THE BISHOP'S STORTFORD HIGH SCHOOL

DATA SECURITY POLICY

Date of last review:	September 2026
Date of next review:	September 2027
Review period:	1 Year
Owner:	Governing Body
Approval:	

The Bishop's Stortford High School Data Security Policy

1. Policy statement and objectives

1.1 The objectives of this Data Security Policy are to ensure that The Bishop's Stortford High School and its governors/ staff/volunteers/students/contractors are informed about, and comply with, their obligations under the UK General Data Protection Regulation ("the UK GDPR") and other data protection legislation.

1.2 The School is the Data Controller for all the Personal Data controlled/processed by the School.

1.3 The purpose of this policy is to inform everyone about their specific responsibilities in maintaining and improving security standards and data management, through their working practices and day-to-day interaction with the School's ICT systems.

1.4 We hold personal data on students, staff and others to allow the School to conduct its day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can also result in media coverage and potentially damage the reputation of the School, its staff and students. Therefore everybody has a shared responsibility to be mindful about data security when they are going about their daily activities and consider how data security risks and threats can be minimised.

1.5 The policy applies to all staff of the School whether temporarily or permanently employed as well governors, volunteers and students. It also applies to contractors engaged by/working with the School or who have access to information held by the School.

1.6 The School should ensure all staff are aware of and understand the content of and their responsibilities within this policy. If any staff member is found to have breached this policy, they could be subject to the Disciplinary and Dismissal Policy & Procedure. Students should also be made aware of Data/Computer Security and breaching this policy could be subject to student disciplinary procedures.

1.7 The policy applies to all locations from which the School systems are accessed by governors/staff/volunteers/students including remote use and the use of portable devices.

2. Status of the policy

2.1 This policy has been approved by the Governing Body of the School. It sets out our rules on data security and the legal conditions that must be satisfied in relation to the secure handling, processing, storage, transportation and destruction of personal information.

3. Network/Server Security

3.1 Servers must be physically located in an access-controlled environment. Unrestricted access to the computer facilities will be confined to designated staff whose job function requires access to that particular area/equipment. Restricted access may be given to other staff or third party support where there is a specific job function need for such access (Eg: fixing a particular specialist application installed on a particular server at a particular time. Such access will be monitored and logged).

3.2 The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.

3.3 Servers must have security software (Anti-Virus and Anti-Spyware) installed appropriate to the machine's specification.

3.4 Servers must always be password protected, and locked when not in use.

3.5 Security-related events must be reported to the Network Support Team (IT Team) and to the DPO, using our standard reporting procedures. Corrective measures will be prescribed as needed. Security-related events could include, but are not limited to, port-scan attacks, evidence of unauthorised access to privileged accounts.

3.6 IT infrastructure such as routers, switches, wireless access points etc. must be kept securely and only be handled by authorised personnel.

3.7 Backup Procedures:

- 3.7.1 Backup software must be scheduled to run routinely, as required, to capture all data as required. For most systems this is at least once a day.
- 3.7.2 Backups must be monitored to make sure they are successful. For most systems this is at least once a day.
- 3.7.3 A test restoration process will be run regularly. For most systems this is at least once a month.
- 3.7.4 Non-Cloud Backup media must be securely stored in a fireproof container.
- 3.7.5 Backup media stored off-site must be transported and stored securely.

4. Workstation Security

4.1 Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitive information is restricted to authorised users, including:

- 4.1.1 Restricting physical access to workstations to only authorised users. Offices and classrooms are not to be left unlocked when unattended/unsupervised.
- 4.1.2 Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorised access.
- 4.1.3 Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected.
- 4.1.4 Complying with all applicable password expectations and procedures. For example, passwords not written down at all and most definitely not attached to monitor screens.
- 4.1.5 Ensuring that monitors are positioned away from public view. If necessary, install privacy screen filters or other physical barriers to public viewing.

4.1.6 Ensuring workstations are used for authorised purposes only. Anyone who is not authorised to access our network must only be allowed to use terminals under supervision.
4.1.7 Never installing unauthorised software on workstations.
4.1.8 Storing all confidential information on network servers.
4.1.9 Complying with the Anti-Virus policy. (ie: Not disabling the virus checker).

