The Lowry Academy
The best in everyone™
Part of United Learning

General Data Protection Regulation (GDPR) Policy 2024 - 2026

Aspiration | Resilience | Respect | Confidence | Creativity

Data GDPR – General Data Policy			
Approved / Accepted by	Adopted from United Learning template Policy The Local Governing Board		
Author	United Learning		
Policy Originator	United Learning Data Protection Lead Reviewed by: DPO – The Lowry Academy		
Originated/ Adopted	**Accepted by**	**Review Period**	
March 2024		2 Year	
Date to LGB	**Reason**	**Outcome**	**Next review date**
27.03.2024	Adopted Policy	Ratified	March 2026

United Learning Group Data Protection Policy

Scope

The policy set out in this document applies to all United Church Schools Trust (UCST) and United Learning Trust (ULT) schools and offices. The two companies (UCST and ULT) and its subsidiaries are referred to in this policy by their trading name, 'United Learning'.

Where this policy refers to 'School' or 'Head Teacher', within Central Office this should be interpreted to refer to the department where a member of staff works and their Head of Department.

As a values-led organisation our values of ambition, confidence, creativity, respect, enthusiasm and determination are key to our purpose and underpin all that we do.

Definitions

"Personal data" means any information relating to an identified or identifiable natural person ("data subject")

An **"identifiable person"** is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person

"Processing" means any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Policy Statement

United Learning values the personal information entrusted to us and will process personal data in accordance with the principles set out in the General Data Protection Regulation (UK GDPR). United Learning has put in place policies, procedures and guidance to ensure that we will always:

- determine the legal basis for the processing of personal data and document;
- be open with individuals about how we use their information and who we give it to;
- only process personal data in a manner consistent with the purpose for which it was collected;
- consider and address the privacy risks when we are planning to use or hold personal information in new ways, such as when introducing new systems;
- have processes in place to ensure the accuracy of personal data held;
- keep personal information to the minimum necessary and delete it when we no longer need it;
- have processes in place to enable individuals to exercise their rights as set out in the UK GDPR,
- have appropriate technical and organisational measures in place to make sure personal information is kept securely and only accessed on a need to know basis;

- provide training to staff who handle personal information and treat it as a disciplinary matter if they deliberately or recklessly misuse or don't look after personal information properly;
- put appropriate financial and human resources into looking after personal information.

Accountability

To enable United Learning to demonstrate compliance with the UK GDPR schools will implement the following Data Protection policies and procedures, and maintain appropriate records as required by these procedures:

1. Data protection roles and responsibilities
2. Privacy notice policy and appendices
3. Employee data protection policy
4. Policy for obtaining and recording consent and handling requests to withdraw consent
5. Rights of the data subject policy and guidance
6. Policy for responding to a subject access request
7. Policy for responding to a request for personal data from a third party
8. Policy on the application of exemptions to the UK GDPR
9. Procedure for disclosing information safely
10. Records Management Policy
11. Records Retention Schedule
12. Procedure for keeping records of data processing activities
13. Data minimisation policy
14. Information Security Policy
15. Security of personal data policy
16. Clear desk policy
17. Password Policy
18. Technology Handbook
19. Procedure for notification of a personal data security breach
20. Data sharing policy and procedure
21. Data Protection Impact Assessment policy, procedure and guidance

United Learning has a Data Protection Officer who is responsible for:

(a) providing information and advice to employees who carry out data processing regarding their obligations pursuant to UK GDPR and other relevant Data Protection Legislation and advising employees on the implementation of Group policies;

(b) monitoring the Group's compliance with

- the above policies and procedures,
- the assignment of responsibilities for the processing of personal data;

(c) ensuring there is a programme of awareness-raising and training of staff involved in data processing operations;

(d) to provide advice where requested as regards the data protection impact assessment and monitor the Group's performance pursuant to Article 35 UK GDPR;

(e) to cooperate with the Information Commissioner's Office;

(f) to act as the contact point for the Information Commissioner's Office on issues relating to processing, including the prior consultation referred to in Article 36 UK GDPR, and to consult, where appropriate, with regard to any other matter.

The Head Teacher must appoint an individual of sufficient seniority who will be the school's Data Protection Lead (DPL). The DPL will be responsible for:
(1) Implementing the above data protection policies and procedures at the school and ensuring that they are adhered to;
(2) Ensuring that all staff complete data protection training appropriate to their role including refresher training;
(3) The school keeps records to demonstrate compliance;
(4) Participating in data protection compliance audits conducted by central office;
(5) Responding to any requests by a data subject to exercise their rights under the UK GDPR.

In the event that the school does not have a DPL it is the Head Teacher's responsibility to ensure compliance.

