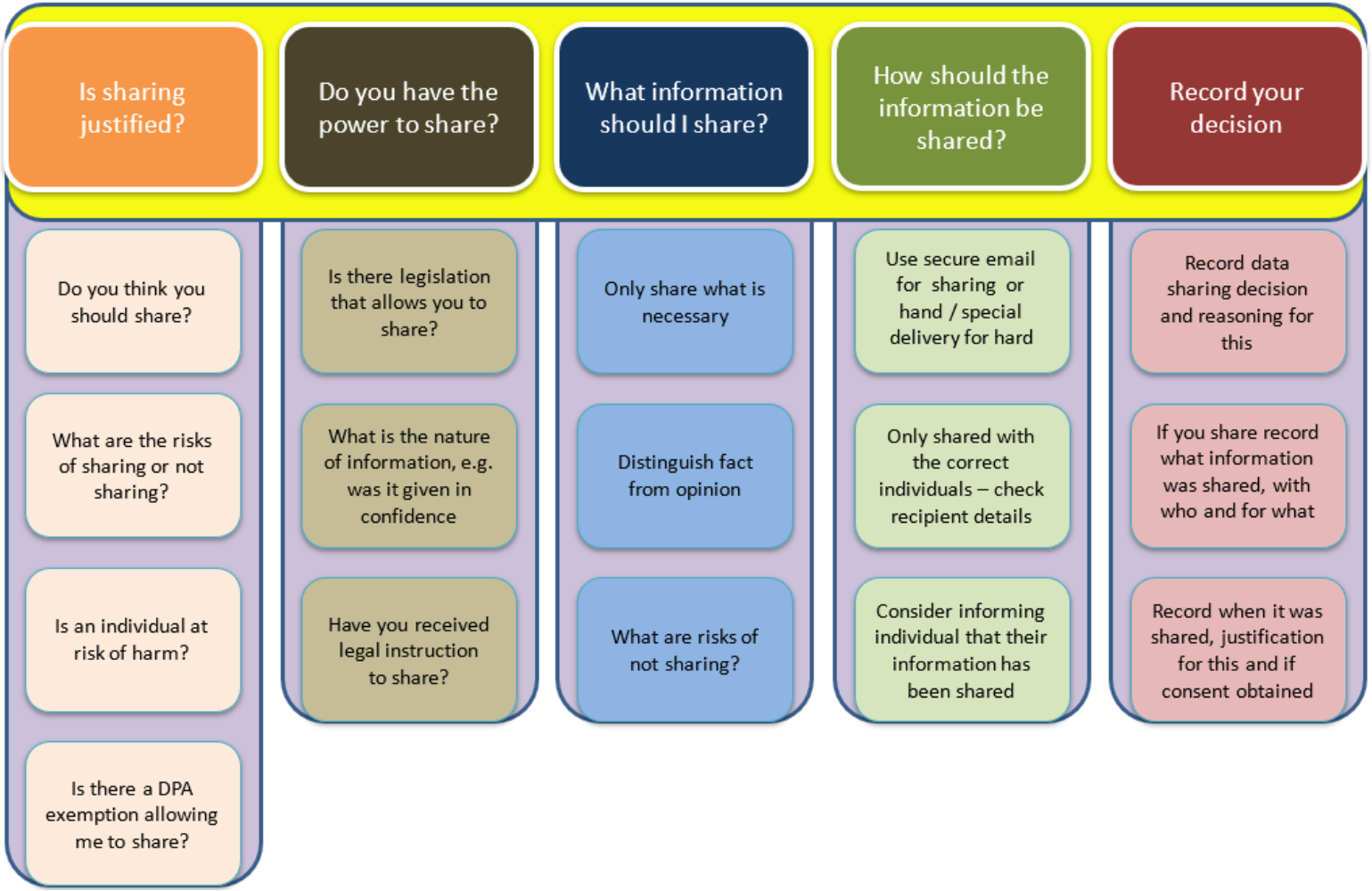
8.1 If the information shared is compromised, e.g. sent to an incorrect recipient, viewed by an unauthorised individual, etc. the School's Information Security Breach Procedure (ISBP) should be instigated immediately.

8.2 As per the ISBP procedure, all potential information security incidents should, as a minimum, be reported to the School Business Manager/Head Teacher and the Data Protection Officer as soon as the incident has been identified.

9. Further Information

9.1 Appendix 1 provides 5 steps to effective data sharing. This can be used as a reference when considering sharing information.

5 Steps to Effective Data Sharing



Appendix 2

School Information Security Policy (SISP)

FREQUENCY OF REVIEW:	**Annually**
COMMITTEE:	**Audit & Risk Committee**
RATIFICATION DATE:	**2nd December 2025**
DATE OF NEXT REVIEW:	**Autumn 2027 unless there is a material change**

Signed…… Date ……
Chair of Audit & Risk Committee

Contents

	Section		Page
	important notice – acceptance of this document		2
1	introduction		2
2	roles & responsibilities		3
3	acceptable & non acceptable use		3
4	asset & information classification		3
5	information sharing		4
6	physical & environmental		5
7	loss or theft of equipment/files & information		6
8	staff/user access management		6
9	working from home & mobile working overview		8
10	security responsibility for staff & delivery units		8
11	monitoring system access, use and auditing		9
12	communications & operations manager		9
13	outsourcing		11
14	systems development & maintenance		11
15	business continuity		12
16	legal, regulatory & contractual compliance		12
17	artificial intelligence (AI)		16
18	advice and guidance		16

IMPORTANT NOTICE - ACCEPTANCE OF THIS DOCUMENT

This policy and all associated policies applies to all full time and part time employees, casuals, volunteers, temporary/agency staff, Governors of the school and all contracted third parties working for the school and partner employees, whether they are working on

Who should read this policy?