5. Password Security

5.1 Requirements:
5.1.1 All system-level passwords (Administrator, etc.) must be changed from any generic default, and then reset when required (e.g. on a regular basis and most definitely after a suspected breach).
5.1.2 All user-level passwords (e.g. email, web, desktop computer, etc.) must be changed from any generic default, and then reset when required (e.g. on a regular basis and most definitely after a suspected breach, or after a change in staffing).
5.1.3 Good practice recognises passwords should be rotated at a minimum of every 90 days.
5.1.4 All user-level and system-level passwords must conform to the standards described below.

5.2 Standards - All users should be aware of how to select strong passwords. Strong passwords have the following characteristics:
5.2.1 Contain at least eight alphanumeric characters.
5.2.2 The password is NOT a word found in a dictionary (English or foreign).
5.2.3 The password is NOT a name or common pattern (e.g. 12345678).
5.2.4 Passwords could also contain several of the five following character classes: Lower case characters; Upper case characters; Numbers; Punctuation; "Special" characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/). However, this should only be used in conjunction with the above rules ('P4ssw0rd' is no more secure than 'Password').

5.3 Protective Measures
5.3.1 Do not share passwords with anyone. All passwords are to be treated as sensitive, confidential information.
5.3.2 Passwords should never be written down, unless securely stored, or stored electronically without encryption.
5.3.3 Do not reveal a password in email, chat, or other electronic communication.
5.3.4 Do not speak about a password in front of others.
5.3.5 Always decline the use of the "Remember Password" feature of applications.
5.3.6 Where Single Sign On is not available you should use a different password for each system.

6. Access Control

6.1 All users must only access systems for which they are authorised. Under the Computer Misuse Act 1990 it is a criminal offence to attempt to gain access to computer information and systems for which they have no authorisation.

6.2 All contracts of employment and conditions of contract for contractors should have a non-disclosure clause, which means that in the event of accidental unauthorised access to information (whether electronic or manual), the member of staff or contractor is prevented from disclosing information which they had no right to obtain.

6.3 Permission to access restricted systems must be initially sought from the Network Support Team (IT Team), who may in turn have to refer some requests to the relevant SLT link if there are further considerations need to be made.

6.4 Users must pay particular attention to the return of items which may allow future access. These include personal identification devices, access cards, keys, passes, manuals and documentation. They must be personally returned to a member of the Network Support Team and not just left somewhere to be picked up later.

6.5 Line managers should ensure that all PC files of continuing interest to the business of the School are transferred to another user before a staff member leaves their employment (ie: Check files [particularly commercially-sensitive/financial data] have been most definitely uploaded to the network where they should already be stored anyway).

6.6 Any contractors (working on site or working remotely via a communications link) to maintain or support computing equipment and software for the School must comply with the terms of this policy and any access control measures with which they are requested to comply with by School staff. They should be monitored/escorted at all times.

6.7 Physical security to all office areas must be maintained. Staff should feel confident about challenging strangers in the office areas without an ID badge.

6.8 Clear Desk Policy:
6.8.1 Staff are required to clear working documents, open files, and other paperwork from their desks, working surfaces and shelves when they are not being used and to place them securely into desk drawers and cupboards as appropriate.
6.8.2 Although security measures are in place to ensure only authorised access to office areas, staff members must ensure that documents, particularly of a confidential nature are not left lying around.

7. Security of Portable Equipment and Mobile Devices

7.1 All Users using portable computers/laptops must have appropriate access protection, for example passwords and encryption.

7.2 Devices must not be left unattended in public places or left in unattended vehicles at any time. Users are also responsible for the security of the hardware and the information it holds at all times on or off School property. The equipment must only be used by the individual to which it is issued, be maintained and batteries recharged regularly.

7.3 Staff must always secure laptops, handheld equipment and any removable media when leaving an office unattended and lock equipment away when leaving the office.

7.4 Users working from home must ensure appropriate security is in place to protect equipment or information not be used by non-School users. This will include ensuring equipment and information is kept out of sight.

