Data Management & ICT Security Policy & Procedures 2023

The Link Academy Trust is a company limited by guarantee and an exempt charity, regulated by the Education & Skills Funding Agency (ESFA). All Members of the Board of Trustees of the exempt charity are also Directors of the company; the term 'Trustee' used in this Policy also means Director. This Policy applies to all academies within the Link Academy Trust

Context

Safety of the pupils and staff within the schools of the Link Academy Trust (the 'Trust') is our top priority and we work hard to reduce any risk of compromise of that safety. Safeguarding and protection of children is driven by the measures the schools put in place throughout the whole school ethos. This extends beyond the curriculum and extra-curricular activities to encompass data protection. This policy sets out the measures the Trust takes to protect the data of children, parents and staff along with procedures that Trust staff are obliged to follow. This policy is one in a suite of many that relate to data protection.

Glossary

General Data Protection Regulations (GDPR) - Regulations that come into force on 25 May 2018 which the Trust is obliged to comply with.

Data Protection Act / Bill - The Data Protection Act 1998 shall be replaced in 2018. It sets out the principles that organisations are expected to comply with to protect the data of individuals.

SIMS.net - The school management information system managed by Capita.

Personal Data - Any information relating to an identifiable person who can be directly or indirectly identified.

Sensitive Personal Data - Data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning sexual orientation.

Electronic Data Management – Management Information System

Pupil and staff data is uploaded to the school's management information systems. The system currently used at school are SIMS.net, Selima and Power Bi. They hold the data of every pupil from Nursery to Year 6 as well as every member of staff. SIMS.net management information system is hosted by an external provider, Capita, who have provided the school with confirmation of their compliance with the General Data Protection Regulations (GDPR).

Access rights are set according to requirements within the Trust, so that staff members can only access data that is relevant to their needs. Every user has a unique username and password that is not shared with any other person.

- Every class teacher and support staff member can access basic pupil details, along with attendance data. This allows them to take the register for each pupil, assess their attendance levels and performance, and have access to emergency contact details should they be required.

- The school's Special Educational Needs Co-ordinators (SENDCO's) have access to general pupil data together with the special educational needs data, performance data, attendance data and emergency contact details. This is to ensure that the SENDCO's has sufficient data to support the child with special educational needs.
- The HR Officer and the school's Designated Safeguarding Leads (DSL's) have access to general pupil data together with the welfare data of the pupil which includes information on children in care, child protection plans in place, disability information. This ensures that the DSL's have access to all relevant data and can ensure data shared by other agencies, in compliance with GDPR, is current. Does this require clarification?
- The admin support team has access to general pupil data, emergency contact details and attendance data. The admin team is required to update registers for children absent or late and will be required to contact parents on a regular basis for general school matters or in the event of an emergency.
- The Executive/Academy Heads have access to all data of the pupils so that they may discharge their duties relating to pupil attendance and general communication with parents. The Executive/Academy Heads also have access to staff data to facilitate fulfilling their responsibilities in ensuring staff have the correct contracts of employment and paid accordingly.
- The Executive/Academy Heads have access to all pupil data and all staff data.

Electronic Data Management

We acknowledge the continued growth in the use of electronic communication and data storage. The Trust has a shared network that staff can access to save documents. The Trust has a secure ICT infrastructure in place and only staff members employed to work within the Trust can access the network.

Where any document is created or edited by a staff member, and that document contains personal data, the staff member shall save the document in the shared network area only. In the event that the document contains ***sensitive personal data*** the document shall be saved with password protection as an added security measure. Only staff members who have a legitimate reason to access the document in line with their statutory obligation to the education of pupils shall be granted access.

The Executive/Academy Heads, SENDCO's and DSL's frequently communicate with parents and other agencies about sensitive and confidential matters. Where documents created contain sensitive personal data those individuals shall save the document to the hard drive of their work PC in the area set up by the ICT support company.

Paper Files

In accordance with GDPR requirements the Trust is committed to data minimization and shall comply with Principle 3 of GDPR which states that:

> '*personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed*.'

As an education provider the Trust has a duty to retain specific paper documents such as proof of identity of a pupil. This data is held in the pupil files which are stored in locked cupboards in the administrator's office. These files may be accessed by staff members only.

The Trust's Records Retention and Disposal Policy outlines how long data shall be kept in the schools. This schedule was based on the Schools' Toolkit produced by the Records Management Society and shall be updated as new guidance is issued by the Information Commissioner's Officer (ICO), the Department for Education (DfE) or the Local Authority (LA).

Staff members who retain hard copies of personal data about pupils in their class ensure that such papers are filed in appropriate folders and stored in locked cupboards within their classroom.

Clean Desk Policy

To help the Trust comply with the privacy principles of data protection staff are required to operate a clean desk policy. This policy requires that all members of staff clear their desks of documents, notes and removable media at the end of each working day. No paper, removable media or post-it notes will be left on desks when staff members leave.

Clear Screen Policy

All members of staff are required to lock their PCs when leaving their office/classroom. This will ensure that access to files and personal data is restricted. Staff shall be mindful at all times as to what is visible on their PC during the working day. Should an individual member of staff have a meeting with a parent or an external agent the staff member shall lock their screen where possible. If that staff member is not able to lock their screen because they require access to the PC they shall close any documents that they have been working on. They must also close their email programme.

ICT Security

The Trust has a robust back-up mechanism in place so that all personal data is backed up on a daily basis. Staff members will not save personal data to any removable media. USB sticks will not be made available or used by staff.

In the event that a member of staff downloads personal data onto his or her own personal USB stick and that personal data is lost or mislaid the staff member must report its loss **immediately** to the Trust's Data Protection Officer. Where staff members are found to be using USB sticks for downloading personal data the Executive/Academy Heads shall conduct an enquiry in line with the school's disciplinary procedures.