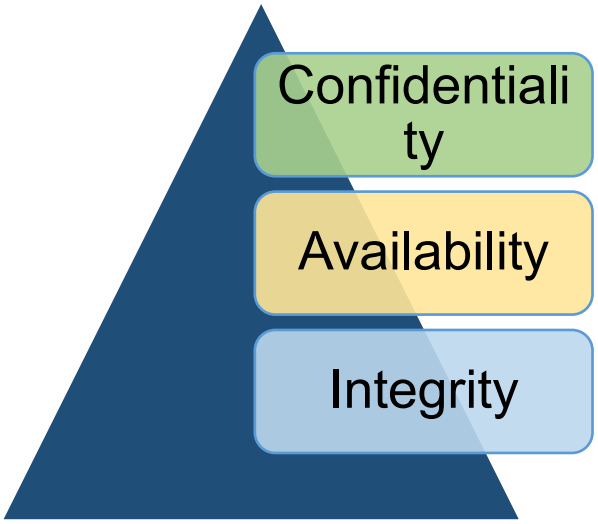
All school staff and Governors should read this policy

When you have read this policy document or the summary version, please indicate you have done by using the form at the end of this policy.

1. Introduction

1.1 Information can exist in many forms. It can be printed, written, stored electronically, transmitted by post, email, and fax or even spoken in conversations. The purpose of information security is to ensure that all information (including personal information) and associated processing systems are protected to an adequate level.

1.2 This policy sets out minimum standards and common acceptable use for confidentiality, integrity and availability of information to meet internal and legal requirements.



Ensuring that information is accessible only to those authorised to have access.

Ensuring that authorised employees have access to information when required.

Safeguarding accuracy and completeness of information and processing methods.

1.3 The policy has been written to conform, where possible, to standards such as ISO 27001 (Information Security Management standard), HMG Data Handling Guidelines, Government Functional Standard (GovS 007: Security) and PCI-DSS (Payment Card Industry – Data Security Standard).

2. Roles & Responsibilities

2.1 All employees within the school have a responsibility to ensure that they take steps to safeguard the security of the information that they are using and seeing.

All employees must:

- Read and comply with this policy (including linked acceptable use policies)
- Read and comply with the Information Security Breach Procedure (ISBP)



- Be personally responsible for work information held by them

3. Acceptable & Unacceptable Use

- The school will not tolerate the use of any of its equipment/information for any purpose, which contravenes this policy and associated policies/documentation. Employees found not complying with these requirements might be subject to disciplinary action. This policy covers the following areas of use:



To view what is acceptable use and non-acceptable use for each of the categories above press the 'Ctrl' key and click on the relevant topic.

Employees should also ensure they are familiar with the requirements of other related policies on records management, data protection and social media.

Acceptable use in relation to artificial intelligence (AI) is detailed in section 17 of this policy.

4. Asset & Information Classification

4.1 In order to make sure that the School's information/assets receive an appropriate level of protection, all information will be treated in accordance with the requirements of ISO 27001 (Information Security Standard) and Government Security Classifications Policy.

5. Information Sharing

5.1 The schools Information Sharing Policy must be complied with at all times. Key points to note from this policy are that you should:



- Only share personal identifiable information (PII - Data about an individual that could, potentially identify that person) where there is legal justification to do so.
- Know the objective/reasons for sharing PII.
- Investigate whether the objective can be met without sharing PII.
- Only send the minimum PII needed to meet the objective/reasons.
- Where possible, anonymise the information you send so it is not personally identifiable
- Confirm the recipients contact details, e.g. postal address, email address, etc. before sharing information
- Appropriately protect the PII you are sharing by using a secure solution if it is electronic, sending post by special delivery/courier, etc.

5.2 The School will, where there is a defined justifiable purpose, sign up to information sharing agreements with partner organisations, where these agreements are within the boundaries of applicable legislation and regulation and do not compromise the School or the confidentiality of the personal and/or sensitive data that it holds.

5.3 The School will have put in place information sharing agreements where regular sharing of information from School systems/records takes place.

5.4 The Data Protection Officer has produced a standard data sharing agreement checklist and will advise and guide the school in developing data sharing agreements that cover specific requirements, suitable to their needs.

5.5 In order to ensure that information sharing takes place in an appropriate manner, all data sharing agreements should be approved by the Head Teacher.

