Breaches

Schools may be required to report a data breach, if the breach is likely to result in a risk to the rights and freedoms of to the relevant supervisory authority and, if necessary, the individuals affected.

A breach notification must contain:

- The nature of the personal data breach, including the categories and approximate number of individuals, as well as personal data records concerned.
- The name and contact details of the DPO or other contact point where more information can be obtained.
- A description of the likely consequences.
- A description of the measures taken, or proposed to be taken, to deal with the breach.

The relevant authority, e.g. the ICO, must be notified of the breach with 72 hours of the school becoming aware of it.

FAQs

Are images of children considered to be personal data under the GDPR?

An image of a child is considered to be personal data under the GDPR; meaning that, where the child is under the age of 13, the consent of the concerned individual's parent is required before their data can be processed.

Under the GDPR, how long should we keep permission slips for school trips and visits?

Parental consent forms for school trips and visits where no major incident occurred should be kept until the conclusion of the trip; where a major incident did occur, the relevant permission slips should be kept until the pupil is 25-years-old (as part of their record of education).

In line with the GDPR, can schools display images of past pupils?

Schools are able to use pupil photographs as part of a display if they have a lawful basis for doing so, such as the individual's consent; however, depending on the purpose of use consented to prior to the photograph being taken, the individual's consent may need to be refreshed.

The ICO state that "the consent gained at the time of the photo being taken will have been for a different purpose; therefore, in line with fair processing, the school would need to inform the individual of their plans to use the image and gain consent in relation to this new purpose".

The General Data Protection Regulations (GDPR) information leaflet

This leaflet is an introduction to the GDPR and includes a summary on the following:

What is the GDPR?

The GDPR is a set of guidelines for the collection and processing of personal information of individuals within the EU and is effective in the UK from 25 May 2018 – replacing the Data Protection Act (DPA) 1998.

Last updated: 24 April 2018

Definitions

Data subject – is an individual who is the subject of the personal data.

Data controller – a person, or organisation who determines the purposes and ways that data is processed.

Data processor – any person who processes data on behalf of the data controller.

Data protection officer (DPO) – the person(s) responsible for ensuring the school is compliant with data protection legislation.

Personal data – information that can identify an individual, such as an address.

Sensitive data – information consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, etc.

Consent

Under the GDPR, consent **must** be:

- Freely given.
- Specific.
- Informed.
- Unambiguous.
- Firm confirmation or a positive opt-in (not pre-ticked boxes for example).

Consent **cannot** be obtained from the following:

- Silence
- Pre-ticked boxes
- Inactivity

Consent obtained under the DPA may need to be reobtained in compliance with the GDPR.

Individuals' rights

The GDPR has created new rights for individuals and strengthens some that existed under the DPA –these are the following:

- **The right to be informed**
- **The right of access**
- **The right of rectification**
- **The right to erasure**
- **The right to restrict processing**
- **The right to data portability**
- **The right to object**
- **Rights to automated decision-making and profiling**

Pupils' data and children

The GDPR has introduced new provisions that are intended to enhance the protection of children's data.

Under the GDPR, children may, from the age of 13, consent for themselves, if it is deemed by the school that they have the capacity to understand the privacy notice. If not, the school should seek parental consent.

Storage

Article 5 of the GDPR states that personal data must be subject to the appropriate technical and organisational measures required to protect it against unlawful processing, and against accidental loss, destruction or damage. This could include a locked filing cabinet for paper files and encrypted, password-protected files for digital data.

Accountability and governance

Under the GDPR, schools are expected to have comprehensive and proportionate governance measures in place to minimise the risk of data breaches. Schools should:

- Implement internal data protection policies, e.g. staff training or reviews of internal HR policies.
- Maintain relevant documentation and processing activities.
- Appoint an appropriate DPO.
- Implement measures that meet the principles of data protection by default, including data minimisation and transparency.
- Use data protection impact assessments where appropriate.

DPO

The DPO for St Luke Academies Trust is Nathalie Young

Any questions that you have regarding the GDPR can be directed to Nathalie using Nathalie.young@st-luke-at.co.uk or 01536 203251