Data Protection Impact Assessment 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.

Definition of Personal Data

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

An **"identifiable person"** is one who can 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.

"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.

Purpose

With so much information being collected, used and shared in the provision of education, it is important that steps are taken to protect the privacy of United Learning's employees, pupils and members of the public and to ensure that personal information is handled legally, securely, efficiently and effectively.

Data Protection Impact Assessments (DPIA) are a tool which will enable United Learning to comply with its obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, control how our use of personal information impacts on individual privacy and ensure that personal data is processed in accordance with the Data Protection Principles which are detailed in appendix D.

Through the use of DPIAs we will be able to identify and assess any risks to privacy created by a new project or an adaptation of an existing project. A DPIA will be required when new personal information is to be collected and when information already held will be accessed by different employees, transferred out of the organisation or processed in a previously unforeseen way.

Through the use of DPIAs United Learning aims to:

- Ensure personal data is processed in accordance with the data protection principles;
- Identify privacy risks to individuals;

- Analyse how such privacy risks can be avoided or mitigated while meeting the aims of the project;
- Implement privacy solutions that are proportionate to the aims of the project;
- Enable the timely location and retrieval of personal information to meet the requirements of Subject Access requests;
- Protect the organisation's reputation.
- Demonstrate compliance with data protection law.

Data Protection Impact Assessment Procedure

1. Data Protection Impact Assessment screening

DPIA screening will be a part of all new projects that may involve the processing of personal data. The screening will be used to determine whether a full DPIA is required. It will be carried out by the project team at the initial stages using the form in **appendix A** and will be signed off by the project sponsor.

If no further action is required the project team should remain mindful of obligations to process personal data in accordance with the data protection principles which are listed in appendix D. A record of the decision not to carry out a DPIA should be kept on the EIP. Should the way in which personal data is processed change during the project's lifecycle the project leader should revisit the screening questions to determine whether a DPIA has become necessary.

2. The Data Protection Impact Assessment Process

The time and resources dedicated to a DPIA should be scaled to fit the nature of the project. It should be started early in the project and can run alongside the project development process.

3. The DPIA form

The DPIA will be carried out by the project team or the school's Data Protection Lead using the template in appendix B and referring to the guidance in appendix C. During the DPIA the team will:

- Identify the need for a DPIA;
- Describe the project's information flows;
- Answer the questions in the form which will help to;
    - Identify the privacy risks;
    - Identify the privacy solutions.
- If you are engaging a data processor the cyber security questionnaire must be used to identify the security risks.

4. Assessing the Risks

The DPIA will be reviewed by the project lead and the project sponsor. The risks will be assessed. Low risk DPIAs can be signed off by a trained school Data Protection Lead. Medium risk DPIAs must be reviewed and signed off by a member of the Data Protection Officer's team or the Information Security Officer. High Risk DPIAs must be signed off by the Data Protection Officer.

High risk projects are those which:

1. Are using data we already hold for a new purpose;
2. Involve special category personal information or financial information;
3. Involve building a bespoke system;
4. Send personal data outside of the EU;
5. Cyber security due diligence questionnaire score of more than 75.

Medium risk projects are those which meet one or more of the following criteria:

1. Collecting a new data set;
2. Involve the processing of more than basic amounts of personal data (for example, pupil characteristics, assessments/progress data, home contact details);
3. Cyber security due diligence questionnaire score of more than 75;
4. Involves the filming individuals.

Low risk projects are those which meet all of the following criteria:

1. Involve data we already hold;
2. Involves using data for a purpose that is already covered by our privacy notices;
3. Involves limited data, for example name and school email address only.

Implementation

The project lead will be responsible for ensuring that the agreed privacy solutions are integrated back into the project plan and that everyone working on the project is aware of the DPIA outcomes.

Review

A post project review will be carried out by the project lead to ensure that the privacy solutions identified by the DPIA have been implemented. The review date will be documented on the DPIA

Record keeping

The DPIA will be signed and recorded in the school's DPIA log on the EIP.

The final version of the DPIA will be stored in the DPIA log on the EIP.