Working Remotely

From time to time Trust staff members may wish to work from home outside of school hours (eg in the evenings, weekends or during holidays). All staff have access to Office 365 and therefore, to minimise the risk of compromise to personal data, the following stringent security measures are to be applied:

- Electronic documents containing personal data should only be accessed remotely in an environment in which another individual will not see the document on screen;
- Where a staff member is working on a document containing personal data that staff member must use the lock screen facility (clear screen procedures below) each time they leave the PC, irrespective of how long they may be away from the document;
- Where staff members are accessing the SIMS.Net they should close the application down when not directly using it;
- Any documents accessed and edited on an individual's PC must not be stored or saved on that PC or laptop. Documents should be saved to the Office 365 OneDrive or Google Drive facility;
- All staff must ensure they **log out** when they are finished.

Accessing emails remotely and/or on mobile devices

All members of staff are able to access emails remotely using Google Gmail or Office 365 Outlook. These are secure websites and all staff have distinct email credentials to access their emails. Staff members using this facility must ensure they **log out** when they have finished.

As technology has advanced many individuals like to access emails *on the go*. If a staff member has set up their email account on their mobile phones they must ensure that:-

- Their phones are secured through a log-in passcode or one-touch authentication;
- Where the staff member allows other individuals to use their mobile phone they must ensure they have additional security measures in place so that emails cannot be accessed;

This policy shall be updated as new guidance is issued to provide clarity around compliance with GDPR and the Data Protection Bill 2018.

Procedures for Staff

Every member of staff is required to follow procedures outlined below in order to minimise the risk of compromise to the data of any individual that the Trust may hold. Every member of staff has access to the shared network, SIMS.net, Selima and an email programme. Access is only available at the time that they are employed and, when they cease employment, all access is revoked immediately.

Printing of personal data

To comply with the data minimization principles of GDPR staff members must not print documents or reports that contain personal data and/or sensitive personal data unless such printing is necessary in discharging their duties. Where it is deemed necessary to print documents that contain personal data that staff member shall ensure that the document is kept in legible lever arch files within a locked cupboard or other locked storage device. Staff shall only retain personal data for the purpose identified and the timeframe for which it is required.

Disposal of personal data documents

Where a document containing personal data has been printed and the staff member has identified that it is no longer required for its original stated purpose that staff member is responsible for ensuring that it is destroyed securely. Any documents containing personal data may only be destroyed through shredding or document disposal sacks. Staff will use the school shredders and document disposal sacks in the main admin offices. Staff must ensure that no documents containing personal data are re- used or put into the recycle bin.

Use of removable media

Staff members may not use personal USB sticks in school computers whether or not these are encrypted so that the risk of spreading a virus is minimised.

Any staff member who is found to be using personal USB sticks in school property may be subject to a disciplinary investigation.

Saving electronic documents containing personal data

Class teachers, classroom based support staff and admin team staff who have created or edited a document containing personal data or sensitive personal data must save the document(s) in the school shared network only. Documents containing personal data must not be saved on individual classroom PCs. The rationale for this is to minimise unauthorised access to documents saved locally within the classroom and admin office. Where personal data contains sensitive information the staff member saving the file should use password protection.

The Executive/Academy Heads, DSL's and SENDCO's regularly create or edit documents containing sensitive personal data. They shall be allowed to save such documents to the hard drive of their work PC but shall be required to password protect documents/folders to minimise unauthorised access.

Taking paper documents off-site

We acknowledge that there will be occasions when members of staff will need to take documents off-site. If documents, laptops, or paperwork have been lost or stolen it needs to be reported to the DPO as soon as the breach occurs and reported to the ICO by the DPO within 72 hours. This may be because the staff member is attending a meeting at a different venue or because they wish to work on the document outside of school hours. However staff shall continue to comply with the data protection requirements.

- If the document(s) does not contain personal data, sensitive or otherwise, the data protection principles do not apply. However, staff should minimise the quantity of document(s) that they remove from the school site to ensure that the school is able to access the document(s), if required.
- If the document(s) contains personal data the staff member shall ensure that he or she takes appropriate measures to minimise the risk of damage to the subject through loss, damage or access. The member of staff shall ensure that all documents taken from the school site are kept secure at all times by:-
    - Ensuring that documents are not left in an unattended vehicle at any time;
    - Ensuring that documents are only worked on in a location that accommodates the need for privacy;
    - Ensuring that the documents are in a secure, inaccessible location overnight.

If school staff remove personal data from school and that data is accessed by another individual leading to damage, or potential damage, to the subject data the Executive/Academy Heads shall conduct a full investigation in line with the school's disciplinary procedures.

Prior to removing sensitive personal data from school the member of staff must inform their Executive/Academy Head or, in the absence of their Executive/Academy Head, the Data Protection Officer.

Clean Desk Procedures

Staff members shall ensure that their workplace desk contains no personal data or sensitive personal data when they leave school at the end of the working day. Any papers that contain personal data, whether sensitive or not, shall be placed in a secure area within the classroom or office.

Clear Screen Procedures

When school PCs are not in use or where the staff member is leaving the workstation, irrespective of the length of time he or she may be absent from the room, the computer must be locked by using the CTRL+ALT +DEL function. Access to the computer will require the staff member's password.

Staff are responsible for ensuring that personal data is not compromised and shall follow this policy and procedures document to ensure that any risks are minimised.

This policy shall be read in conjunction with other data protection policies in school, specifically the Data Protection Policy.

Approved by the Audit Committee: 18 January 2023
Next Review: Spring 2025