GDPR Data Security Policy

Start Date:	**Autumn 2021**
Date of Next Review:	**Autumn 2024**
Author:	**Ms J Howard**
Responsible Committee:	**Finance & Resources Committee**

GDPR Data Security Policy

1. Policy statement and objectives

1.1 The objectives of this Data Security Policy are to ensure that Haileybury Academy Trust and its governors and employees 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 a Trust school and is the Data Controller for all the Personal Data controlled/processed by the Trust.

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

1.4 We hold personal data on pupils, staff and others to allow the Trust to conduct its day-today 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 Trust, its staff and pupils. 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 Trust whether temporarily or permanently employed. It also applies to contractors engaged by/working with the Trust or who have access to information held by the Trust.

1.6 The Trust should ensure all staff are aware of and understand the content of this policy. If any staff member is found to have breached this policy, they could be subject to the Disciplinary Policy.

1.7 The policy applies to all locations from which the Trust systems are accessed by staff 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 Trust. 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 should 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.

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

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

3.5 Security-related events should be reported to the IT team and to the DPO. 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. should 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.

3.7.2 Backups should be monitored to make sure they are successful.

3.7.3 A test restoration process will be run regularly.

3.7.4 In addition to cloud backups, local backup media are securely stored in a fireproof container.

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 personnel.

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 policies and procedures.

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.

4.1.7 Never installing unauthorised software on workstations.

4.1.8 Storing all confidential information on network servers.

4.1.9 Keeping food and drink away from workstations in order to avoid accidental spills.

4.1.10 Complying with the Anti-Virus policy.

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. 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. after a suspected breach, or after a change in staffing).

5.1.3 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 should be easily remembered. One way to do this is create a password based on a song title or other phrase, or to string together three random words e.g. coffeetrainfish.

5.2.5 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.

6. Access Control

6.1 Staff should 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 nondisclosure 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 Formal procedures will be used to control access to systems. An authorised manager must request each application for access and access privileges will be modified/removed - as appropriate - when an individual changes job or leaves. Staff with management responsibilities must ensure they advise IT of any changes requiring such modification/removal.

6.4 Staff should 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.

6.5 Line managers should ensure that all PC files of continuing interest to the business of the Trust are transferred to another user before a staff member leaves their employment. It is also good practice for a meeting to be held during which the manager notes all the systems to which the member of staff had access and informs the relevant system administrators of the leaving date. Particular attention needs to be taken when access to personal, commercially sensitive or financial data is involved.

6.6 Any contractors (working on site or working remotely via a communications link) to maintain or support computing equipment and software for the Trust must comply with the terms of this policy and any access control measures with which they are requested to comply with by Trust staff.

6.7 Physical security to all office areas should 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 at the end of each working day 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 should ensure that documents, particularly of a confidential nature are not left lying around.

7. Security of Portable Equipment and Mobile Devices

7.1 Staff 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. Staff are also responsible for the security of the hardware and the information it holds at all times on or off Trust property. The equipment should only be used by the individual to which it is issued, be maintained and batteries recharged regularly

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

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

7.5 Staff should ensure that any machine not routinely connected to the school network, is brought in regularly to receive updates by the IT team.

7.6 Staff must ensure that all school data is stored on the school network, and not kept solely on the laptop and should synchronise all locally stored data with the Trust 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 Trust owned, that may connect to or access the information systems at the Trust. 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 or equally strong measures 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 IT department and/or the DPO.

7.7.4 Non-departmental owned device that may connect to the Trust network must first be approved by the IT department.

8. Acceptable Use

8.1 While the [School/Trust'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 Trust.

8.2 Staff must pay particular attention to the protection of personal data and commercially sensitive data. All sensitive files must be password protected or encrypted where possible.

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

8.4 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.

8.5 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 Trust 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.

8.6 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.

8.7 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.

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

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

8.10 If it is suspected that there may be a virus on any Trust ICT equipment, staff should stop using the equipment and contact the IT team immediately. They will advise what actions to take and be responsible for advising others that need to know.

8.11 It is imperative that staff do not access, load, store, post or send from Trust ICT system any material that is, or may be considered to be: illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the Trust or may bring the Trust into disrepute. This includes, but is not limited to: jokes, chain letters, files, emails, clips or images that are not part of the Trust's business activities; sexual comments or images, nudity, racial slurs, gender 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 Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act).

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

8.13 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 1998.

9. Printing, Copying and Transmission of Data

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

9.2 Staff 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.

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

9.4 When sending data, the most secure method of transmission must be selected, especially where information is particularly sensitive or confidential. All staff should 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.

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

9.6 Sending information by email:

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

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

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

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

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

9.7 Sending information by post:

9.7.1 Check that the address is correct.

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

9.7.3 Consider using tracking, e.g. recorded delivery or a courier if appropriate.

10. Use of Email

10.1 The Trust gives all staff and governors their own email account to use for all Trust business as a work based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious emails and to avoid the risk of personal profile information being revealed.

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

10.3 Monitoring – Trust employees shall have no expectation of privacy in anything they store, send or receive on the Trust email system. The Trust may monitor messages without prior notice.

10.4 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.

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

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

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

10.8 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:

10.8.1 Encrypt and/or password protect attachments. Provide the encryption key or password by a separate contact with the recipient(s).

10.8.2 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.

10.8.3 Verify the details of a requestor before responding to email requests for information.

10.8.4 Consider using other secure file transfer methods, such as HertsFX or Schoolsfx (Hertfordshire schools).

10.8.5 Request confirmation of safe receipt.

10.9 The Trust email system shall not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, 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

Trust employee should report the matter immediately. The following activities are strictly prohibited, with no exceptions:

10.9.1 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).

10.9.2 Any form of harassment via email, telephone or messaging, whether through language, frequency, or size of messages.

10.9.3 Creating or forwarding "chain letters", "joke" emails, or "pyramid" schemes of any type.

10.10 Users should actively manage their email account by:

10.10.1 Checking emails regularly.

10.10.2 Deleting all emails of short-term value.

10.10.3 Organising email into folders and carrying out frequent house-keeping on all folders and archives.

10.10.4 Activating an out-of-office notification when away for extended periods.

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

10.12 The Trust email account should not be used for personal advertising.

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

11. Data Breaches

11.1 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.

11.2 Staff are responsible for:

11.2.1 Ensuring that no breaches of information security result from their actions.

11.2.2 Reporting any breach, or suspected breach of security without delay.

11.2.3 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.

11.2.4 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.

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

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

11.5 For staff any policy breach is grounds for disciplinary action in accordance with the Trust Disciplinary Procedure. Policy breaches may also lead to criminal or civil proceedings.

11.6 If a member of staff or governor knows or suspects that a Personal Data Breach has occurred, then the actions in the Data Breach Guidance must be followed. In particular, the DPO or such other person identified in the Data Breach Guidance must be notified immediately.

11.7 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.

12. Disposal of Redundant ICT Equipment Policy

12.1 All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data

12.2 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 Trust will only use authorised companies who will supply a written guarantee that this will happen.

12.3 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.

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

12.4.1 Date item disposed of.

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

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

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

12.5 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.

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 every 2 years or if any new technologies are introduced. Recommendations for any amendments should be reported to the DPO.

13.2 The Trust 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.