# Data Protection for Schools and Higher Education

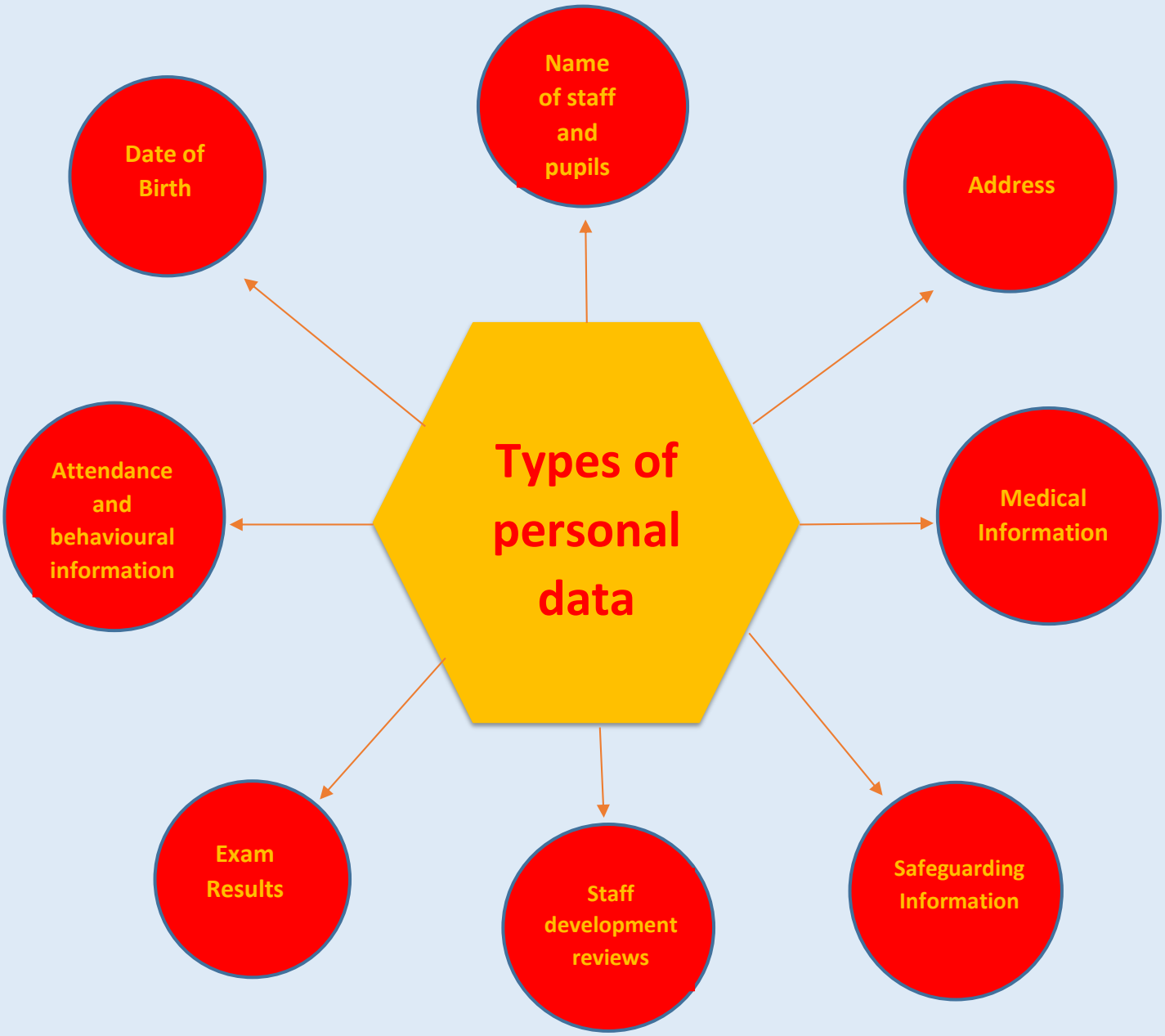
Cardiff council provides the contracted role of the Data Protection Officer for schools across Cardiff.  Our team is dedicated to helping schools meet and exceed the requirements of GDPR advocating accountability and demonstrating compliance in the sometimes challenging world of data protection. We are on hand to offer friendly and timely guidance to support you in achieving this goal.

What we offer:

- Day-to-day advice on data protection matters.
- Guidance on handling of Data Security incidents.
- Regional training events and bespoke, in-house training for schools.
- Developing and review of school Data Protection and Freedom of Information Policies.
- Access to e-learning training modules.

