Data Protection Policy 2021/22

APPROVED ON

Applies to:	
Harrogate College	X
Keighley College	X
Leeds City College	X
Leeds Conservatoire	X
White Rose Academies Trust	X

CHANGE CONTROL

Version:	1.3	
Approved by:		
Date approved:		
Name of author:	Graham Eland	
Name of responsible committee:	SELT	
Related policies: (list)		
Equality impact assessment completed	**Date:**	
	Assessment type ☐ **Full** X **Part** ☐ **Not required**	
Policy will be communicated via:	Policy Portal and Luminate Education Group Intranets	
Next review date:	December 2022	

luminate
EDUCATION GROUP

Contents

1. INTRODUCTION

1.1 General Data Protection Regulation

The General Data Protection Regulation ('GDPR'). The General Data Protection Regulation 2018 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of persons and to ensure that personal data is not processed without their knowledge, and wherever possible, that it is processed with their consent.

The GDPR applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.

The GDPR applies to all controllers that are established in the EU (European Union) who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU including Great Britain that process personal data in order to offer goods and services,or monitor the behavior of data subjects who are resident in the EU.

1.2 GDPR Definitions

Personal data – any information relating to an identified or identifiable 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, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a person, data concerning health or data concerning a person's sexual orientation.

Data controller – the legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law.

Data subject – any living individual who is the subject of personal data held by an organisation.

Processing – any operation or set of operations which is performed on personal data or on 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, restriction, erasure or destruction.

Profiling **–** is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behavior.

Personal data breach **–** a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority (Information Commissioners Office) and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data subject consent **-** means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear action, signifies agreement to the processing of personal data.

Child **–** the GDPR defines a child as anyone under the age of 16 years old, although this may be lowered to 13 by law. The processing of personal data of a child is only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Luminate Education Group – "the group" organisation members Leeds City College, Harrogate College, Keighley College, Leeds Conservatoire and the White Rose Academies Trust including any additional members added to the group from November 2021.

2. Policy Statement

2.1 The Luminate Education Group Board and management are committed to compliance with all relevant laws in respect of personal data,and the protection of the "rights and freedoms" of individuals whose information the group collects and processes in accordance with the General Data Protection Regulation (GDPR).

2.2 Compliance with the GDPR is described by this policy and other relevant policies along with connected processes and procedures.

2.3 The GDPR and this policy apply to all of the group and personal data processing functions, including those performed on customers', clients', employees', suppliers' and partners' personal data, and any other personal data the organisation processes from any source.

2.4 Organisation Data Protection Officer/GDPR Owner roles are Graham Eland (FE Colleges), Eleanor Moore (Leeds Conservatoire) and Lee Garner (White Rose Academies Trust)

2.5 Organisation Data Protection Officer/GDPR Owners are responsible for reviewing the register of processing annually in the light of any changes to the group activities This register needs to be available on the Information Commissioners supervisory authority's request.

2.6 This policy applies to all staff of the group and outsourced suppliers. Any breach may be a criminal offence in which case the matter will be reported as soon as possible to the appropriate authorities.

2.7 Partners and any third parties working with or for the group, and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by the group without having first entered into a data sharing or data confidentiality agreement which imposes on the third party obligations.

3. Responsibilities and Roles

3.1 Leeds City College, Leeds Conservatoire and the White Rose Academies Trust are individual data controllers under the GDPR and are registered with the Information Commissioners Office (ICO).

3.2 The Data Protection Officer/GDPR Owner Job Description, is a role specified in the GDPR, is at Director (FE/HE) or Assistant Principal (Schools) level. The role is responsible for ensuring that compliance with data protection legislation and good practice can be demonstrated.This accountability includes:

3.2.1 development and implementation of the GDPR as required by this policy
3.2.2 security and risk management in relation to compliance with the policy.

3.3 Organisation Data Protection Officer/GDPR Owners, have been allocated responsibility for the group compliance with this policy on a day-to-day basis and, in particular, has direct responsibility for ensuring that the group complies with the GDPR, as do managers in respect of data processing that takes place within their area of responsibility.

3.4 Organisation Data Protection Officer/GDPR Owners have specific responsibilities in respect of procedures such as the Subject Access Request Procedure and are the first point of call for staff seeking clarification on any aspect of data protection compliance.

3.5 Compliance with data protection legislation is the responsibility of all staff of the group who process personal data.

3.6 Staff in the group are responsible for ensuring that any personal data about them and supplied by them to the group is accurate and up- to- date.

