GLEBE PRIMARY SCHOOL
UNITED LEARNING ACADEMY

Data Protection Policy
Roles and Responsibilities
2024-2025

Updated: Autumn 2024
New Review: Summer 2025

Approved by the Local Governing Board on 08.10.24

Signed by: Mr. James Dempster
Position: Chair of the Local Governing Body

Group Data Protection Policy - Roles & Responsibilities

1.1 **Document Control**	
Document Title:	Group Data Protection Policy - Roles & Responsibilities (Risk Architecture)
Version:	1
Summary of Changes from Previous Version:	New
Name of Originator/Author (including job title):	Alison Hussain, Company Secretary and Data Protection Officer
Target Audience:	All staff
Review By Date:	N/A
Date Issued:	March 2020

Contents

This section details the roles and responsibilities of the Board, the Local Governing Bodies and each individual employee. The "Local Organisation of Data Protection" must be completed by the relevant school or central office and populated with the names and roles of those with the specific duties contained within.

2. Trustees

2.1 The Trustees of United Church Schools Trust and United Learning Trust as the employers are responsible for ensuring compliance Data Protection laws.

2.2 The Trustees will appoint a Data Protection Officer.

2.3 The Trustees will hold the Chief Executive Officer, Executive Directors and the Data Protection Officer to account for their performance in relation to the duties set out in this document and the Group Data Protection policies.

3. Link Trustee

The Link Trustee will:

3.1 retain a high level of oversight of Information Governance matters on behalf of the Trustees;

3.2 engage with the Data Protection Officer to understand the health of data governance

4. Chief Financial Officer (SIRO)

The Chief Financial Officer (CFO) is the Senior Information Risk Owner and as such is the executive responsible for the management of information governance risks. The CFO will support the Board to ensure compliance with Data Protection law by:

4.1 ensuring the Group has a plan for continuous improvement in respect of information governance;

4.2 taking visible steps to support that plan (including completing own training);

4.3 acting as the focal point for information risk management in the organisation including resolution of any escalated risk issues raised by the Data Protection Officer or Auditors;

4.4 reviewing all key information risks to the Group and ensure that mitigation plans are robust;

5. Executive Directors

The Executive Team are responsible for:

5.1 Ensuing the Data Protection Officer has sufficient resource to carry out the duties defined in the General Data Protection Regulation (GDPR);

5.2 Ensuring that Regional Directors and Head Teachers promote and foster a culture of compliance with data protection policies in their schools;

5.3 Review and approve Data Protection policy.

6. Group Data Protection Officer

The Data Protection Officer is responsible for developing and implementing the Group's Information Governance Strategy with responsibility and accountability for the development, implementation and delivery of the Group's Information Governance work programme, incorporating Data Protection and Confidentiality, Records Management and, where appropriate, Information Security.

The Data Protection Officer will:

6.1 Deliver the key elements of Information Governance within the Group, working with senior managers, staff and schools to ensure that Information Governance strategies, policies and procedures are developed in line with legislation and best practice and that those standards are understood and adhered to;

6.2 Ensure robust arrangements are in place to ensure the safety and security of personal information.

6.3 Chair the Information Governance Steering Committee;

6.4 Be the nominated officer in the Data Protection register maintained by the Information Commissioner and maintain the accuracy and currency of the Group's notifications;

6.5 Act as subject matter expert for information governance, assisting in the investigation of incidents and breaches of Data Protection;

6.6 To act as lead for serious incidents involving information governance breaches;

6.7 Audit and assess systems and processes currently utilised within the Group with relevance to Information security and confidentiality;

6.8 Be responsible for developing the plan for continuous improvement and overseeing the implementation of this;

6.9 Develop and roll out training programmes to managers and staff to support information governance, ensuring all employees are aware of and appreciate the importance of information governance;

6.10 Advise on Data Protection Impact Assessments and address privacy issues;

6.11 Advise on Freedom of Information and Subject Access requests guiding colleagues to the correct course of action;

6.12 Report on defined information governance KPIs to the Executive Team and the Board of Trustees.

7. Head Teachers

Head Teachers are responsible for fostering a culture of compliance with policy and best practice in implementing information governance by:

7.1 Appointing a Data Protection Lead (DPL) of sufficient seniority;

7.2 Provide the DPL with adequate support and resource to fulfil their role;

7.3 Ensuring all school staff complete mandatory training;

7.4 If the Head Teacher does not appoint a DPL the Head Teacher is the school's DPL by default.

8. Data Protection Leads

Each school is required to appoint a Data Protection Lead (DPL). It is advised that schools also appoint a Deputy Data Protection Lead. It is DPL's duty to:

8.1 Ensure all staff have watched the latest data protection training video;

8.2 Ensure all staff have watched the latest cyber awareness / information security video;

8.3 Ensure these videos are part of the induction process for new staff;

8.4 Ensure staff are aware of all Data Protection policies relevant to their role;

8.5 Ensure that the school has regular sessions / email reminders to raise awareness with regard to the following policies:

- Responding to SARS
- Data sharing
- Third party requests for personal data
- Managing data breaches
- Secure transfer of personal data

8.6 Ensure an initial school level personal data audit has been carried out and review every two years;

8.7 Ensure the record of data processing activities has been completed on the EIP and is updated as required

8.8 Provide the record of data processing activities to LGB for annual review;

8.9 Ensure the school has appropriate privacy notices in place for pupils, parents, employees, volunteers, governors and contractors (use the templates available on the Hub);

8.10 Ensure pupil and parent privacy notice is in a prominent place on the school website;

8.11 Put in place a process for ensuring new pupils/parents are aware of the privacy notice;

8.12 Update the privacy notices as required and make relevant data subjects aware of this;

8.13 Provide pupil and parent privacy notice to LGB for annual review;

8.14 Keep a list of all the data collection forms that the school uses (i.e. enquiries, admissions, school trips, health data etc) This includes both paper forms and website forms. Ensure all data collection forms have appropriate transparency information on them and link to the full privacy notice;

8.15 If the school website contains forms that collect personal data ensure appropriate processes are in place to keep these data secure in transit and at rest;

8.16 Maintain a record of which data processing activities the school collects consent for and ensure that forms used meet the GDPR requirements set out in the consent policy;

8.17 Ensure that records are kept of who has consented and who has not and that relevant staff know how to access this;

8.18 Ensure there is a process in place to review consents periodically to consider if they are still appropriate;

8.19 Use the personal data audit to identify all instances of data sharing with a data processor;

8.20 Check that there is a compliant data processing contract in place for each instance of data sharing with a processor;

8.21 Check that the data processor is GDPR compliant in terms of technical and organisational measures to keep data secure (use cyber security questionnaire);

8.22 When engaging a new data processor ensure that the DPIA policy is followed;

8.23 Before sharing data with another data controller ensure the Data Sharing and DPIA policies are followed and, if required, ensure a data sharing agreement is in place and signed;

8.24 Put processes in place to ensure compliance with the record retention schedule and monitor compliance with this;

8.25 Ensure that the school's Network Manager (or contractors if this is outsourced) can demonstrate compliance with the Technical Assurance advice document and Technology Handbook;

8.26 Ensure that Network managers are encrypting all laptops and any other portable devices owned by the school are encrypted;

8.27 Make sure that paper copies of personal data are held securely in school and that and personal data put on display is the minimum amount necessary to achieve the purpose for which it is displayed;

8.28 Ensure staff understand the acceptable use form and ensure it is signed by all staff and held on their HR file;

8.29 Ensure staff understand the BYOD policy and require all staff using their own devices to register their devices and sign the policy;

8.30 Have a plan in place for ensuring all data is returned to school when a member of staff who uses their own device leaves employment;

8.31 Keep records of the actions taken in respect of the above.

8.32 Keep your school's SLT and LGB informed. Ensure data protection is a regular agenda item and report to SLT in respect of your progress in relation to the above;

8.33 The DPL will receive the following training:

- Data Protection Lead training provided by the Group Data Protection Officer (DPO).
- Refresher training at the annual Data Protection Lead conference.

8.34 The DPL may request additional training and support from the DPO as needed.

9. Local Governing Bodies

9.1 Ensure the school has a Data Protection Lead;

9.2 Review the school's Privacy Notice and record of data processing activities on an annual basis;

9.3 Review the school's progress against KPIs in relation to staff training, data breaches, requests for information, data protection impact assessments and, where relevant, outstanding data protection audit actions.