7.5 Users must ensure that any machine not routinely connected to the school network, is switched on regularly to receive critical updates. If an update fails the machines must be brought in to the Network Support Team (IT Team) as soon as possible.

7.6 Staff must ensure that all school data is stored on the school network, and not kept solely on the laptop and must synchronise all locally stored data with the School network server on a frequent basis.

7.7 Mobile Computing and Storage Devices include, but are not limited to: laptop computers, plug-ins, Universal Serial Bus (USB) port devices, Compact Discs (CDs), Digital Versatile Discs (DVDs), flash drives, smartphones, tablets, wireless networking cards, and any other existing or future mobile computing or storage device, either personally owned or School owned, that may connect to or access the information systems at the School. These devices are easily lost or stolen, presenting a high risk for unauthorised access and introduction of malicious software to the IT network. These risks must be mitigated to acceptable levels:

7.7.1 Encryption - portable computing devices and portable electronic storage media that contain confidential, personal, or sensitive information must use encryption to protect the data while it is being stored.

7.7.2 Database or portions thereof, which reside on the network shall not be downloaded to mobile computing or storage devices.

7.7.3 Report lost or stolen mobile computing and storage devices immediately to the Network Support Team (IT Team) and/or the DPO.

7.7.4 Non-departmental owned device that may be needed to connect to the School network must first be approved by the Network Support Team (IT Team).

8. Printing, Copying and Transmission of Data

8.1 It is the responsibility of individual users to ensure the security of any personal, sensitive, confidential and classified information contained in documents emailed, faxed, copied, scanned or printed. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used.

8.2 Anyone sending a confidential or sensitive fax must notify the recipient before it is sent.

8.3 Users should ensure that the entire document has copied or printed and check that the copier has not run out of paper. This is particularly important when copying or printing large documents.

8.4 Users should not leave the printer unattended when using it, as another person may pick up the printing by mistake.

8.5 When sending data, the most secure method of transmission must be selected, especially where information is particularly sensitive or confidential. All Users must consider the risk of harm or distress that could be caused to the relevant data subject if the information was lost or sent to another person, then look at the most appropriate way of sending the information to the recipient.

8.6 Send only the minimum amount of personal or sensitive information, by whichever method is chosen.

8.7 Sending information by email:

8.7.1 Carefully check the recipient's email address before pressing send - this is particularly important where the 'to' field autocompletes.

8.7.2 If personal or sensitive information is regularly sent via email, consider disabling the auto complete function and regularly empty the auto complete list.

8.7.3 Take care when replying 'to all' - do they really all need to receive the information being sent.

8.7.4 If emailing sensitive information, password protect any attachments. Use a separate email or different method to communicate the password e.g. telephone call.

8.7.5 When sending sensitive files, consider the use of secure file transfer systems where available, such as Schoolsfx or HertsFX (Hertfordshire schools).

8.8 Sending information by post:

8.8.1 Check that the address is correct.

8.8.2 Ensure only the relevant information is in the envelope and that someone else's letter has not been included in error.

8.8.3 Consider using tracking, particularly when sending sensitive information, e.g. recorded delivery or a courier if appropriate.

9. Use of Email

9.1 The School gives all Users (governors/staff/volunteers/students) their own email account to use for all School business as a work based tool. This is to protect users, minimise the risk of receiving unsolicited or malicious emails and to avoid the risk of personal profile information being revealed.

9.2 Staff and governors should use their school email for all professional communication.

9.3 Take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Remember that you have no control over where your email may be forwarded by the recipient. Avoid saying anything which would cause offence or embarrassment if it was forwarded to colleagues or third parties or found its way into the public domain.

9.4 Email messages are required to be disclosed in legal proceedings or in response to a subject access request in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable, either from the main server or using specialist software.

9.5 Monitoring - School email users shall have no expectation of privacy in anything they store, send or receive on the School email system. The School may monitor messages without prior notice.

9.6 It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced.

9.7 Under no circumstances should staff contact students, parents or conduct any school business using personal email addresses.

9.8 All emails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.

9.9 Staff should avoid sending or forwarding attachments unnecessarily. Whenever possible, the location path to the file on a shared drive should be sent instead.

