Avenue
CENTRE FOR EDUCATION

Information and Security Policy 2022 – 2025

Author:	Luton Borough Council
Date Updated:	May 2022
Approval Level:	Senior Leadership Team
SLT Review Date:	13th July 2022
Review Cycle:	Three Years
Next Review Date:	July 2025

Contents Page

1 Introduction

1.1 The Data Protection Act 2018 and the General Data Protection Regulation (GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

1.2 As a school we are dedicated to ensure the security of the information that it holds and will implement the highest standards of information security in order to achieve this. This document sets out the measures taken by the school to achieve this, including:

- to protect against potential breaches of confidentiality;
- to ensure that all information assets and IT facilities are protected against damage, loss or misuse;
- to support our Data Protection Policy in ensuring all school staff are aware of and comply with law and our own procedures applying to the processing of data; and
- to increase awareness and understanding at the school of the requirements of information security and the responsibility of staff to protect the confidentiality and integrity of the information that they themselves handle.

2 Purpose

2.1 The school will ensure the protection of all information assets within the custody of the school.

2.2 High standards of confidentiality, quality and availability of information will be maintained at all times.

2.3 Our school will demonstrate support for, and commitment to, information and cyber security through the issue and maintenance of this information and cyber security policy.

3 Scope

3.1 This policy applies to all members of staff, including temporary workers, other contractors, volunteers, interns, governors and any and all third parties authorised to use the IT systems. All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the School's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

3.2 This policy does not form part of any individual's terms and conditions of employment with the school and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

3.3 Information used by the school exists in many forms and this policy includes the protection of all information:

- stored electronically, on site or transmitted across networks
- any information assets in Cyberspace (The Cloud).
- hard copy data printed or written on paper
- communications sent by post / courier or using electronic means.
- stored tape or video including photos and CCTV images

- speech recordings

4 General Principals

4.1 All data stored on our IT systems and our paper records shall be available only to members of staff with legitimate need for access and shall be protected against unauthorised access and/or processing and against loss and/or corruption.

4.2 All IT systems are to be installed, maintained, serviced, repaired, and upgraded by IT.

4.3 The responsibility for the security and integrity of all IT Systems and the data stored thereon lies with the Head Teacher unless expressly stated otherwise.

4.4 All staff have an obligation to report actual and potential data protection compliance failures to Head Teacher/Business Manager who shall investigate the breach. Any breach which is either known or suspected to involve personal data or sensitive personal data shall be reported to the Data Protection Officer (full details of the DPO can be found in appendix A of this policy).

5 Physical security and procedures

5.1 Paper records and documents containing personal information, sensitive personal information, and confidential information shall be positioned in a way to avoid them being viewed by people passing by as much as possible, e.g. through windows. At the end of the working day, or when you leave your desk unoccupied, all paper documents shall be securely locked away to avoid unauthorised access.

5.2 Available locked filing cabinets and locked cupboards shall be used to store paper records when not in use.

5.3 Paper documents containing confidential personal information should not be left on office and classroom desks, on staffroom tables, left in pigeon holes or pinned to noticeboards where there is general access unless there is legal reason to do so and/or relevant consents have been obtained. You should take particular care if documents have to be taken out of school.

5.4 The physical security of buildings and storage systems shall be reviewed on a regular basis. If you find the security to be insufficient, you must inform the Head Teacher/Business Manager as soon as possible. Increased risks of vandalism and or burglary shall be taken into account when assessing the level of security required.

5.5 The school carries out regular checks of the buildings and storage systems to ensure they are maintained to a high standard.

5.6 The school has an intercom system to minimise the risk of unauthorised people from entering the school premises.

5.7 The school closes the school gates during certain hours to prevent unauthorised access to the building. An alarm system is set nightly.

5.8 CCTV cameras are in use at the school and monitored by office staff.

5.9 Visitors should be required to sign in at the reception, accompanied at all times by a member of staff and never be left alone in areas where they could have access to confidential information.