5.6.1 Receiving and sending confidential/personal information

School staff have control over confidential/personal information they send to other parties. It is critical that appropriate security measures are in place before information is sent out. Staff have little control over how other organisations or the public may send confidential or personal information to the School. Staff must:



POST

Send information via special delivery, or if sensitive or a large number of personal details are included, use a reliable courier who will deliver to a named recipient only.

Consider hand delivery if local, to someone known to you. Senders should be encouraged to send confidential/personal information to the School by special delivery/courier.



EMAIL

Only use secure email accounts



FAX

Only to be used in exceptional circumstances. Should send to a known fax number only and verify the number before sending. Ask if the fax is a safe haven (area that is secure and accessible only by authorised staff). If not request that the recipient

stands and collects the fax as it is received. Also, discourage senders from using faxes.

6. Physical and Environmental Security

6.1 All employees have a responsibility for the physical security of School's assets (including information) including securing their laptops, locking away sensitive information, etc.

6.2 The school will be responsible for the provision of suitable physical, technical, procedural and environmental security controls in line with best practice such as ITIL (Information Technology Infrastructure Library – standard for IT service management) in order to prevent unauthorised access to, interference with, or damage to information.

6.3 Access Control

6.3.1 The management team have responsibility for authorising their staff to access information including IT networks, offices, secure filing cabinets etc. No School employee may access or attempt to access any information for which they have not been given authorisation.

6.3.2 The management team will remove access to information during periods of extended leave or sickness of more than 3 months. A review of employee's level of access to School information must be undertaken by their Manager during supervision.

6.3.3 Additional security measures shall be implemented by data owners to control access to especially personal/sensitive School data.

6.3.4 To control access to information, care must be taken (within the constraints of new ways of working) as to the physical positioning of desks and equipment used to view key personal,

sensitive or confidential data. Desks used to process or view such data must be positioned away from doors/windows and public areas.

6.3.5 Managers must ensure appropriate access controls are in place for information processed in open plan offices. Adequate clear desk arrangements should be adhered to as outlined in this policy.

6.4 Physical security (equipment)

6.4.1 Desktop machines in public areas must be secured to protect against theft and/or unauthorised access.



6.4.2 Multi-functional devices (MFD) machines must be sited appropriately in areas where sensitive information can be handled.

6.4.3 Backup equipment and media must be sited at a safe distance to avoid damage from a disaster at the main site(s) and must be subject to the same environmental and physical protection as the main system.

6.5 Security of premises

6.5.1 Premises security consists of:



IDENTITY BADGES

All staff are issued with identity badges which include their photograph and these must be worn visibly at all times when working in/entering School buildings.

Staff must question anyone in any School building not wearing identification, where they are confident to do so. Staff must understand that they may be asked for identification at any time

Passes for visitors are controlled by Reception. Visitors to School offices must not be allowed to wander around the buildings and must be accompanied at all times. They must sign in and out at Reception and wear identification badges visibly at all times when progressing beyond public areas.



SECURITY PASS/FOB

Access to School premises is controlled by the issue of security passes or FOB's. Lleavers swipe cards / FOBs must be deactivated.



PHYSICAL ACCESS

Access to areas containing sensitive School information must be strictly controlled and given on a need-to-know basis. A record of privileged access granted to nominated individuals will be kept by the respective manager.

Physical security (door locks, locked cabinets, security card access) is

the responsibility of all employees. Doors and windows must be locked as and when appropriate and blinds or curtains in place, with external protection considered for windows, particularly at ground and lower ground level.

7. Loss and/or Theft of Equipment, Files and Information

7.1 In the event of any loss/theft of equipment, files and information, the School's Information Security Breach Procedure should be followed. The key immediate actions include:

- Theft of equipment should be immediately reported to the police (obtain crime number) and to your SBM/Head and the schools ICT support. The SBM/Head will then inform the DPO.
- Theft/loss of files or information should be reported to the SBM/Head Teacher and DPO

8. Staff/User Access Management

8.1 Staff registration

8.1.1 The SBM/Head Teacher or Information Asset Owner must authorise access to information / systems for the provisional user with access being granted on a 'need to use' basis in order to carry out their duties. Access should not be granted prior to authorisation being given.

8.2 Password responsibilities

8.2.1 Good, secure passwords are essential, and staff must be aware of what constitutes a suitable password. The School's Password Management Policy should be adhered to at all times.

Passwords must be:

- Changed regularly or immediately if there is any doubt at all that a password may have been compromised
- Kept confidential and never shared
- Changes at the first opportunity from default assigned passwords

Passwords must NOT:

- Be easily guessable, and this includes dates of birth, family names, pet names, or other personal details
- Be shared with anyone else
- Be the same as your system user id
- Re-used on an alternate basis

- At least 12 characters long and complex, i.e. not be a simple word, name easily associated with you and contain numbers, a mixture of upper- and lower-case characters and allowed symbols

Passwords should NOT

- Where possible be written down
- Where possible be duplicates of passwords used for other systems.