4. Data Protection Principles

All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. The group policies and procedures are designed to ensure compliance with the principles.

4.1 Personal data must be processed lawfully, fairly and transparently

Lawful – identify a lawful basis before you can process personal data. These are often referred to as the “conditions for processing”, for example consent.
Article 6 of the GDPR, a lawful basis is necessary whenever organisations process personal data.

It outlines six bases that are available, depending on the circumstances:

If the data subject gives their explicit **consent** or if the processing is necessary
To meet **contractual obligations** entered into by the data subject
To comply with the data controller's **legal obligations**
To protect the data subject's **vital interests**
For tasks carried out in the **public interest**
For the purposes of **legitimate interests** pursued by the data controller

Fairly – in order for processing to be fair, the data controller has to make certain information available to the data subjects as practicable. This applies whether the personal data was obtained directly from the data subjects or from other sources.

The GDPR has increased requirements about what information should be available to data subjects.

Transparently – the GDPR includes rules on giving privacy information to data subjects. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language.

The specific information that the group will provide to the data subject must, as a minimum include:

4.1.1 the identity and the contact details of the controller and, if any, of the controller's representative;
4.1.2 the contact details of the Data Protection Officer/GDPR Owner;
4.1.3 the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
4.1.4 the period for which the personal data will be stored;
4.1.5 the existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;
4.1.6 the categories of personal data concerned;
4.1.7 the recipients or categories of recipients of the personal data, where applicable;
4.1.8 where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;
4.1.9 any further information necessary to guarantee fair processing.

4.2 Personal data can only be collected for specific, explicit and legitimate purposes

Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the supervisory authority.

4.3 Personal data must be adequate, relevant and limited to what is necessary for processing

4.3.1 Organisation Data Protection Officer/GDPR Owners are responsible for ensuring that the group does not collect information that is not strictly necessary for the purpose for which it is obtained.

4.3.2 All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must include a fair processing statement or link to privacy statement.

4.3.3 The Data Protection Officer / GDPR Owner will ensure that, on an annual basis all data collection methods are reviewed by resource owners to ensure that collected data continues to be adequate, relevant and not excessive.

4.4 Personal data must be accurate and kept up to date with every effort to erase or rectify without delay

4.4.1 Data that is stored by the data controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

4.4.2 It is also the responsibility of the data subject to ensure that data held by the group is accurate and up to date. Completion of a registration or application form by a data subject will include a statement that the data contained therein is accurate at the date of submission.

4.4.3 Staff should be required to notify the group of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of the group to ensure that any notification regarding change of circumstances is recorded and acted upon.

4.4.4 The Organisation Data Protection Officer / GDPR Owners are responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

4.4.5 On at least an annual basis, the organisation Data Protection Officer / GDPR Owners will review the retention dates of all the personal data processed by the group, by reference to the data inventory, and will identify any data that is no longer required in the context of the registered purpose. This data will be securely deleted/destroyed.

4.4.6 The Organisation Data Protection Officer / GDPR Owners are responsible for responding to requests for rectification from data subjects within one month. This can be extended to a further two months for complex requests. If the group decides not to comply with the request, the Data Protection Officer / GDPR Owner must respond to the data subject to explain its reasoning and inform them of their right to complain to the supervisory authority.

4.5 Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

4.5.1 Personal data will be retained in line with the organisation Retention of Records Procedure and, once its retention date is passed, it must be securely destroyed as set out in this procedure.

4.5.2 The organisation Data Protection Officer / GDPR Owners must specifically approve any data retention that exceeds the retention periods defined in Retention of Records Procedure and must ensure that the

justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written.

4.6 Personal data must be processed in a manner that ensures the appropriate security

In determining appropriateness, the organisations Data Protection Officer / GDPR Owner should also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or students) if a security breach occurs, the effect of any security breach on the group itself, and any likely reputational damage including the possible loss of customer trust.

When assessing appropriate IT technical measures, the Group Director of IT and organisations ITSS managers will consider the following:

- Password protection
- Automatic locking of idle terminals;
- Removal of access rights for USB and other memory media
- Virus checking software and firewalls
- Role-based access rights including those assigned to temporary staff
- Encryption of devices that leave the organisations premises such as laptops
- Security of local and wide area networks
- Identifying appropriate international security standards relevant to the group.