6 Computers and IT

6.1 The IT service, in conjunction with the Senior Leadership Team, shall be responsible for the following:

- Ensuring that all IT systems are assessed and deemed suitable for compliance with the school's security requirements;
- Ensuring that IT security standards within the school are effectively implemented and regularly reviewed, working in consultation with the school's management, and reporting the outcome of such reviews to the school's management;
- Ensuring that all members of staff are kept aware of this policy and of all related legislation..
  - Public facing systems i.e. school systems used by the public or available from the internet must be security tested prior to going live.
  - If these systems are upgraded they must again be hardened, patched and security tested before going live
  - All security tests will be arranged through the ICT Service
  - It is the responsibility of the school to ensure that when system delivery is undertaken by a third party on behalf of the school, equivalent security testing processes are agreed and applied
  - Effective and up-to-date anti-virus software will be run on all servers and PCs - we will check regularly to ensure that Anti-virus software on computers are current and fully functional.
  - Where a virus or malware is detected the event will be reported to the ICT Service at the earliest practical opportunity
  - Storage media that is obsolete or no longer required must be destroyed in a secure and environmentally friendly manner. This must include thorough removal of all data from the storage media to avoid the potential of data leakage.
  - Audit logs of key system events e.g. log on, log off and access to sensitive information will be recorded and reported upon - a minimum of 6 months of logs will be held
  - Ensuring that regular backups are taken of all data stored within the IT systems at regular intervals and that such backups are stored at a suitable location offsite.

6.2 Furthermore, the IT service, in conjunction with the Senior Leadership Team shall be responsible for the following:

- assisting all members of staff in understanding and complying with this policy;
- providing all members of staff with appropriate support and training in IT security matters and use of IT systems;
- ensuring that all members of staff are granted levels of access to IT systems that are appropriate for each member, taking into account their job role, responsibilities, and any special security requirements;

- receiving and handling all reports relating to IT security matters and taking appropriate action in response [including, in the event that any reports relate to personal data, informing the Data Protection Officer];
- taking proactive action, where possible, to establish and implement IT security procedures and raise awareness among members of staff;
- monitoring all IT security within the school and taking all necessary action to implement this policy and any changes made to this policy in the future; and

7 Responsibilities – Members of staff

7.1 All members of staff must comply with all relevant parts of this policy at all times when using the IT systems.

7.2 Computers and other electronic devices should be locked when not in use to minimise the accidental loss or disclosure.

7.3 You must immediately inform Head Teacher/Business Manager of any and all security concerns relating to the IT systems which could or has led to a data breach as set out in the Data Breach Policy.

7.4 Any other technical problems (including, but not limited to, hardware failures and software errors) which may occur on the IT systems shall be reported to a member of the Senior Leadership Team immediately.

7.5 You are not entitled to install any software of your own without the approval of the Head Teacher/Business Manager. Any software belonging to you must be approved by the Head Teacher/Business Manager and may only be installed where that installation poses no security risk to the IT systems and where the installation would not breach any licence agreements to which that software may be subject. Prior to installation of any software onto the IT systems, you must obtain written permission by the Head Teacher/Business Manager. This permission must clearly state which software you may install, and onto which computer(s) or device(s) it may be installed.

7.6 Physical media (e.g. USB memory sticks or disks of any kind) may not be used for transferring files. The Head Teacher/Business Manager approval must be obtained prior to transferring of files using cloud storage systems.

7.7 If you detect any virus this must be reported immediately to the Head Teacher/School Business Manager (this rule shall apply even where the anti-virus software automatically fixes the problem).

7.8 All ICT equipment (including portable computing devices) supplied to users is the property of our school and must be returned by the user either on the request of our school or when the user is no longer working on behalf of our school.

7.9 Access to ICT equipment must be provided on request from the ICT service, for the purposes of installation, maintenance, monitoring or decommissioning

7.10 Any IT equipment supplied to or and installed within our school must be purchased via the ICT service.

8 Access security

8.1 All members of staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy.

8.2 The school has a secure firewall and anti-virus software in place. These prevent individuals from unauthorised access and to protect the school's network. The school also teaches individuals about e-safety to ensure everyone is aware of how to protect the school's network and themselves.

8.3 All staff wishing to access the council network must firstly accept the user agreement. In doing so, the user agrees to abide by the terms and conditions stated as well as the policies of the council.