If a staff member is using Windows Hello to log on to their laptop, then they must use a 6-digit code. Staff should not use easily guessed codes such as employee number, phone number, date of birth, etc. The code should not be a number that is publicly known to be linked to you, i.e. used on your social media platforms

8.3 Leaving procedure

8.3.1 When staff leave the school, as part of the school's leavers procedure their manager is required to:

- Ensure that any information held in the leaver's homes drive (H drive) or One Drive, that is of importance to the school, is moved to a relevant network folder
- Request accounts to access systems to be deleted/disabled
- Ensure email accounts/contacts and membership of email group accounts are removed and, if appropriate, emails will be auto responded to providing alternative contact details
- Ensure leaver returns all work ICT equipment/data

8.4 non-electronic media

8.4.1 Paper media (including carbon copies, computer printouts, etc) containing information that is classified as personally identifiable or sensitive must be shredded on site. Disposal should be in line with the School's Information Retention Schedule.

8.5 Disposal of equipment

8.5.1 ICT equipment for disposal must be disposed of securely either by T&WC ICT or other reputable disposal company. ICT equipment no longer required must not be used by staff for personal use.

8.6 Third party access to systems

8.6.1 It is the responsibility of Information Asset Owners or SBM/Head Teacher in conjunction with ICT Technician to authorise third party access to resources and systems. User accounts and passwords will have to be created and where necessary relevant policies will have to be signed by the school and the third party prior to allow access.

8.6.2 It is the responsibility of the SBM/Head Teacher to advise the ICT Technician as soon as the third-party access is no longer required.

8.7 Internet and intranet web publishing

8.7.1 Some staff will be authorised to publish data on the school website. This privilege must not be shared with staff who are not authorised to publish information.

8.7.2 The school is responsible for content which is published and must ensure that the information is correct, up to date and relevant and is published in plain English.

8.7.3 Inappropriate, illegal or offensive material must not be published. This will be removed immediately and may result in disciplinary action being taken against the offender.

9. Working from Home and Mobile Working Overview

9.1 There is a difference between "working from home" and "home working" and "mobile working".

Working from Home	Home Working	Mobile Working
Work undertaken for limited periods but officer remains school based.	Officer's normal place of work is their home, and they do not visit the school daily.	Officer travels as part of their role and will require access to School facilities (network) whilst travelling.

Staff authorised as mobile workers or who may work from home **must**:

- Adhere to the School's home working and remote working guidance documents
- only use School equipment to do their work unless accessing authorised cloud services
- ensure that all equipment and information is always kept secure, including ensuring that any equipment or information is not left "on show" in parked cars etc,
- only connect their school computers to any other non-School network using approved remote access technology. Personally owned ICT peripherals must not be connected to School computers connection
- never send any work information of any type to "non-work" email addresses
- never dispose of any used media off-site – it should be disposed of securely by ICT Technician

If offshoring is intended to be used for processing data, then the related agreement and impact of processing should be checked with your IT Technician and DPO.

9.2 Staff are responsible for ensuring that unauthorised persons are not able to view confidential information or use School equipment. This includes family members and staff from other organisations.

9.3 Use of any confidential information at home must be for work purposes only. If the use of confidential information at home can be avoided, then the information should not be taken home.

9.4 Staff must ensure that when storing equipment/information at home, it is kept as secure as possible and if available is stored in a locked container.

10. Security Responsibilities for Staff

10.1 SBM/Head Teachers must make it clear to their staff, where the job description is not explicit, the level of responsibility that they have for information that they handle. This includes compliance with key elements of this policy covering:

10.1.1 Password management – see section 8.2 of this policy and Password Management Policy.

10.1.2 Encryption and cryptographic controls - Appropriate encryption should be used to communicate / transfer data outside of the school.

10.1.3 System implementation and software purchase - all systems implementation and software purchases must be undertaken via the ICT Technician. Any projects that include the possible use of new computer systems/applications must engage ICT Technician prior to discussions with suppliers.

10.1.4 Clear screen and clear desk - Staff must ensure that they lock their PC screen when leaving their desk for a limited time, or log out when leaving for extended periods. School systems have an automatic lock out facility on PC's that do not need to be constantly logged on that will activate after several minutes of inactivity.

Desks and other spaces must be kept clear of any confidential information at all times when the information is not being used and you leave your desk for a short period and locked away out of sight after a longer period.

10.1.5 Human Resources employment checks - All appointments must comply with the schools recruitment policy and include verification of an employee's identity, qualifications, employment history and eligibility to work in the UK.

10.1.6 Confidentiality agreements - As part of all employee's terms and conditions of employment, there is a requirement to maintain confidentiality of information both during and after their employment. Casual staff (including contractors/ agency staff) and third parties (including volunteers) not covered by an employment contract are required to sign a confidentiality agreement prior to being given access to information processing facilities. All such staff will be informed about the need to, and method for, maintaining confidentiality regardless of what access their role gives them to information.

10.1.7 Terms and conditions of employment - Employees of the School are expected to be aware of and comply with the all the codes of practice included within the Employee Code of Conduct, which includes responsibility for information security. Employees should also be aware that responsibility for information security continues beyond the end of their employment with the School and extends to all places and all times, including outside work. Breaches of confidentiality can lead to summary dismissal within the school's disciplinary procedure.

10.1.8 Training – All staff must ensure they complete relevant data protection training and keep up to date with information governance related policies and guidance.

