



The Evolution and Henslow School Record Management and Security Policy

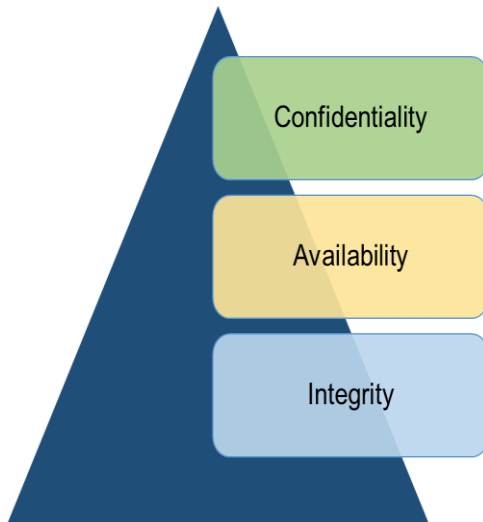
Contents

| Section | Page |
|--|------|
| 1 introduction | 3 |
| 2 roles & responsibilities | 3 |
| 3 acceptable & non acceptable use | 4 |
| 4 information sharing | 5 |
| 5 physical & environmental | 6 |
| 6 loss or theft of equipment/files & information | 8 |
| 7 staff/user access management | 8 |
| 8 working from home & mobile working overview | 10 |
| 9 Records Management | |
| 10 security responsibility for staff | 10 |
| 11 monitoring system access, use and auditing | 11 |
| 12 Communication Management | 11 |
| 12 outsourcing | 12 |
| 13 systems development & maintenance | 13 |
| 14 business continuity | 13 |
| 15 legal, regulatory & contractual compliance | 14 |
| 16 advice & assistance | 15 |

Appendix 1 – Data retention timescales

1. Introduction

- 1.1 Information can exist in many forms. It can be printed, written, stored electronically, transmitted by post, email, social media 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.

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 GDPR, data protection and Information Sharing Policy
- 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:

3.1 Emails

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 in the event that 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
- 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.

3.2 Mobile phones

Unless specifically specified work mobile phones should not be used for personal use

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 Schools 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 schools 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 number
- 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 information must be regularly transferred to the school 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

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; within a contact record or similar.

3.3 Internet

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

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/Head Teacher/line manager
- 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
 - 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. For more guidance on the appropriate use of social media sites please see the Social Media Policy
 - 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

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:

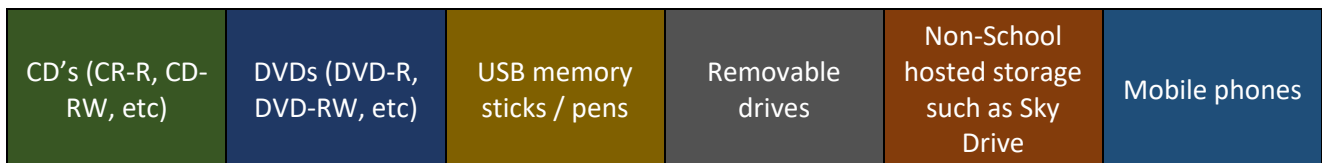
- gaining routine access to business communications
- monitoring standards of service and training
- prevention or detection of crime
- detecting unauthorised use of the internet.

Employees must be aware that the School 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 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.

3.4 Removable media

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 Head Teacher 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.

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 Support 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 Head Teacher.

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

4. Information Sharing

4.1 Schools Policies 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 this information.
- Investigate whether the objective can be met without sharing this information.
- Only send the minimum information 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.

4.2 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.

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

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

4.5 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

5. Physical and Environmental Security

- 5.1 All employees have a responsibility for the physical security of School's assets (including information) including securing their laptops, locking away sensitive information, etc.
- 5.2 The school will be responsible for the provision of suitable physical, technical, procedural and environmental security controls in order to prevent unauthorised access to, interference with, or damage to information.

5.3 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 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 in the induction process and reviewed where required during employment.

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. Where required restricted access to areas should be employed to prevent information being viewed.

5.4 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.



5.5 Security of premises

5.5. Premises security consists of:

IDENTITY BADGES

All staff are issued with identity cards which include their photograph and these must be worn visibly at all times where sites include a variety of staff and are open E.g. Fitzroy. In contained sites staff do not need to wear ID but must have this on them for off site visits. In some settings wrist bands may be worn to prevent accidental or deliberate injury by students with additional needs.