8.4 No one shall be granted access to an information system that does not require that access as part of their work for the council. Any access granted is following agreement with the IAO to ensure that access is limited to that required.

8.5 Access permissions to personal data held on IT systems are managed through role based permissions. Managers of appropriate seniority inform IT professionals of additions, amendments and discontinuation of individual accounts within permission groups.

8.6 Managers are periodically required to confirm that current permissions for which they are the authoriser and details of employees associated with these permissions are accurate.

8.7 All IT systems (in particular mobile devices) shall be protected with a secure password or passcode, or such other form of secure log-in system as approved by the IT service. Biometric log-in methods can only be used if approved by the IT service.

8.8 All passwords must, where the software, computer, or device allows:

- be at least 6 characters long including both numbers, letters and a special character (eg: $%£);
- be changed on a regular basis;
- not be obvious or easily guessed (e.g. birthdays or other memorable dates, memorable names, events, or places etc.)
- Example: where possible you should choose a password using the first letter of each word in a memorable sentence: 'I am a member of the chess club 2020' password is I@amotcc20

8.9 Passwords must be kept confidential and must not be made available to anyone else. Any member of staff who discloses his or her password to another employee will be liable to disciplinary action under the School's Disciplinary Policy and Procedure. Any member of staff who logs on to a computer using another member of staff's password will be liable to disciplinary action up to and including summary dismissal for gross misconduct.

8.10 If you forget your password you should notify the IT service to have your access to the IT systems restored. You must set up a new password immediately upon the restoration of access to the IT systems.

8.11 You should not write down passwords. Passwords should never be left on display for others to see.

8.12 Computers and other electronic devices with displays and user input devices (e.g. mouse, keyboard, touchscreen etc.) shall be protected with a screen lock that will activate after a period of inactivity. You may not change this this time period or disable the lock.

8.13 All mobile devices provided by the school, shall be set to lock, sleep, or similar, after a period of inactivity, requiring a password, passcode, or other form of log-in to unlock, wake or similar. You may not alter this time period.

8.14 Staff should be aware that if they fail to log off and leave their terminals unattended they may be held responsible for another user's activities on their terminal in breach of this policy, the school's Data Protection Policy and/or the requirement for confidentiality in respect of certain information.

9 Data security

9.1 Personal data sent over the school network will be encrypted or otherwise secured.

9.2 All members of staff are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from the Head Teacher/Business Manager who will consider bona fide requests for work purposes. Please note that this includes instant messaging programs, screen savers, photos, video clips, games, music files and opening any documents or communications from unknown origins. Where consent is given all files and data should always be virus checked before they are downloaded onto the school's systems.

9.3 You may connect your own devices (including, but not limited to, laptops, tablets, and smartphones) to the school's Wi-Fi provided that you follow the school's requirements and instructions governing this use. All usage of your own device(s) whilst connected to the school's network or any other part of the IT systems is subject to all relevant school policies (including, but not limited to, this policy). The Head Teacher/Business Manager may at any time request the immediate disconnection of any such devices without notice.

10 Electronic storage of data

10.1 All portable data, and in particular personal data, should be stored on encrypted drives using methods recommended by IT Service.

10.2 No data to be stored electronically on physical media.

10.3 You should not store any personal data on any mobile device, whether such device belongs to the school.

10.4 Data may only be stored on the school's computer network in order for it to be backed up.

10.5 All electronic data must be securely backed up by the end of the each working day and is done by Automated Processing through LGFL.

11 Home working

11.1 You should not take confidential or other information home without prior permission of the Head Teacher, and only do so where satisfied appropriate technical and practical measures are in place within your home to maintain the continued security and confidentiality of that information.

11.2 When you have been given permission to take confidential or other information home, you must ensure that:

- the information is kept in a secure and locked environment where it cannot be accessed by family members or visitors; and
- all confidential material that requires disposal is shredded or, in the case of electronic material, securely destroyed, as soon as any need for its retention has passed.