11. Monitoring System Access, Use and Auditing

11.1 All School systems may be monitored to detect unauthorised activity or potential security breaches. Logged events may be reported and action taken if breaches or suspected breaches occur.

11.2 The School reserve the right to monitor, log, collect and analyse the content of all transmissions on networks/applications, including internet and email/Skype usage, at any time for system performance and fault diagnostic purposes as well as to detect unauthorised use of systems and to ensure that systems are being used in accordance with acceptable use policies.

11.3 Monitoring will be undertaken in accordance with legislation (Lawful Business Practices Regulations 2000 and Regulation of Investigatory Powers Act).

12. Communications and Operations Management

- Employees must not:

  - Copy materials (including newspapers) protected under copyright or patent law or make any materials available to others for copying. Employees are responsible for complying with copyright or patent law and applicable licences that may apply to software, files, graphics, documents, messages and other materials you wish to download or copy.



  - Send, transmit or otherwise distributing proprietary information, data, trade secrets or other confidential information belonging to the School or any other organisation

12.2 Housekeeping

12.2.1 Managers should be aware of School equipment, information or software that is taken off site. In all cases, those personnel taking School assets off-site will be responsible for the security of such equipment/information at all times.

12.2.2 Individuals must be made aware that they may face disciplinary procedures that could lead to dismissal if found responsible for the theft of equipment, software or School information.

12.2.3 Staff handling personal/sensitive information must take extra measures, e.g. encryption, password protection, use of lockable storage, etc, to ensure information in their possession remains private and secure in order to comply with the UK Data Protection Act 2018.

12.2.4 The unnecessary processing of sensitive personal data in an identifiable form must be avoided. Managers are responsible for drawing up procedures for their area of work.

12.2.5 Documents and records must be stored under secure conditions up until the point that they are either destroyed/shredded at work or passed to a third party to carry out physical destruction. This means that they must not be left unsecured in skips, bins, reception areas, corridors etc.

12.2.6 Sensitive or confidential information must not be recorded on voice mail systems.

12.2.7 All employees should be aware of the risk of breaching confidentiality associated with the photocopying (duplication) of sensitive documents. Authorisation from the document owner must be obtained where documents are classified as 'highly confidential' or above.

12.3 Storage

12.3.1 The following requirements should be complied with:

- Compliance with the UK Data Protection Act 2018 for personal data storage
- Data maintained for a period that meets legal/business requirements as per the retention schedule
- Data stored is protected against loss and unauthorised/accidental changes

12.4 Audit trails

12.4.1 To protect both staff and the school, all systems have clear audit trails. This is particularly important for staff with administration rights.

12.5 Complying with legislation

12.5.1 Everyone has an obligation, under legislation such as Freedom of Information Act 2000 and UK Data Protection Act 2018, to deal with information in the stipulated way. Further guidance on this can be obtained from the Data Protection Officer.

12.5.2 It is the responsibility of the SBM/Head Teacher to make sure that staff are aware of any specific legislation applicable to their role including data protection.

13. Outsourcing

13.1 Any outsourcing/third party hosting must be with reputable companies that operate in accordance with quality standards. Such an undertaking must include a suitable Service Level Agreement (SLA), which meets the school's requirements. Where the processing of personal data is outsourced, a data processing agreement should be in place.

13.2 Where outsourcing includes the use of cloud computing the provider must provide assurance that cloud arrangements comply with the NCSC cloud security principles.

13.3 Any agreements or contracts must make it clear to the outsource organisation what their obligations are in respect of the UK Data Protection Act 2018 , Freedom of Information Act 2000 and other relevant information related legislation.

13.4 Outsourcing that may take place where information crosses outside UK and European borders must take into consideration the requirements of the UK Data Protection Act 2018 – the restriction of movement of personal data across boundaries outside the European Economic Area (EEA). This maybe particularly relevant to new technologies such as cloud computing.

14. Systems Development & Maintenance

14.1 Controls will be implemented to ensure that security requirements are considered when developing existing information systems and prior to introducing new ones.

14.2 Information governance (IG) requirements of systems

14.2.1 The Data Protection Officer will be involved in the development of new information system functionality (including new systems and development to existing systems) and processes that include the processing of personal information to ensure that all governance requirements are included.

14.3 Data input

14.3.1 Line managers will have responsibility to ensure their staff are aware of processes and procedures relating to quality of data input in line with data quality policies / requirements.

14.4 Data output validation

14.4.1 Staff must undertake data quality checks on data output to ensure it is accurate/ up to date and complies with any policies on data quality.

14.5 Security/Privacy requirements within projects

14.5.1 Managers are required to undertake a risk assessment/Data Protection Impact Assessment to identify security/data protection requirements for new School systems that process personal information.

14.6 Test environments and test data

14.6.1 Any systems being tested or developed and tested will be separated from live systems. Live data will not be used and on logging in, the user(s) will be informed that they are in a test environment. Where development of systems occurs via a third party, there will an expectation that all testing will be completed to the relevant ISO standard. If there is no alternative to using live data in a test environment, then the DPO should be consulted prior to use to ensure the appropriate risk assessment is completed.