HIGH QUALITY TRAINING
FOR THE PUBLIC SECTOR

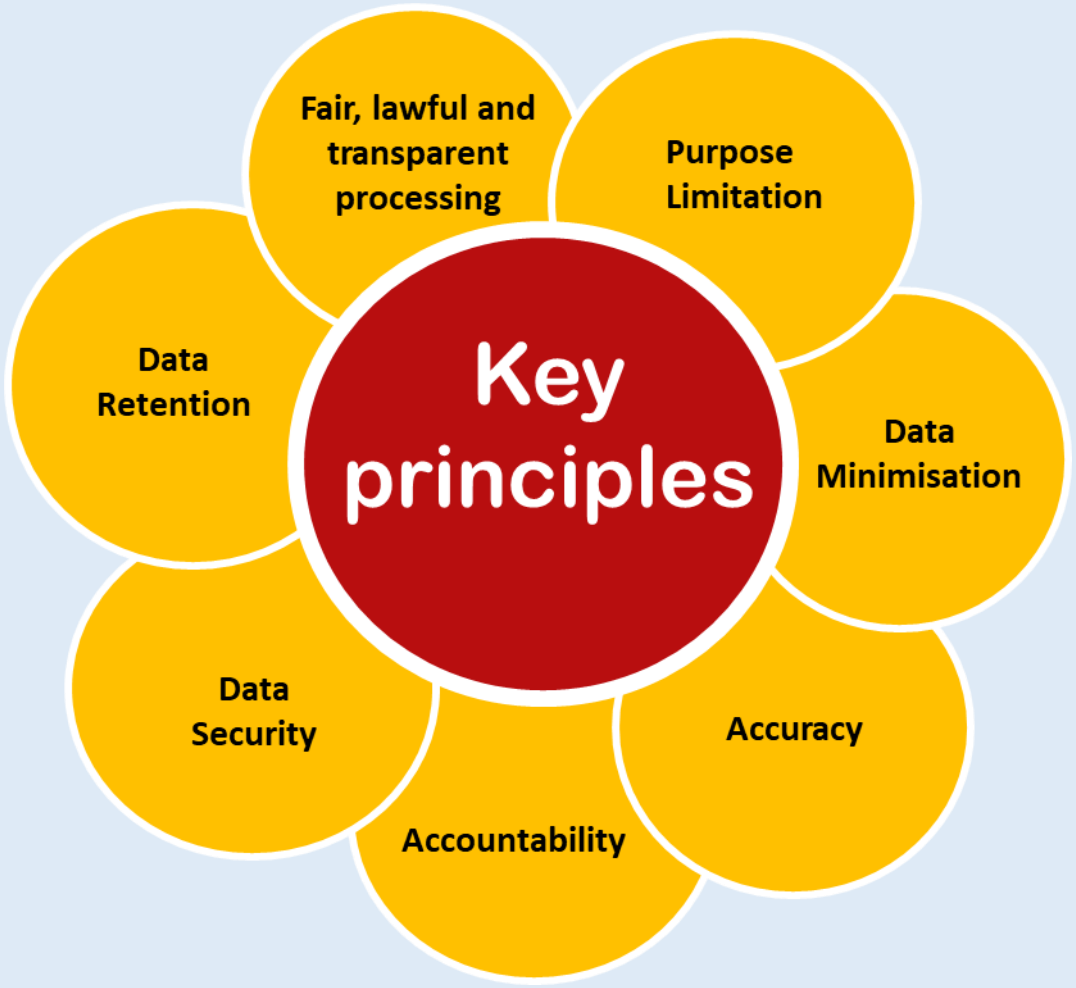
# Personal Data


HIGH QUALITY TRAINING FOR THE PUBLIC SECTOR

# The Key Data Protection Principles

In order to protect data subjects' personal information, schools should follow several key principles:



**Possible security measures for data protection include:**

- Shredding all confidential waste.
- Using strong passwords.

- Installing a firewall and virus checker on your computers.
- Encrypting any personal information held electronically.

- Disabling any ‘auto-complete’ settings.
- Holding telephone calls in private areas.

- Limiting access, i.e. only those who absolutely need to access the data
- Checking the security of storage systems.

- Keeping devices under lock and key when not in use.
- Not leaving papers and devices lying around.

# Understanding the General Data Protection Regulation (GDPR)

1. Awareness

It is important all staff know the importance of Data Protection and how to comply with the law.

2. Information you hold

It is vital to understand what information is being collected and stored in order to fully protect it and comply with legislation. An asset register is a way to help you understand and manage your organisations information assets and organise them. Please see our guidance document for more information.

3. Privacy notices

These must be in plain English and be easy to understand. Privacy notices must be provided at the point of capturing personal data, and individuals must be kept aware of any changes.

4. Individual's rights

Individuals have specific rights in relation to how we process their personal data. Schools must ensure that these rights are not compromised in any way.

5. Individual rights requests

Individuals have the right to request their personal data schools hold on them, as well as the right to erase or rectify personal data where appropriate.