12 Communications, transfer, internet and email use

12.1 The school work to ensure the systems do protect pupils and staff and are reviewed and improved regularly.

12.2 If staff or pupils discover unsuitable sites or any material which would be unsuitable, this should be reported to the Head Teacher/Business Manager.

12.3 Regular checks are made to ensure that filtering methods are appropriate, effective and reasonable and that users access only appropriate material as far as possible. This is not always possible to guarantee and the school cannot accept liability for the material accessed or its consequence.

12.4 All personal information, and in particular sensitive personal information and confidential information should be encrypted before being sent by email (using egress), or sent by recorded delivery. You may not send such information by fax unless you can be sure that it will not be inappropriately intercepted at the recipient fax machine.

12.5 Postal and email addresses should be checked and verified before you send information to them. In particular you should take extra care with email addresses where auto-complete features may have inserted incorrect addresses.

12.6 You should be careful about maintaining confidentiality when speaking in public places. When working at home be aware of the possibility of others in the household overhearing video meetings.

12.7 You should make sure to mark confidential information ‘confidential’ and circulate this information only to those who need to know the information in the course of their work for the school.

12.8 Personal or confidential information should not be removed from the school without prior permission from the Head Teacher/Business Manager. When such permission is given you must take all reasonable steps to ensure that the integrity of the information and the confidentiality are maintained. You must ensure that the information is:

- not transported in see-through or other un-secured bags or cases;
- not read in public places (e.g. waiting rooms, cafes, trains, etc.); and
- not left unattended or in any place where it is at risk (e.g. in car boots, cafes, etc.)
- where possible hard copy data should not be removed and instead transported using an encrypted and password protected mobile device or laptop

13 Reporting security breaches

13.1 All concerns, questions, suspected breaches, or known breaches shall be referred immediately to the Head Teacher/Business Manager. All members of staff have an obligation to report actual or potential data protection compliance failures.

13.2 When receiving a question or notification of a breach, the Head Teacher/Business Manager shall immediately assess the issue, including but not limited to, the level of risk associated with the issue, and shall take all steps necessary to respond to the issue.

13.3 Members of staff shall under no circumstances attempt to resolve an IT security breach on their own without first consulting the Head Teacher/Business Manager. Any attempt to resolve an IT security breach by a member of staff must be under the instruction of, and with the express permission of, the Head Teacher/Business Manager.

13.4 Missing or stolen paper records or mobile devices, computers or physical media containing personal or confidential information should be reported immediately to the Head Teacher/Business Manager.

13.5 All IT security breaches shall be fully documented.

13.6 Full details on how to notify of data breaches are set out in the Data Breach Policy

13.7 The Head Teacher/Business Manager will be responsible for completing a data breach report for all security and data breaches and sending that to the data protection officer for assessment and further advice.

14 Risk management

14.1 The school recognises that there are risks associated with users accessing and handling information in order to conduct official school business.

14.2 The school is committed to maintaining and improving information security and minimising its exposure to risks. It is the policy of the school to use all reasonable, practical and cost effective measures to ensure that risk are minimised, as follows:

- An asset owner will be assigned to all information assets
- All ICT projects and new IT systems will have a completed a privacy impact assessment (PIA) before the project/IT system is approved
- The PIA will be approved by the Data Protection Officer. If risks cannot be mitigated then the PIA will be forwarded to the Information Commissioner's Office for final approval. This process can take up to three months.
- All ICT project risks will be assigned a risk owner responsible for producing a risk treatment plan to address the risk
- The Management Committee will regularly agree what is an acceptable benchmark for risks to ICT assets (minimum annually)
- Where an information asset is observed to exceed this benchmark a risk treatment plan must be developed by the information asset owner, liaising with our data protection officer as required
- All risks, in excess of the benchmark will be recorded in our school risk log
- Governors or a delegate nominated by governors will act as arbiter in disputes over how identified information security risks should be remedied

- Information will be protected against unauthorised access and disclosure
- The confidentiality of information will be assured
- The integrity and quality of information will be maintained
- Authorised staff, when required, will have access to relevant school systems and information. However, the minimum level of access will be granted at all times.
- Business continuity and disaster recovery plans for all critical activities will be produced, tested and maintained
- Access to information and information processing facilities by third parties will be strictly controlled with detailed responsibilities written into contract/documented agreements
- All breaches of information and cyber security, actual and suspected, will be reported and investigated. Corrective action will be taken.
- Data protection training will be available to all staff

14.3 Non-compliance with this policy could have a significant effect on the efficient operation of the school and may result in financial loss and loss of reputation

14.4 The framework and policies recognise that where information or systems used for provision of school services is hosted by a 3rd party, the need for continued compliance is retained and that controls agreed with the 3rd party will be at least equivalent to those operated by us..