15. Business Continuity

15.1 The School has a process for management of business continuity across the school.

15.2 Continuity plans must be in place to ensure continued access to, and protection of, service critical information.

16. Legal, Regulatory and Contractual Compliance

16.1 To avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and any security requirement, compliance with this policy is mandatory. Failure to comply with policy requirements will be viewed as a breach of security. Any such event may be the subject of investigation and possible further action in accordance with the Disciplinary Procedure.

16.2 All parts of the school will be subject to review to ensure compliance with this policy. The Data Protection Officer may commence an investigation when the conditions of use have or may have been broken. Dependent on the circumstances staff may not be informed of the investigation. Whilst the investigation is under way, the staff member or account concerned may have their access rights suspended or reduced. If this occurs, the staff member will be informed.

16.3 Intellectual property rights (IPR)

16.3.1 Intellectual property rights include, but may not be limited to copyright, design and patents and trademarks.

16.3.2 Staff will not load software, video and audio files onto School systems without authorisation from ICT and that authorisation will include checking that any IPR has not been broken by the use of the software.

16.3.3 Licences for systems will be adhered to including making sure that any restrictions in the number of users for a particular piece of software are complied with.

16.3.4 Copies of software and systems will not be made by staff unless authorised to do so by the licence holder and ICT Technician.

16.4 Management of records

16.4.1 Information such as financial records, employee records, customer records and any records that are publicly accountable will be kept in accordance with ISO15489 records management recommended retention periods detailed in the Schools Information Retention Schedule.

16.5 Data protection and personal information

16.5.1 All personal information managed by the school is covered by the UK Data Protection Act 2018. This provides legislation as to how personal information may be used, stored, processed and shared. It contains six principles that the school should conform to and governs how information needs to be handled under certain circumstances.

16.6 Freedom of Information (FOI)

16.6.1 The FOI Act 2000 governs access to non-personal information in public organisations. Any request for information to any member of staff, in written form, could be a request under this legislation. Staff must respond to these requests if they can answer the question quickly (opening times of offices etc) – known as business-as-usual requests.

16.7 Environmental Information Regulations

16.7.1 The Environmental Information Regulations (2004) covers the provision of information that is environmental in nature.

17. Artificial Intelligence (AI)

- There are clear benefits and risks associated with processing data (including voice data) using AI technologies.

17.2 Prior to the implementation of an AI solution, a Data Protection Impact Assessment and an AI Risk Assessment document must be completed and signed off by the DPO.

- All possible use of AI requires approval from the DPO.

18. Advice & Guidance

18.1 Advice on this policy can be sought from your Data Protection Officer.

Appendix A - Acceptance form

School Information Security Policy – Acceptance Form

School	
Full name	
Job title	
Contact telephone	

- I have read, understood, and agree to abide by the Schools Information Security Policy.
- I understand that this policy may change and that I will read any new versions when I am informed that they are available.
- I further understand that I must read, understand and agree to abide by the acceptable use policies and codes of practice that are relevant to me and that if I have any questions that I may ask our Data Protection Officer for assistance.

Signed _____ **Date** _____

Version	Date	Author	Sent To	Comments
6-20	22/9/20	R Montgomery	Schools	Updated policy to reflect changes to good practice
6-22	27/4/22	R Montgomery	Schools	Updated policy to reflect changes to good practice
7.0	23/07/24	R Montgomery	Schools	Updated policy to reflect changes to good practice

Appendix 3

Password Policy

v1

FREQUENCY OF REVIEW:	**Annually**
COMMITTEE:	**Audit & Risk Committee**
RATIFICATION DATE:	**2nd December 2025**
DATE OF NEXT REVIEW:	**Autumn 2027 unless there is a material change**

Signed…… Date ……
Chair of Audit & Risk Committee

Password: A unique string of characters that a programme or user should supply to meet security requirements before gaining access to data.

10. Introduction

1.1 Password management is an integral part of the school's information governance arrangements. This policy outlines the requirements associated with the use and management of passwords and complies with guidance from the National Cyber Security Centre (NCSC). This policy should be read in conjunction with the Schools Information Security Policy (SISP).

11. Using Passwords Securely

11.1 We all require passwords to access information held on a number of IT systems, mobile apps and websites. Using your passwords securely, in adherence to this policy, will help ensure adequate protection for the data you are accessing. The following areas need to be considered:

- How to choose a good password
- Password Protection
- Multiple Passwords
- Password Storage

2.2 Where there is an opportunity to use multi-factor authentication (MFA), to support password use, this functionality should be used.

2.3 How to choose a good password

2.3.1 Password requirements should follow the '12 x 4 Rule' and be/contain:

12 = 12 characters minimum length
4 = 1 lower case + 1 upper case + 1 number + 1 special character*

*A special character is a non numeric or alpha character such as '£' or '!'