Staff must question anyone in any School building not wearing identification (visitors and contractors will be wearing a suitable Identify card) 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 some School premises is controlled by the issue of security passes or FOB's. Leavers swipe cards / FOBs must be collected and accounted for.



PHYSICAL ACCESS

Access to areas containing sensitive School information must be strictly controlled and given on a need to know basis.

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.

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

6.1 In the event of any loss/theft of equipment, files and information, the School's GDPR/Data Protection and information sharing policy should be followed. The key immediate actions include:

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

7. Staff/User Access Management

7.1 Staff registration

- 7.1.1 The Head Teacher 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.

7.2 Password responsibilities

- 7.2.1 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
- 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.

7.3 Leaving procedure

- 7.3.1 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 personal 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

7.4 Non-electronic media

- 7.4.1 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 retention timescales listed in appendix 2

7.5 Disposal of equipment

7.5.1 ICT equipment for disposal must be disposed of securely either by T&WC ICT or other reputable disposal company who should provide a record of correct disposal. ICT equipment no longer required must not be used by staff for personal use.

7.6 Third party access to systems

7.6.1 It is the responsibility of the Head Teacher in conjunction with IT Management company/Person 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.

7.6.2 It is the responsibility of the Head Teacher to advise the IT Management company/Person as soon as the third party access is no longer required.

7.7 Internet and intranet web publishing

7.7.1 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.

7.7.2 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.

7.7.3 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.

8. Working from Home and Mobile Working Overview

8.1 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 the person remains school based. | Person’s normal place of work is their home and they do not visit the school daily. | Person 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 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 IT Management Company/Person

8.2 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.

- 8.3 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.
- 8.4 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.






9 Record Management

Easy retrieval of information is crucial to the school operating effectively and forms part of records management. The following requirements of record keeping should be complied with:

-  Records should be organised in clearly named folders/files
-  Electronic records should be held within shared drives. This means that work information that other staff may need access to should NOT be saved on the hard drive (c:\ drive), homes drive (h:\drive) or on individuals email accounts
-  Duplication of records should be avoided at all costs
-  Records, where possible, should be updated at the time an activity has occurred
-  Record keeping should take into account the requirements of the Freedom of Information Act 2000 in respect to individuals having the right to ask for school information
-  Where records are held on EDMS (Electronic Document Management Systems) consideration should be given to their legal admissibility

9.1 Record Maintenance



The maintenance of records can cover a multitude of activity including movement of records, storage, contingency, etc. The following requirements of record maintenance should be complied with:

-  Tracker systems implemented to control and log the movement of hard copy records
-  Adequate secure storage arrangements are in place which protects the quality and accessibility of records. Access to records stored should be on a need to know basis
-  Business continuity plans are in place that document the arrangements for the protection of records and detail a 'plan B' if records are unavailable for a prolonged period
-  Adequate back up arrangements are in place to ensure a seamless resumption of service in the event that back up copies of records are required
-  Where records have not been required for live processing for a considerable time (and are still within required retention periods) consideration should be given to archiving them.

9.2 Record Access

- 9.2.1 Records are accessed for conducting school business or for legislative reasons (FOI, Data Protection, etc.).

The following requirements of record access should be complied with:

-  Access levels to records are reviewed on a regular basis
-  Access is promptly revoked when it is no longer required

- ✔ Access to records is facilitated via a secure method, e.g. electronic records via a userid and password as a minimum, hard copy records access via the use of a key, security pass, etc
- ✔ Right of access requests via FOIA, DPA and EIR (Environmental Information Regulations) should be channelled through the School Business Manager

9.3 Record Disclosure

9.3.1 There are a number of legislative provisions that limit or set conditions for the disclosure of information, particularly in respect to personally identifiable information. It is therefore important that consideration is given to whether there is a sound legal basis for disclosing records before they are actually disclosed.