Version number:	6.		Target Audience:	All staff
UCST/ULT/Both:	Both		Reason for version change:	Link to new Cyber Security Checklist added
Date Amended:	March 2023		Name of owner/author:	Alison Hussain
Date Authorised:	January 2017			
Authorised by:	FIC		Name of individual/department responsible:	Alison Hussain, Company Secretary and Data Protection Officer
Date reviewed:	21 June 2021			
Reviewed by:	FIC			
Date of next review:	June 2023			

Data Protection Impact Assessment Procedure – Appendix A

Privacy impact assessment screening questions

These questions will help your project team decide whether a full DPIA is necessary. If the answer to any of the following questions is 'yes' then the project team **must** complete the DPIA process outlined in Appendix B.

1. Will the project involve the collection of new personal data about individuals?
2. Will the project compel individuals to provide personal data about themselves?
3. Will personal data about individuals be disclosed to organisations or people who have not previously had routine access to the data? This includes different departments and schools within United Learning.
4. Will you be using personal data about individuals for a purpose it was not originally collected for?
5. Does the project involve you using new technology which might be perceived as being privacy intrusive?
6. Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?
7. Is the personal data of a kind particularly likely to raise privacy concerns or expectations? For example, employees' records or pupils' educational records.
8. Will the project require you to contact individuals in ways which they may find intrusive?

Data Protection Impact Assessment Procedure – Appendix C

Guidance for completing the privacy impact assessment template in appendix B.

Step one – identifying the need for a DPIA, describing the information flows and consulting with relevant stakeholders.

Use this section to identify the project aims and the benefits to the organisation, individuals and other parties. This will assist with identifying stakeholders and facilitate balancing identified risks against the aims and benefits of the project. You may find it helpful to link to other relevant documents related to the project, for example the project proposal.

Understanding the information flows involved in a project is essential to a proper assessment of the privacy risks. You should describe how information will be collected, stored, used and deleted. This will include what information will be used, what it will be used for and who will have access to it.

During the implementation of a new project it may be necessary to transfer data to external companies or allow them access to that data. Alternatively for a research project to take place it may be necessary to allow departments within the organisation access to data that they would not usually access. All such temporary data flows should be considered as part of the DPIA as well as the end outcomes.

This process can help to identify potential 'function creep', which is the unforeseen or unintended uses of personal data.

Where relevant internal and external stakeholders should be consulted with to ensure that you identify and address any privacy risks. Consultation can take place at any point during the DPIA process but it is useful to identify who the stakeholders are to ensure all relevant perspectives are taken into account.

Relevant stakeholders may include (but are not limited to) the project management team, external consultants, any potential suppliers, developers and external data processors, individuals and organisations who will have access to the personal data, departments within United Learning who have experience of similar types of projects, the IT team, the Company Secretarial team and employees at schools who may be impacted. It will also be useful to consult with the end users of any new system being developed. If there is the potential for any new information gathered to be used for statistical analysis the Data Team should also be consulted. Dependent on the project type it may also be advisable to consult with the individuals whose personal data will be processed.

Step two: Establishing the lawfulness of the processing.

The GDPR requires organisations to identify the legal basis for processing activity. There are 6 different legal bases. No one legal basis is more important than another, the important thing is to select the basis most appropriate to the processing. The options are set out in full in the DPIA template (appendix B).

If you are processing special category data you need to identify both a lawful basis for general processing and an additional condition for processing this type of data. The special categories of personal data and the conditions for processing are set out in full in the DPIA template.

Step three– assessing compliance & identifying risks

The questions in step three are intended to establish whether the project complies with the data protection principles (appendix D) and identify any additional actions needed to ensure compliance.

Further Actions to be taken

In these sections you should detail who has been consulted internally and externally to ensure that you identify and address any privacy risks. Consultation can take place at any point during the DPIA process but it is useful to identify who the stakeholders are to ensure all relevant perspectives are taken into account.

Relevant stakeholders may include (but are not limited to) the project management team, external consultants, any potential suppliers, developers and external data processors, individuals and organisations who will have access to the personal data, departments within United Learning who have experience of similar types of projects, the IT team, the Company Secretarial team and employees at schools who may be impacted. It will also be useful to consult with the end users of any new system being developed. If there is the potential for any new information gathered to be used for statistical analysis the Data Team should also be consulted. Dependent on the project type it may also be advisable to consult with the individuals whose personal data will be processed.