2.3.2 The National Cyber Security Centre (NCSC) suggests that passwords should include 3 random words to make it difficult to guess. This is in addition to incorporating the 12 x 4 rule. Examples here could be:

Rot2Big!dot75
4New8£ran9ear

2.3.3 There are a number of things to **avoid** when choosing a password, in the main these include (but not limited to) **not**:

- Using your userid as part of your password
- Using the name of a family member, friend or pet
- Using personal information about you that can be easily obtained such as date of birth, phone number, vehicle registration number, etc.
- Use sequences, i.e. consecutive alpha/numeric characters, e.g. qwertym, 12345, etc
- Use words with just one number substitution, e.g. Passw0rd

- Using the same base word for your password and then changing one character to create a new one, e.g. old password – Miranda1! changed new password to Miranda2!
- Using common names such as days or months
- Using common place names particularly those near where you live/work, e.g. Telford, school name, etc

2.3.5 Remember what information you post on public social media accounts and do not use any of this as part of your password.

2.4 Password Protection

2.4.1 The following is a list of techniques that should be followed to protect your password.

- When entering a password ensure no one is able to see what you are typing
- "Shoulder" surfing is a common way for individuals to gain access to your device / account. Ensure when typing your password that no one is looking over your shoulder
- Using a mobile phone is not a secure way of holding your userid/password information
- Diaries/notepads are not a secure medium for recording your userid/password.

2.4.2 Where the 12 x 4 rule is followed in terms of password format the duration that a user has to change their password can be lengthened, i.e. 12 x 4 character password should be changed as a minimum once every 180 days.

2.5 Multiple Passwords

2.5.1 Where possible you should set different passwords for the various information systems you access. Given the number of different passwords you may have to remember there is a temptation to set the same password for all systems. If the same password is used it dilutes the strength of security the password access provides. Also this may lead to confusion as the password expiry settings for multiple systems may differ.

2.5.2 If the same password is used for a number of systems then a compromised password can lead to unauthorised access to several systems rather than just one system if different passwords were used for each system.

2.5.3 You should not use the same passwords you use for personal use for work use.

2.6 Password Storage

2.6.1 There are considerable difficulties with remembering different passwords for multiple systems. The schools ISP states that where possible you should not write down passwords for systems you access due to the security implications of doing this.

2.6.2 Schools should consider the use of password management applications. There is an application called KEEPASS which can be used to store your passwords to access all applications. A password will need to be set to access KEEPASS, the format of this password should follow the guidance in section 2.3. Use of these applications should be discussed with your IT support.

3 Specification for password management parameters for systems

3.1 There are no legal requirements/regulations for the management of passwords but the school strives to meet the good practice guides produced by the NCSC. Detailed below is a list of key minimum password requirements for any system development extracted from these good practice guides (this is not an exhaustive list):

A. Users with standard privileges (a typical end user) should be forced to change their password every 180 days dependent on the type of data held by the system, i.e. for systems holding sensitive data forced password change should be more frequent.

B. Users with enhanced privileges (mainly IT support) such as admin accounts should be forced to change their password more frequently, i.e. nearer 30 days than 90.

C. Password format should enforce the 12 x 4 / 3 random words rule as detailed above

D. Rules should be set to not allow the password to be the same as the relevant user ID

E. The previous 4 passwords should not be able to be re-used

F. Systems should store passwords in a well-hashed, salted or encrypted format

G. Users should be locked out after 7 unsuccessful attempts to input their password. The account should then only be unlocked by the System Administrator.

4 Password Management for 'Privileged' Accounts

4.1 A privileged user account is one where the account has enhanced access that is denied to a standard user, e.g. an account with administrator rights. Given these accounts have enhanced functionality rights they require more robust password management arrangements than a standard user account. The main accounts covered by this are Local Administrators, Privileged User and Domain User.

4.2 Schools IT support should adopt a fine-grained password policy to allow different password restrictions for privileged user accounts in a domain. As a minimum the password settings for privileged accounts should follow the requirements for a sophisticated password (see 2.3 above) but password length should be increased from 12 characters to a minimum of 16 characters.

Other Top Tip's / Information

Tips

- On websites always type your password in incorrectly on your first log in – this will prevent you accessing rogue sites that are set up to pretend they are official sites
- Never provide your password in an email or verbally to another individual
- Never click on a link in an email that asks you to confirm your log on details
- Never choose the 'Remember my password' option when presented to you
- All factory-set default passwords should be changed before deployment
- Do not use the same password on school systems that you would use for your own personal use on websites
- Use the password reset tool if you forget your network password
- Never write your password down

Information

- 5 letter passwords have 10 billion possible combinations which mean it could be cracked in approximately 5 seconds.

- 6-character passwords could be cracked in approximately 500 seconds; 7 characters passwords could be cracked in approximately 13 hours and 8 character passwords could be cracked in approximately 57 days.

- If you feel your password has been compromised, please ensure this is reported to your IT support as soon as possible to enable your password to be reset.

- If you require further guidance on password management or any aspects of information security, then contact your Data Protection Officer.

Appendix 4

Cyber Security Policy

v1

FREQUENCY OF REVIEW:	**Annually**
COMMITTEE:	**Audit & Risk Committee**
RATIFICATION DATE:	**2nd December 2025**
DATE OF NEXT REVIEW:	**Autumn 2027 unless there is a material change**

Signed…… Date ……
Chair of Audit & Risk Committee

Signed …… Date ……
CEO

School Cyber Security Policy (v1)

Definition of Cyber Security: Application of technologies, processes and controls to protect systems, networks and data from cyber-attacks.