Version number:	3.		Target Audience:	All staff
UCST/ULT/Both:	Both		Reason for version change:	No changes
Date Authorised:	September 2018		Name of owner/author:	Alison Hussain
Authorised by:	FIC		Name of individual/department responsible:	Alison Hussain, Company Secretary and Data Protection Officer
Date reviewed:	April 2023			
Reviewed by:	DPO			
Date of next review:	April 2025			

The Lowry Academy specific:

Statutory
The Lowry Academy collects and uses personal information about staff, students, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

Schools have a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website. Schools also have a duty to issue a Privacy Notice to all students/parents, this summarises the information held on students, why it is held and the other parties to whom it may be passed on.

Aims
Our school aims to ensure that all personal data collected about staff, students, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

Legislation and guidance
This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the Education (Student Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

The data controller
Our school processes personal data relating to parents, students, staff, governors, visitors and others, and therefore is a data controller.

Roles and responsibilities
This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. **Staff who do not comply with this policy may face disciplinary action**.

Governing Board
The Governing Board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

Data Protection Officer
The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

The DPO is the first point of contact for individuals whose data the school processes, and for the ICO.

Our **DPO is Mrs Rosie Aylward – Vice Principal** who is contactable by e-mailing: ask.lowry@lowryacademy.org.uk or via telephone on **0161 529 5200.**

Principal
The principal acts as the representative of the data controller on a day-to-day basis.

All staff
Staff are responsible for:
- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  - If they have any concerns that this policy is not being followed
  - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
  - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
  - If there has been a data breach
  - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
  - If they need help with any contracts or sharing personal data with third parties

6. Data protection principles
The GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:
- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure
- This policy sets out how the school aims to comply with these principles.

Collecting personal data

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:
- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract

- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a student) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to students, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the student is under 13 (except for online counselling and preventive services).
Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

Limitation, minimisation and accuracy
We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.
If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.
Staff must only process personal data where it is necessary in order to do their jobs.
When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the **Information and Records Management Society's Toolkit for Schools.**

Sharing personal data
We will not normally share personal data with anyone else, but may do so where:
There is an issue with a student or parent/carer that puts the safety of our staff at risk
We need to liaise with other agencies – we will seek consent as necessary before doing this
Our suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies. When doing this, we will:
- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:
- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

- We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our students or staff.
- Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Subject access requests and other rights of individuals
Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:
- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter or email to the DPO. They should include:
- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO.

Children and subject access requests
Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students at our school may not be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

Responding to subject access requests
When responding to requests, we:
- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the student or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.
A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.
When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

Other data protection rights of the individual
In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)
- Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

Parental requests to see the educational record
Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a student) within 15 school days of receipt of a written request.

Biometric recognition systems
Where we use students' biometric data as part of an automated biometric recognition system (for example, students use finger prints to receive school dinners instead of paying with cash), we will comply with the requirements of the **Protection of Freedoms Act 2012**.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and students have the right to choose not to use the school's biometric system(s) if school choose to install this. School will provide alternative means of accessing the relevant

services for those students. For example, students can pay for school dinners in cash at each transaction if they wish.

Parents/carers and students can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a student refuses to participate in, or continue to participate in, the processing of their

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

CCTV
We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to School DPO.

Photographs and videos
As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers for photographs and videos to be taken of students for communication, marketing and promotional materials.
Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where we don't need parental consent, we will clearly explain to the student how the photograph and/or video will be used.

See our Child Protection and Safeguarding Policy for more information on our use of photographs and videos.

Data protection by design and default
We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices

- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant

Maintaining records of our processing activities, including:
- For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
- For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

Data security and storage of records
We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

Disposal of records
Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Personal data breaches
The school will make all reasonable endeavours to ensure that there are no personal data breaches.
In the unlikely event of a suspected data breach, we will follow the procedure set out in app1.

When appropriate, we will report the data breach to the **ICO within 72 hours**. Such breaches in a school context may include, but are not limited to:
- A non-anonymised dataset being published on the school website which shows the exam results of students eligible for the student premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about students

Training
All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

Monitoring arrangements
The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed **every 2 years** and shared with the full governing board.

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people

- The DPO will alert the headteacher and the chair of The Governing Board
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school's computer system.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website **within 72 hours**. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:

- The categories and approximate number of individuals concerned
- The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on the schools computer system

- The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- *If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error*

- *Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error*
- *If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it*
- *In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way*
- *The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request*
- *The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted*
- *Details of student premium interventions for named children being published on the school website*
- *Non-anonymised student exam results or staff pay information being shared with governors*
- *A school laptop containing non-encrypted sensitive personal data being stolen or hacked*
- *The school's cashless payment provider being hacked and parents' financial details stolen*