9.10 Where appropriate, staff sending emails to external organisations, parents or students are advised to cc. the Headteacher, line manager or designated line manager.

9.11 When emailing confidential/personal data, obtain express consent from a manager to provide the information by email and exercise caution when sending by performing the following checks:

- 9.11.1 Encrypt and/or password protect attachments. Provide the encryption key or password by a separate contact with the recipient(s).
- 9.11.2 Verify the details, including accurate email address, of any intended recipient of the information. Do not copy or forward the email to any more recipients than is absolutely necessary.
- 9.11.3 Verify the details of a requestor before responding to email requests for information.
- 9.11.4 Consider using other secure file transfer methods, such as HertsFX or SchoolsFx (Hertfordshire schools).
- 9.11.5 Request confirmation of safe receipt.

9.12 The School email system shall not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, sex, hair colour, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any School employee must report the matter immediately. The following activities are strictly prohibited, with no exceptions:

- 9.12.1 Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- 9.12.2 Any form of harassment via email, telephone or messaging, whether through language, frequency, or size of messages.
- 9.12.3 Creating or forwarding "chain letters", "joke" emails, or "pyramid" schemes of any type.

9.13 Users should actively manage their email account by:

- 9.13.1 Checking emails regularly.
- 9.13.2 Deleting all emails of short-term value.
- 9.13.3 Organising email into folders and carrying out frequent house-keeping on all folders and archives.
- 9.13.4 Activating an out-of-office notification when away for extended periods.

9.14 Personal Use - using a reasonable amount of School resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email.

9.15 The School email account should not be used for personal advertising.

9.16 All the above apply whether accessing the School email account onsite, or through webmail or on non-School devices.

10. Data Breaches

10.1 The Information Commissioner's Office (ICO) has the power to serve notices requiring organisations to pay up to €20 million or 4% of annual global turnover, whichever is higher, for serious breaches of the UK GDPR and Data Protection Act 2018.

10.2 Users are responsible for:

- 10.2.1 Ensuring that no breaches of information security result from their actions.
- 10.2.2 Reporting any breach, or suspected breach of security without delay.
- 10.2.3 Ensuring information they have access to remains secure. The level of security will depend on the sensitivity of the information and any risks which may arise from its loss.
- 10.2.4 Ensuring they are aware of and comply with any restrictions specific to their role or service area. All staff should be aware of the confidentiality clauses in their contract of employment.

10.3 Advice and guidance on information security can be provided by the School DPO and/or Data Protection Lead.

10.4 A breach or suspected breach of policy by a school employee, contractor or student may result in the temporary or permanent withdrawal of School ICT hardware, software or services from the offending individual.

10.5 For staff any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure or, for Support Staff, in their Probationary Period as stated. Policy breaches may also lead to criminal or civil proceedings.

10.6 If a member of the School (governor/staff/volunteer/student) knows or suspects that a Personal Data Breach has occurred, then the actions in the Data Security/Breach Response Plan must be followed. In particular, the DPO or such other person identified in the Data Security/Breach Response Plan must be notified immediately.

10.7 Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's relevant responsible person. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person.

11. Disposal of Redundant ICT Equipment Policy

11.1 All redundant ICT equipment will be disposed of through an authorised agency. This must include a written/electronic receipt for the item including an acceptance of responsibility for the destruction of any data/software.

11.2 All redundant ICT equipment that may have held personal data will have the storage media overwritten multiple times to ensure the data is irretrievably destroyed. If the storage media has failed it will be physically destroyed. The School will only use authorised companies who will supply a written guarantee that this will happen.

11.3 Disposal of any ICT equipment will conform to: the Waste Electrical and Electronic Equipment Regulations 2018, the Data Protection Act 2018, the Electricity at Work Regulations 1989.

11.4 The School will maintain a comprehensive inventory of all its ICT equipment including a record of disposal. This will include:

11.4.1 Date item disposed of.

11.4.2 Authorisation for disposal, including: verification of software licensing, any personal data likely to be held on the storage media.

11.4.3 How it was disposed of e.g. waste, gift, sale.

11.4.4 Name of person and/or organisation who received the disposed item.

11.5 Any redundant ICT equipment being considered for sale/gift will have been subject to a recent electrical safety check and hold a valid PAT certificate.

