United Learning Group personal data security breach policy and procedure

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

"ICO" means Information Commissioners Office

"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.

"Personal data security breach" means any loss, corruption or any unauthorised release of personal data. For the avoidance of doubt as well as data loss caused by malicious cyber-attacks data security breaches include personal data going missing in the post, emails containing personal data being sent to the wrong recipient and loss of unencrypted devices containing personal data. The ICO has confirmed that we do not need to report the loss of personal data on encrypted devices.

Policy Statement

All personal data security breaches that result in a risk of harm to data subjects will be reported to the ICO within 72 hours of our becoming aware of the breach. Staff will receive training on how to recognise a data security breach and who to inform of a personal data security breach. The ICO will be given all of the information detailed on the Personal data security breach notification form. If it is not

possible to provide all of this information within the 72 hours the information will be given to the ICO in phases without undue further delay.

Action will be taken to minimise the potential consequences of any personal data security breach.
When the personal data security breach is likely to result in a high risk to the rights and freedoms of the data subject we will communicate the personal data security breach to the data subject without undue delay.

Procedure

The school and central office departments will ensure that **all** staff receive training regarding:

- What a personal data security breach is.
- Who to report a personal data security breach to.
- The potential consequences of a personal data security breach to the data subject and the organisation.
- The personal consequences that could result from the unauthorised accessing of personal data.

The school and central office departments will ensure that a sufficient number of individuals are trained to respond to personal data security breaches to enable us to comply with the requirement to report a breach within 72 hours.
In the wake of a personal data security breach swift containment and recovery of the situation is vital.

When a member of staff reports a personal data security breach the Data Protection Lead will take whatever steps are necessary to minimise the potential consequences of the personal data security breach and will complete the data security breach log on the EIP as soon as possible.

The Data Protection Officer or delegate will decide whether to report the incident to the ICO and whether the data subjects should be informed.

Version number:	3.		Target Audience:	All staff
UCST/ULT/Both:	Both		Reason for version change:	Periodic review - no changes made.
Date Authorised:	25/09/2017		Name of owner/author:	Alison Hussain
Authorised by:	FIC		Name of individual/department responsible:	Data Protection Officer
Date reviewed:	12/01/2023			
Reviewed by:	IGSC			
Date of next review:	January 2025			