THE SHROPSHIRE GATEWAY EDUCATIONAL TRUST

Information Security Policy (ISP)
Version 6-22 Final

Author	Executive Headteacher
Review Cycle	Triennially
Date Approved	February 2023
Approved By	Heads board and Directors
Next Review Date	February 2026

Contents

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 school premises or at any other premises, including their home.

Who should read this policy?

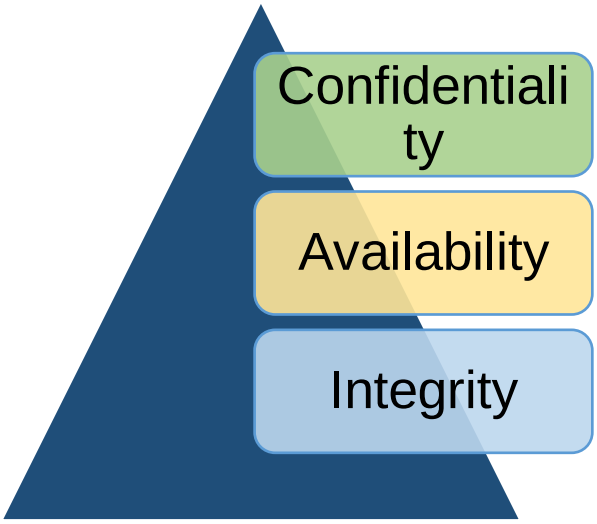
All Trust staff and Governors should read this policy.

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

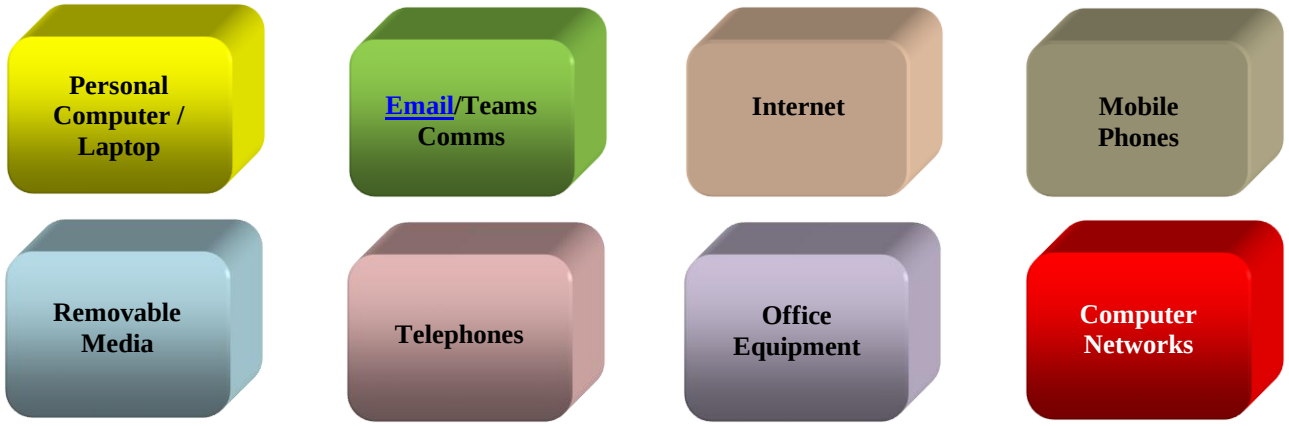
2.1 All employees within the Trust have a responsibility to ensure that they take steps to safeguard the security of the information that they are using and seeing.

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

3.1 The Trust 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 please see the appendices at the end of this policy. Employees should also ensure they are familiar with the requirements of other related policies on records management, data protection and social media.

4. Asset & Information Classification

4.1 In order to make sure that the Trust'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 Trust or the confidentiality of the personal and/or sensitive data that it holds.

5.3 The Trust will have put in place information sharing agreements where regular sharing of information from School/Trust 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 Trust's assets (including information) including securing their laptops, locking away sensitive information, etc.

6.2 The Trust 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 Trust 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/Trust 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/Trust 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. Leavers swipe cards / FOBs must be deactivated.

PHYSICAL ACCESS

Access to areas containing sensitive School/Trust 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 Trust'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
- Changed at the first opportunity from default assigned passwords
- 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 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

Passwords should NOT

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

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&W 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**:

- only use School equipment to do their work unless accessing authorised cloud services
- ensure that all equipment and information is kept secure at all times, 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

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 and Delivery Units

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 Trust's 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 Trust 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 Trust and extends to all places and all times, including outside work. Breaches of confidentiality can lead to summary dismissal within the Trust'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

12.1 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 licenses 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 Trust or any other organization

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 Trust 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 Trust, 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 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 Trust's/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 recognised cloud security standards.

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.

15. Business Continuity

15.1 The Trust has a process for management of business continuity.

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 Trust 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 Trusts Information Retention Schedule.

