United Learning Group personal data 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 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 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 breaches 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 breach and who to inform of a personal data breach. The ICO will be given all of the information detailed on the Personal data 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 breach.

When the personal data breach is likely to results in a high risk to the rights and freedoms of the data subject we will communicate the personal data breach to the data subject without undue delay.

Procedure

The school will ensure that all staff receive training regarding:

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

The school will ensure that a sufficient number of individuals are trained to respond to personal data breaches to enable us to comply with the requirement to report a breach within 72 hours.

In the wake of a personal data breach swift containment and recovery of the situation is vital. When a member of staff reports a personal data breach the designated individual will take whatever steps are necessary to minimise the potential consequences of the personal data breach and will inform the Group Director of Technology, the Information Security Manager (ISM), the Company Secretary and the Assistant to the Company Secretary (ACS) as soon as possible.

The designated individual will work with the ISM and ACS to complete the personal data breach notification form. The Company Secretary or delegate will submit the form to the ICO.

The DSO will keep a record of all personal data breaches.

Version number:	1.0		Target Audience:	All staff
UCST/ULT/Both:	Both		Reason for version change:	GDPR
Date Authorised:			Name of owner/author:	Alison Hussain
Date issued:			Name of individual/department responsible:	Steve Whiffen, Company Secretary
Date Reviewed:				