12. Other Points and Legal Requirements

12.1 While the School's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the systems remains the property of the School.

12.2 Users must pay particular attention to the protection of personal data and commercially sensitive data. All sensitive files must be Password protected, at a minimum, aligned with the password policy and where technologically possible encrypted both at rest and in transit.

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

12.4 Authorised staff may inspect any ICT equipment owned or leased by the school at any time without prior notice. If staff are in doubt as to whether the individual requesting such access is authorised to do so, they should ask for their identification badge and contact their department. Any authorised staff member will be happy to comply with this request.

12.5 Authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, emails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain School business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of the ICT systems; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 2018, or to prevent or detect crime.

12.6 Authorised staff may, without prior notice, access the email or voicemail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

12.7 All monitoring, surveillance or investigative activities are conducted by authorised staff and comply with the Data Protection Act 2018, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2018 (RIPA) and the Lawful Business Practice Regulations 2000.

12.8 Please note that personal communications using School ICT systems may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

12.9 All users must use extreme caution when opening email attachments received from unknown senders, which may contain viruses, email bombs, or Trojan horse code.

12.10 If it is suspected that there may be a virus on any School ICT equipment, users should stop using the equipment and contact the Network Support Team (IT Team) immediately. They will advise what actions to take and be responsible for advising others that need to know.

12.11 It is imperative that users do not access, load, store, post or send from School ICT system any material that is, or may be considered to be: illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the School or may bring the School into disrepute. This includes, but is not limited to: jokes, chain letters, files, emails, clips or images that are not part of the School's business activities; sexual comments or images, nudity, racial slurs, sex specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Equality Act 2010).

12.12 Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act or a Subject Access Request.

12.13 Where necessary, permission should be obtained from the owner or owning authority and any relevant fees paid before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1988.

13. Policy Review

13.1 It is the responsibility of the Governing Body to facilitate the review of this policy on a regular basis, and at least annually or if any new technologies are introduced. Recommendations for any amendments should be reported to the DPO.

13.2 The School will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.

14. Enquiries

14.1 Further information can be found in the Online Safety policy and the Data Protection Policy.

Data Protection Officer / ICO

We have a Data Protection Officer (DPO) to oversee our moral and legal obligations with the handling of Personal Data. If you have any questions about this document or how we handle personal information, please contact our Data Protection Officer. If you have a concern about the way we are collecting or using personal data, we request that you raise your concern with us in the first instance.

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

You can contact the school by email, letter or telephone. The contact details are set out below. To help us process your request within expected legal timescales, please clearly mark any correspondence "DATA PROTECTION OFFICER" (in CAPITALS please).

DATA PROTECTION OFFICER	
The Bishop's Stortford High School	Email: dpo@tbshs.org
Beaumont Avenue	
Bishop's Stortford	Telephone: +44 (0) 1279 868686
Hertfordshire	
CM23 4SH UK	

Document Control

Date modified	Description of modification	Modified by
2023-10-08	Major Version 001a (Based on Hertfordshire For Learning format)	AJO
2024-09-02	Major Version 002a (New School address and various HFL updates)	AJO
2024-12-29	Minor Version 002b (Minor amendments for new School site)	AJO
2025-02-28	Minor Version 002c (Minor amendments for new School site)	AJO
2025-03-24	Minor Version 002d (Minor amendments for new School site)	AJO
2025-07-03	Minor Version 002e (PBS amendments for new School site)	AJO/PBS
2025-10-05	Minor Version 002f (Check against Hertfordshire For Learning format)	AJO
2025-10-10	Major Version 003a (Annual Review - Fast Technology Advancements/JCQ)	AJO/PBS
2026-02-19	Minor Version 003b (Minor amendment - Dates)	AJO
2026-03-04	Minor Version 003c (Further standardisation of formatting)	AJO
2026-06-12	Major Version 004a (Grooming Gang Inquiry data retention / DPO correction)	AJO
2026-07-29	Major Version 005a (Annual Review / Footer Change / Iris Connect Removal)	AJO