When assessing appropriate organisational measures the orgainsations Data Protection Officer /GDPR Owners will consider the following:

- The appropriate IT security training levels throughout each organisation;
- Measures that consider the reliability of employees (such as references etc.);
- The inclusion of data protection in employment contracts;
- Monitoring of staff for compliance with relevant security training completion;
- Physical access controls to electronic and paper based records;
- Storing of paper based data in lockable fire-proof cabinets;
- Adopting clear rules about passwords;
- The contractual obligations to take appropriate security measures when transferring data outside the EEA.

These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

4.7 The organisation controller must be able to demonstrate compliance with the GDPR's other principles (accountability)

The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. The accountability principle in Article 5(2) requires organisations to demonstrate compliance with the principles and states explicitly that this is the responsibility of each organisation.

The group will demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, breach notification procedures and incident management response plans.

5. Data Subjects' Rights

5.1 Data subjects have the following rights regarding data processing, and the data that is recorded about them:

- 5.1.1 To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- 5.1.2 To prevent processing likely to cause damage or distress.
- 5.1.3 To prevent processing for purposes of direct marketing.
- 5.1.4 To be informed about the mechanics of automated decision-taking process that will significantly affect them.
- 5.1.5 To not have significant decisions that will affect them taken solely by automated process.
- 5.1.6 To take action to rectify, block, erase, including the right to be forgotten, or destroy inaccurate data.
- 5.1.7 To request the supervisory authority to assess whether any provision of the GDPR has been contravened.
- 5.1.8 To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.
- 5.1.9 To object to any automated profiling that is occurring without consent.

5.2 The group ensures that data subjects may exercise these rights:

- 5.2.1 Data subjects may make data access requests as described in the Subject Access Request Procedure, this procedure also describes how the group will ensure that its response to the data access request complies with the requirements of the GDPR.

- 5.2.2 Data subjects have the right to complain to their organisation related to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled in line with the Complaints Procedure.

6. Consent

6.1 The group understands 'consent' to mean that it has been explicitly and freely given, and a specific,informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time.

6.2 There must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication. The Controller must be able to demonstrate that consent was obtained for the processing operation.

6.3 For sensitive data, explicit written consent (Consent Procedure) of data subjects must be obtained unless an alternative legitimate basis for processing exists.

6.4 In most instances, consent to process personal and sensitive data is obtained routinely by the group using standard consent documents e.g. when a new student signs a learning agreement,or during induction for participants on programmes.

6.5 Where the group provides online services to children, parental or custodial authorisation must be obtained. This requirement applies to children under the age of 16 unless the state has made provision for a lower age limit, which may be no lower than 13.

7. Security of Data

7.1 All Staff are responsible for ensuring that any personal data that the group holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by the group to receive that information and has entered into a confidentiality or data sharing agreement.

7.2 All personal data should be accessible only to those who need to use it. All personal data should be treated with the highest security and must be kept:

- in a lockable room with controlled access; and/or
- in a locked drawer or filing cabinet; and/or
- if computerised, password protected in line with corporate requirements

7.3 Care must be taken to ensure that staff PC screens and terminals are not visible except to authorised staff of the group.

7.4 Manual records may not be left where they can be accessed by unauthorised personnel.

7.5 Personal data may only be deleted or disposed of in line with the organisation Retention of Records Procedure. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed as required before disposal.

7.6 Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off site.

8. Disclosure of Data

8.1 The group must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the police. All staff should exercise caution when asked to disclose personal data held on another individual to a third party and should approach their organisation Data Protection/GDPR Owner.

8.2 All requests to provide data for one of these reasons must be supported by appropriate paperwork, notably the Subject Access Request Form and all such disclosures must be specifically authorised by the organisation Data Protection Officer / GDPR Owner.

9. Retention and Disposal of Data

9.1 The group shall not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.

9.2 The group may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

9.3 The retention period for each category of personal data are set out in the Retention of Records Procedure along with the criteria used to determine this period including any statutory obligations the group has to retain the data.

9.4 Personal data must be disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of data subjects. Any disposal of data will be done in accordance with the secure disposal procedure.

10. Data Transfers

10.1 All exports of data from within the European Economic Area (EEA) to non-European Economic Area countries (referred to in the GDPR as 'third countries') are unlawful unless there is an appropriate "level of protection for the fundamental rights of the data subjects". There is a level of protection with Great Britain and the EEA.

11. Related Documents

Student Privacy Notice
Staff Privacy Notice
GDPR Subject Access Request Record
GDPR Subject Access Consent Form
GDPR Subject Access Withdrawal Form
GDPR Subject Access Procedure
GDPR Privacy Procedure
Data Disposal and Retention Schedule
Retention of Records Procedure