Introduction

The protection of information and communication technologies (ICT) within a school environment is paramount. This Cyber Security Policy aims to establish a framework for maintaining the security and integrity of digital resources, protecting personal data, and ensuring a safe digital environment for students, staff, and stakeholders.

This policy is aligned with the requirements of the Department for Education and National Cyber Security Centre.

Scope

This policy applies to all students, staff, governors and external partners, who have access to school ICT resources.

Objectives

- To protect the confidentiality, integrity, and availability of digital information.
- To safeguard the personal data of students, staff, and stakeholders.
- To ensure compliance with relevant legal and regulatory requirements.
- To foster a culture of cyber security awareness and responsibility.
- To respond effectively to cyber security incidents and breaches.

Roles and Responsibilities

School Administration

The administration is responsible for:

- Ensuring the development and implementation of the cyber security policy.
- Ensuring adequate resources are allocated for cyber security measures.
- Overseeing cyber security training and awareness programs.
- Reviewing and updating the policy periodically.

IT Support

IT support is tasked with:

- Maintaining and securing the school's IT infrastructure.
- Implementing technical measures to protect against cyber threats including:
    - Use of anti-malware and firewalls
    - Regular patching and software updates
    - Secure configuration of devices and networks

- Use of **Multi-Factor Authentication (MFA)** for staff and privileged accounts
- Controls over user accounts and access privileges including a review of accounts and prompt removal of leavers

- Monitoring network activity for potential security breaches.
- Responding to and mitigating the effects of cyber security incidents.
- Back-ups are periodically tested with at least one back up kept offline
- Provide web filtering and monitoring of internet access to prevent access to malicious sites

Staff

All staff members must:

- Adhere to the cyber security policy and procedures.
- Participate in cyber security training and awareness programs.
- Report any suspicious activities or security incidents.
- Safeguard their login password.
- Use **MFA** where possible

Students

Students have the responsibility to:

- Follow the school's cyber security guidelines and rules.
- Respect the privacy and security of others.
- Report any cyber security concerns to a teacher or other school staff.

Acceptable Use Policy

All users of the school's IT resources must adhere to the Information Security Policy, which includes:

- Using school IT resources for educational purposes only.
- Not accessing, sharing, or downloading inappropriate content.
- Respecting intellectual property rights and avoiding plagiarism.
- Not engaging in cyberbullying, harassment, etc.
- Protecting personal information and not sharing login details.

Data Protection

The school is committed to protecting the personal data it processes. Measures include:

- Where necessary, encrypting sensitive data to prevent unauthorised access.
- Regularly updating software and systems to address vulnerabilities.
- Implementing access controls to restrict data access based on roles.
- Conducting data audits to ensure compliance with data protection laws.

Cyber Security Training and Awareness

To ensure a culture of security:

- Training sessions will be conducted for staff and students.
- Awareness campaigns on the importance of cyber security will be promoted.
- Resources and materials on best practices will be made available.

Incident Response

In the event of a cyber security incident:

- The IT department will initiate an immediate investigation.
- Containment measures will be implemented to prevent further damage.
- Affected individuals will be informed promptly.
- A report detailing the incident and response actions will be documented.
- Preventative measures will be revised to avoid future occurrences.

In addition, all incidents and near misses will be reviewed with lessons learnt feeding into policy update and staff training.

Annual Cyber Risk Assessment

It is best practice to complete an annual Cyber Risk Assessment and undertake termly reviews of this assessment. An assessment should include:

- Identifying and prioritising critical assets
- Identifying threats and vulnerabilities
- Assess the likelihood and impact of each risk
- Evaluate existing controls relating to each risk
- Identify gaps and actions needed to fill these
- Assign responsibilities and timescales for each action
- Document your assessment and review
- Review assessment regularly

A simple example of a cyber risk assessment can be found on ***Appendix A*.**

Compliance and Review

Compliance with this policy is mandatory. The policy will be reviewed every 2 years or as required to:

- Ensure it covers evolving cyber security threats and best practices.
- Incorporate feedback from stakeholders.
- Adapt to changes in legal and regulatory requirements.

Conclusion

Cyber security is a collective responsibility. By adhering to this policy, the school can protect its digital resources, maintain the integrity of personal data, and create a safe and secure environment conducive to learning and growth. Let us all commit to fostering a culture of vigilance and responsibility in our digital interactions.

Further Reading

NSCS Cyber Essentials Framework - Cyber Essentials - NCSC.GOV.UK

NCSC Cyber Security for schools - Cyber Security for Schools - NCSC.GOV.UK

DfE Cyber Security Standards - Meeting digital and technology standards in schools and colleges - Cyber security standards for schools and colleges - Guidance - GOV.UK

LGfL Elevate Cyber Security Toolkit - Elevate Cyber Security Toolkit | LGFL

Example of a cyber security assessment

Asset	Threat	Vulnerability	Likelihood	Impact	Existing Controls	Action Needed	Deadline
Staff email	*Phishing*	*Lack of training*	*Medium*	*High*	*MFA*	*More training*	*Autumn term*