The following requirements of record disclosure should be complied with:

- ✔ The schools Information Sharing Policy is adhered to
- ✔ Decisions on disclosure of records containing personal information are made by appropriately qualified staff with the Information Asset Owner being aware of the decision making process and/or the actual decision made
- ✔ A record should be maintained of what records have been disclosed, to who, when and on what basis disclosure was made

9.4 Record Closure

9.4.1 The closure of a record and its subsequent treatment needs to be made on a consistent basis.

The following requirements of record closure should be complied with:

- ✔ Services should set criteria for when a records status changes from live to closed
- ✔ Arrangements are in place to archive records where possible
- ✔ If there is further activity in respect to the main subject of the closed record, a decision should be made by as to whether the closed record should be reactivated or a new record set up

9.5 Record Disposal/Archiving

9.5.1 The importance of the correct secure disposal/archiving of records cannot be underestimated particularly in regard to personally identifiable information.

The following requirements of record disposal should be complied with:

- ✔ The schools retention policy is adhered to
- ✔ Arrangements are in place to either flag up records that are due for disposal or to instigate a manual review to identify such records
- ✔ Disposal is only in a secure manner in compliance with school requirements, e.g. hard copies disposed of via school shredders, electronic records disposed of via IDT
- ✔ Where records are archived via EDMS (Electronic Document Management Systems) consideration should be given to the legal admissibility of such documents if they were ever required to be used as legal evidence
- ✔ Access to archived records should be clearly defined and established on a need to know basis



Archived records should be reviewed on a periodic basis to establish if these records should be maintained or permanently disposed of.

10. Security Responsibilities for Staff

10.1 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

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

10.1.3 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.

10.1.4 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.

10.1.5 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.

10.1.6 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.

10.1.7 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/teams 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

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 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 are made aware on reading this policy 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 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 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 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. **Please refer to the Business Continuity Policy**

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 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 retention periods detailed in the Schools Data 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 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 Head Teacher and Data Protection Officer

| | | |
|----------------------------|------------------------|---------------------------|
| Reviewed by: | J Brooks/A. Clarke | Date: January 2024 |
| Last reviewed on: | Implemented April 2024 | |
| Next review due by: | April 2025 | |

Appendix 1

Data retention timescale table

Appendix 1 - Data Retention Schedule

| Data type and action once not required | Short term retention Event + half a term | Medium term Leaver = 1 year | Long term Until student is 25 years old | Very Long term As per care 75 years | Reasoning |
|---|---|--------------------------------|--|--|---|
| Admissions Information Shred/delete soft files | | | ✓ | | Mostly used in the initial stages and up to the first few weeks of admission. Some validation and checking of information whilst student is on role. Information then becomes part of the central record held on Schoolpod and should be held here. |
| Attainment information Shred/delete soft files | | ✓ (formative) | ✓ (summative) | | Formative assessment – only required whilst student is on role + 1 year. Summative assessment is the main outcome of the schools work with the student, may be required for future queries/concerns. |
| Attendance Request Schoolpod delete record | | | ✓ | | Part of the school's main role and could be required in legal proceedings. Kept on Schoolpod as an electronic record. |
| Behaviour and exclusions Request Schoolpod delete record | | | ✓ | | May form part of any legal proceedings. Kept on Schoolpod as an electronic record. |
| PEP's EHCP's and annual reviews, LAC's and similar | | | ✓ | | Scanned to Schoolpod to be kept electronically, May be needed to evidence decisions taken and provision offered. |
| Identity management | | ✓ | | | Used for initial checks of identity |

| | | | | | |
|---|-----------------|---|---------|--------------------------|---|
| (photo of student) Request Schoolpod delete record/ delete soft files | | | | | and may be required for any exams sat externally. Not required after this. |
| Trips and activity records Request Schoolpod delete record | ✓(trip details) | | | ✓ (incident or accident) | Once the trip returns safely, log attendance but nothing further required. If there is an accident or incident this will be logged in case of future legal action on the Schoolpod system. |
| Safeguarding Shred/delete soft files | | | | ✓ | Part of an important story that may need to be referred to for a long time. |
| On role register containing basic personal information Request Schoolpod delete record | | | ✓ | | May be required for references and to prove dates on school role, potential for legal action requiring this information. |
| Minutes of school meetings Shred/delete soft files | | ✓ | | | Any key information is transferred to other reports anyway. Information may be required by three yearly OFSTED. |
| Office and Headteacher records relating to individual student Shred/delete soft files | | ✓ | | | Unless relating to a serious matter. |
| Examination results | | | ✓ | | Students often lose certificates and need proof of qualifications |
| BTEC course related materials | | | 3 years | | BTEC stipulated |