16.5 Data protection and personal information

16.5.1 All personal information managed by the Trust 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 Trust should conform to and also 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. Advice & Guidance

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

Appendix 1: S1 Acceptable Use of Equipment & Media (v6.22)

This section covers the acceptable use specific to work equipment that staff may use. It also covers staff using their own devices to access School services via O365. It is important that all staff are aware of the types of equipment that the School uses and what is acceptable and unacceptable. Any computer equipment, be it storage, computer, application or mobile phone must be purchased through authorised channels and be authorised to connect to the School's networks and systems. Computing resources not owned by the School must not be connected to the School's network unless via O365.

If you lose or have your ICT equipment stolen this is considered a security breach. The incident should be reported immediately to the Head Teacher and the Information Security Breach Procedure followed.

Personal Computer (desktop)/Laptop/Tablet Use

For personal computer/laptop tablet use staff must abide by the tables below.

Acceptable

Computers are provided to staff in order for them to carry out their role within the School/Trust
When left unattended staff should lock their computers so that they cannot be accessed by others. This is activated by pressing the ctrl-alt-del buttons simultaneously and selecting "Lock Computer" or holding down the windows key and pressing 'L'
Any media being used to transfer data from a laptop to another piece of School equipment must be procured via ICT and/or be encrypted.
Accessories and laptop or tablet PC equipment must be purchased through approved channels.

Unacceptable

Software must not be downloaded from the Internet without approval
Confidential information must not be accessed in a public place where unauthorised persons may view information displayed on the screen
Laptop and tablets must not be left unattended in an insecure area. The boot of a car is an acceptable storage place for mobile workers who have to leave equipment in a vehicle unattended for **short periods of time**. However, any School equipment including laptops and tablets **must not be left in a vehicle overnight** or over a weekend
Files of a personal nature, such as images for example, must not be stored on the local drive (more commonly known as the C drive) or on any network drives such as your homes (h) drive or shared network storage area
Staff must not allow access to their computer/laptop (when they are logged on) to any other staff members. The staff member logged in to the pc/laptop is responsible for any actions completed with their user id/password

Anti Virus

ICT Technician Responsibility	Officer 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.	Employees must: • 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 check 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

Multi-Functional Devices

Officer Responsibility: Employees must:

- Ensure work documents are not left unattended on the MFD
- Not leave a jam in the MFD in case when the jam is resolved their document prints unattended
- When using the scan to me option employees must ensure they check the receiving email address on the MFD is correct

Appendix 2: S2 Use of Email/Teams/Other Communication/Video Conferencing Technologies (v6.22)

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 Trust time and money. The Trust reserves the right to impose mailbox quotas on any or all staff in the event that storage becomes an issue.

IMPORTANT - Private Usage
Limited personal use of the School's email system, Teams and other communication technologies is acceptable but this use must be confined to outside an employees working hours and staff must still abide by School rules on acceptable and unacceptable use set out below.

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
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 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

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 of SMS (text)

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
- Only be used on a mobile phone provided by the School

A record should be held on a business record that the SMS communication has taken place.

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 must always be used wherever possible.
When using Microsoft Teams, the requirements of the SISP should be complied with.

Security & Monitoring

Security	Monitoring
• Private, confidential, personal or sensitive information should not be revealed or sent by email except to Shropshire Gateway Educational Trust staff and/or school staff also on the same email system. 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 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.	• If any emails are stopped by the content filter they may be read by an appropriate ICT officer, if the decision to stop the email is challenged. • The Trust 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 Trust. Separate legal proceedings may be necessary including seeking prosecution under the Computer Misuse Act 1990. • Email/saved Teams or other 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**

Appendix 3: S3 Use of Internet (v6.22)

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 employees must abide by the tables 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/Trust or its officers to the SBM/Head Teacher
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/Trust
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 infrastrucuture, including but not limited to: Video and audio files Photo searches Sexually explicit/pornographic Intolerance/hate Criminal action Tasteless/Offensive 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/Trust on any websites

Knowingly distribute or otherwise be involved in virus, Trojans or other malware use

Post School/Trust information on personal social media sites

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.

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

The School/Trust reserves the right to block access to any website deemed inappropriate and to report access of inappropriate material to the Head Teacher in the event that this type of activity is logged. Misuse of the internet can lead to disciplinary action being taken.

Appendix 4: S4 Mobile Phone Use (v6.22)

NOTE: Work devices must not to be used for personal purposes

The term mobile phone includes but not limited to:

Mobile Phones	Smart Phones	Other 'sound picture voice' (SPV) devices

These devices, as with all School/Trust equipment, are provided for work use only.

For mobile devices staff must abide by the tables below

Acceptable

Always use PIN security provided on phones
Conduct all verbal and text (where text is appropriate) conversations in a professional manner and within the School's/Trust's acceptable standards of behaviour
Be aware of your surroundings, e.g. do not discuss confidential matters where they could be overheard, i.e. on a crowded train
Ensure that all files stored on mobile devices are moved to the school's network so that they are backed up. Files should then be removed from the mobile device.
Close down the mobile device when not using it to prevent unauthorised access

Unacceptable

Never call or access inappropriate numbers, e.g. chat lines, premium rate numbers
Never use cameras on devices to take inappropriate, pornographic, obscene, discriminatory or otherwise offensive images
Never download unauthorised software including ring tones
Never allow anyone else to use the device including family, friends and children
Never leave the device unattended/unsecured or in a parked car
Do not use mobile devices whilst driving (unless using hands free facilities)

Monitoring of mobile devices

Mobile devices may be recalled at any time by the school to check compliance with this policy. All monitoring will be done in line with the Lawful Business Practice Regulations 2000.