15 Related documents

- Computer Misuse Act (1998)
- Data Protection Act (2018) & the GDPR
- The Human Rights Act (1998)
- Regulation of Investigatory Powers Act (2000) aka RIPA
- The Electronic Communications Act (2000)

16 Appendix A - Roles and Responsibilities

17 Role of the Senior Information Risk Owner (SIRO)

17.1 The SIRO is a senior member of staff within the school who is familiar with information risks and the school's response. The SIRO at Avenue Centre for Education school is the Business Manager, contact information businessmanager@avenuecentre.co.uk

17.2 The SIRO has the following responsibilities:

- own and maintain the Information and Cyber Security Policy
- establish standards, procedures and provide advice on their implementation
- act as an advocate for information risk management
- appoint the Information Asset Owners (IAOs)
- Monitor the school's compliance with the Data Protection Act 2018 and other data protection legislation and internal policies
- Monitor performance
- Identify safeguards to apply to mitigate any risks identified
- Maintain a record of processing activities
- Maintain records and evidence of the school's compliance with the Data Protection Act

17.3 Additionally, the SIRO will be responsible for ensuring that:

17.4 Staff receive appropriate training and guidance to promote the proper use of information and ICT systems. Staff will also be given adequate information on the policies, procedures and facilities to help safeguard the school's information. A record of the training provided to each individual member of staff will be maintained.

17.5 Staff are made aware of the value and importance of school information particularly information of a confidential or sensitive nature, and their personal responsibilities for information security.

17.6 The associated guidance relating to information security and the use of particular facilities and techniques to protect systems and information will be disseminated to staff.

17.7 The practical aspects of ICT protection are performed, such as maintaining the integrity of the data, producing the requisite back-up copies of data and protecting the physical access to systems and data.

17.8 There are appropriate controls over access to ICT equipment and systems and their use including defining and recording the requisite level of protection.

17.9 They are the official point of contact for ICT or information security issues and as such have responsibility for notifying the Senior Leadership Team, Data Protection Officer and Chair of Governors of any suspected or actual breach occurring within the school.

18 Role of the Data Protection Officer (DPO)

18.1 Article 37 of the General Data Protection Regulation (GDPR) mandates that schools and academies have a Data Protection Officer (DPO) in place.

18.2 The role of the DPO within school is to:

- Advise the school, their data processors and their employees of their responsibilities
- Advise on data protection impact assessments (PIA)
- The DPO will also be the contact point for the Information Commissioner's Office (ICO).

18.3 The schools Data Protection Officer is: Kat Barker, Email: dataprotection@luton.gov.uk

19 Role of the Information Asset Owner (IAO)

19.1 Once the school has identified its information assets, including personal information and data relating to pupils and staff, for example, assessment records, medical information and special educational needs data, schools should identify an Information Asset Owner (IAO) for each asset or group of assets as appropriate.

19.2 The role of an IAO is to understand:

- what information is held and for what purposes
- how information will be amended or added to over time
- who has access to the data and why
- how information is retained and disposed of.

19.3 Typically, there may be several IAOs within a school, for example, ICT Manager, HR Officer.

19.4 The IAO is responsible for managing and addressing risks to the information and ensuring that information handling both complies with legal requirements and is used to fully support the delivery of education.

19.5 Important information assets will include, but are not limited to, the following:

- Filing cabinets and stores containing paper records e.g. archives
- Computer databases
- Data files and folders

19.6 On the introduction of this policy Information Asset Owners may need to conduct a thorough information risk assessment to identify any necessary operational or technological changes that may be required within the school