You must record any actions that need to be taken to identify risks and solutions that are in place or need to be put into place and who is responsible for those actions.

Identify and evaluate privacy solutions

The purpose of the DPIA is to reduce risk to an acceptable level while still allowing a useful project to be implemented. The aim of this stage is to ensure that the impact on privacy is proportionate to the aims of the project.

The DPIA should evaluate the costs and benefits of all the possible solutions to each privacy risk identified and state whether they would result in the risk being eliminated, reduced or accepted.

There are many different steps which can be taken to reduce a privacy risk. Some of these are:

- Deciding not to collect or store particular types of information
- Devising retention periods which only keep information for as long as necessary and planning the secure destruction of information.
- Implementing appropriate technological security measures.
- Ensuring that staff are properly trained and aware of privacy risks.
- Anonymise information when it is possible to do so.
- Producing guidance for staff on how to use new systems and how to share data if appropriate.
- Using systems which allow individuals to access their information more easily and make it easier to respond to subject access requests.

- Taking steps to ensure that individuals are fully aware of how their information is used and can contact the organisation for assistance if necessary.
- Selecting data processors who will provide a greater degree of security and ensuring that agreements are in place to protect the information which is processed on an organisation's behalf.
- Producing data sharing agreements which make clear what information will be shared, how it will be shared and who it will be shared with.
- Confirm that the project is complying with the data protection principles.

Step four – Identify risk of harm to data subjects / school / United Learning.

In this section you should

- Record any risks to individuals, including possible intrusions on privacy where appropriate.
- Assess any risks to the group, including regulatory action, reputational damage and loss of public trust.
- Maintain a record of the identified risks.

Risk to individuals

The following are possible risks to individuals that should be considered:

- Information being shared inappropriately through inadequate disclosure controls.
- Information being used for a new purpose without the individual's knowledge.
- New surveillance methods creating an unjustified intrusion on privacy.
- Intrusive measures being taken against individuals as a result of collecting the information.
- Collecting more personal data than is needed for the purposes.
- The sharing or merging of data sets can allow organisations to collect a much wider set of information than individuals might expect.
- Enabling identifiers to be linked to anonymised data may mean it is no longer safely anonymised.
- Information collected and stored unnecessarily presents a greater security risk.
- Allowing the creation of duplicate records creates the risk that information will become out of date or unsecure.
- Retention periods must be established so that information is not held for longer than necessary.

Risks to the Group

- Non-compliance with the DPA can lead to sanctions, fines and reputational damage.
- Problems identified after the project has launched are more likely to require expensive fixes.
- Information that is not properly managed is less useful to the group.
- Public distrust about how information is used can damage the group's reputation.
- Data losses which damage individuals could lead to claims for compensation.

Sign off and record DPIA outcomes

The DPIA should be signed by the project lead, the school DPL and, if high risk, by a member of the Data Protection Officer's team .

Integrate the DPIA outcomes into the project plan

The results of the POA process should be fed back into the wider project management process. You should use the template to record what actions will be taken and who will be responsible for their implementation.

Step six – Detail the results of the post project review.

A date must be identified for a post project review which should be carried out to ensure that the privacy solutions identified in the DPIA have been successfully implemented and to ensure that decisions taken in the DPIA are still valid.

Appendix D

Data Protection Principles

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Appendix E

Article 28 requirements for data processing agreements

Data processing contracts must set out:

- The subject matter and duration of the processing;
- The nature and purpose of the processing;
- The type of personal data and categories of data subject; and
- The obligations and rights of the controller.

Contracts must require the processor to:

- Only act on the written instructions of the controller;
- Ensure that people processing the data are subject to a duty of confidence;
- Take appropriate measures to ensure the security of processing;
- Only engage sub-processors with prior consent and under a written contract;
- Assist the controller in providing SARs and allowing data subjects to exercise their rights;
- Assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- Delete or return all personal data to the controller as requested at the end of the contract;
- Submit to audits and inspections;
- Provide the controller with whatever it needs to ensure both are meeting Article 28 obligations;
- Tell the controller immediately if it is asked to do something infringing the GDPR.