Breaches

One of the most important considerations with data is loss, destruction, alteration or unauthorised disclosure. A data breach can be incredibly serious and the school may have to inform the Information Commissioners Office.

Information reported 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.

Sharing Data

Before you share data with any other organisation you need to consider the following:

- Is the request justifiable?
- Are there appropriate security measures in place?
- How will it be transferred?
- How long will it be retained?
- Is a data protection impact assessment required?

Data Safeguarding

As staff have access to personal/sensitive data, it is important to think about the following:

Do I have complexity to my passwords, do I change passwords regularly?

Is data that I take off site on my laptop/external drive encrypted?

Do I lock my workstation when I leave the room?

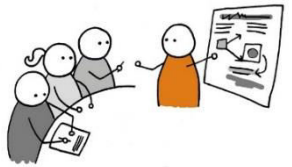
If I access school email on my phone is there 2 factor authentication? Is my phone software up to date?

Do I ask permission before I send any personal information about pupils to other organisations or upload it to a software app?

'Data Shadow'

In schools we ensure the safeguarding of children in everything we do. Part of this safeguarding duty is ensuring the security of a child's information, a 'data shadow' that accompanies them.

The General Data Protection Regulations (GDPR) staff training leaflet



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

- What the GDPR is
- Consent
- Individuals' rights
- Storage
- Responsibility
- Data sharing & safeguarding
- Accountability and governance
- Data protection officer (DPO)
- Data breaches

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: 18th May 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 name, address.

Sensitive data – information consisting of racial or ethnic, health, safeguarding info 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 re-obtained 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**

Responsibility

As schools collect & store information about pupils, parents & staff **ALL** staff in school have a responsibility to ensure that they think about data security in all aspects of their work.

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 minimization and transparency.
- Use data protection impact assessments where appropriate.

DPO

The DPO for Birkwood is Tim Pinto.

Any questions that you have regarding the GDPR can be directed to Tim via Suzanne Savage in the school office.

Contact information for parents is given on the school's privacy notice available on the school website.