Security of mobile devices

It is the user's responsibility to ensure that the physical device and any information stored on it is as secure as possible.

All School/Trust information must be regularly transferred to the school/trust networks to ensure it is backed up. Mobile devices are not automatically backed up.

If a device is lost or stolen it must be reported to the police immediately (if stolen) and a crime reference number obtained. It should then be reported to the Head Teacher as per the Information Security Breach Procedure.

Never attempt to factory reset your work mobile phone without ICT Technician support.

Appendix 5: S5 Removable/External Media Use (v6.22)

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

CD's (CR-R, CD-RW, etc)	DVDs (DVD-R, DVD-RW, etc)	USB memory sticks / pens	Removable drives	Non-School hosted storage such as Sky Drive	Mobile phones

The introduction of O365 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

Only use encrypted removable/external media provided through authorised channels.

Ensure that CDs and DVDs are "clean", if not new; i.e. all previous information has been deleted.

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 Head Teacher.

Appendix 6: S6 Telephone Use (v6.22)

School based telephone equipment includes, but is not necessarily limited to:

Phone handsets and headsets	Answer machines and voicemail	Fax machines	Virtual phones	Modems	Modems	Switches and switchboards	Contact Centres

The following conditions must be followed:

Acceptable

Be supplied by the school and will remain the property of the school at all times.

Only be relocated by ICT staff via an ICT Technician.

Wherever possible, unattended phones must be forwarded to other available staff or a works mobile phone. Voicemail is available if there is a business need, for example to inform callers of outside-hours emergency numbers. This should be authorised by the SBM/Head Teacher.

Analogue phone lines are still required, for example for remote alarm systems and as a backup to the existing phone system. ICT Technician must be involved in all contracts for analogue lines.

Unacceptable

Work telephones must not be used for personal use

Users must not log into the softphone solution on a non-work device

Appendix 7: S7 Office Equipment Use (v6.22)

Office equipment acceptable use

- Office equipment in the form of printers, scanners, fax machines, photocopiers, multifunctional devices, cameras and video cameras are provided for official use only.
- Staff must comply with trademark and copyright regulations when making copies of documents.
- The transfer of images (sending, emailing, and copying) should be limited wherever possible as this greatly increases the cost per use of the device. Permission of people appearing in images must be given before sending these.
- Scanners should not be used to scan sensitive or confidential documents without due regard to the storage of such information (records management).
- When scanning documents for archiving, advice should be taken in respect of retention schedules for the storage and deletion of the information. Advice can be obtained from the Data Protection Officer.
- Unacceptable use of office equipment may result in disciplinary action being taken. Any illegal use such as printing, copying, scanning information that may be considered obscene, pornographic or discriminatory will be reported to the Police.
- Images scanned can be viewed by the school through the network. Cameras and video cameras may be recalled at any time for the school to monitor any images taken.

Appendix 8: S8 Computer Networks Use (v6.22)

Computer networks include:

- virtual private networks (VPN)
- direct access
- 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 schools 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

- As mentioned elsewhere in this policy 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.
- The "home drive" (commonly known as the H: drive) on the school network, is a networked storage area specifically for an individual to store information. The H drive is normally backed up however; **confidential information must not be stored here** as school ICT reserve the right to not backup these drive(s). This also applies to the use of One Drive.
- 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 specified in section 6 is not allowed and will result in disciplinary action and where appropriate, police action.
- Any information stored on network drives may be monitored and opened in line with the Lawful Business Practices Regulations 2000.
- 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 or not 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

ICT will backup school systems in line with their backup policies and procedures. Users should be aware that all confidential and critical information should be stored on the corporate networks. The "local drives" on PC's (commonly referred to as the C: drive) are not backed up by ICT. ICT also reserves the right to reduce the backup frequency, or cancel backups of the "home drive" (commonly known as the H: drive). If this becomes the case all affected staff will be informed and asked to move critical files to other locations on the network.

OneDrive is not backed up by Microsoft, however if any file is deleted, it can be recovered via the recycle bin in OneDrive. Data stays in the recycle bin for up to 6 months and can be recovered as long as the item is not permanently deleted from the recycle bin.

Other ICT Responsibilities

ICT will undertake the following tasks in respect to school networks:

- Ensure that server configuration/security complies with relevant server configuration/security standards
- Ensure that patches are applied to all relevant servers on a timely basis relevant to their release
- Ensure that appropriate change control processes are followed in respect to server changes
- Provide router/switch management services
- Use diagnostic tools to ensure networks are running securely at optimum levels
- Ensure up to date and fit for purpose anti-virus solutions are deployed on school servers and end user work devices.

Appendix 9 - 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** _____

Document Version Control

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