6. Lawful basis for processing data

You must have a valid lawful basis in order to process personal data. A toolkit is available to help you identify which lawful basis you are relying upon.

7. Consent

Consent should only be obtained and relied upon if there is no other lawful reason for processing. Consent must be given actively, and must be able to be withdrawn at any time.

8. Children

Children over the age of 13 now have the same rights as adults when it comes to personal data, and this must be reflected in our privacy notices.

9. Data breaches

Data breaches now need to be reported to the ICO within 72 hours. All breaches must be reported to the Data Loss Team within 24 hours; do not undertake your own investigation before reporting it to us.

# Data Breaches

**Printing Error**

**Asset Loss**

**The accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. Art. 4 (12)**

**Email Incident**

**Data loss**

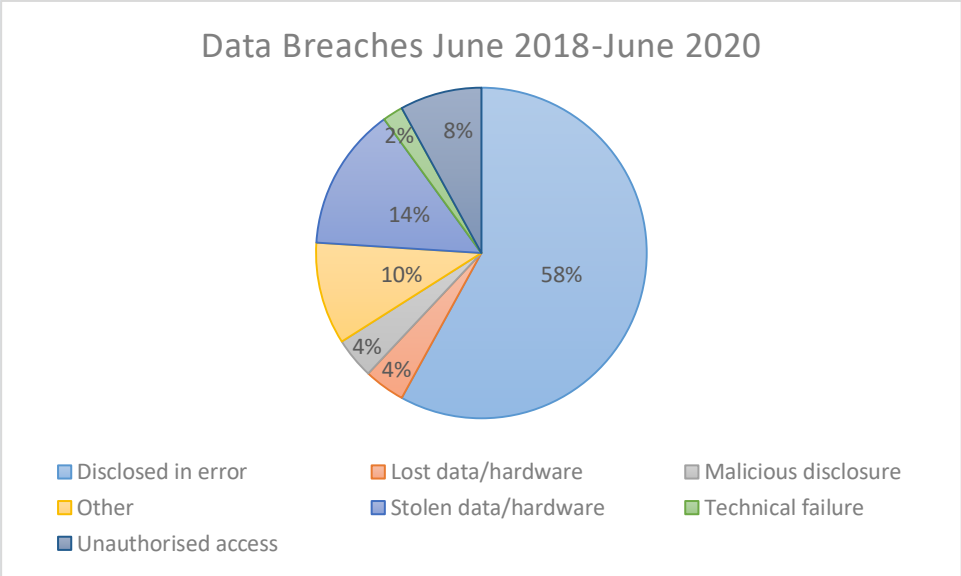
**All potential data breaches must be reported to Information Governance within 24 hours of being made aware of the breach.**

**Email: Schoolsinformationmanagement@cardiff.gov.uk**

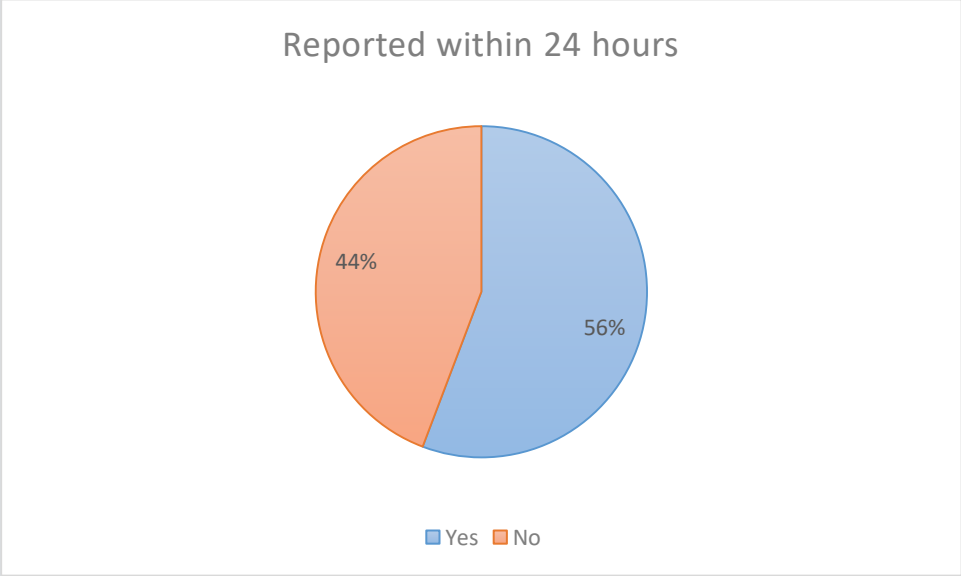
HIGH QUALITY TRAINING FOR THE PUBLIC SECTOR

SOLUTIONS

## Types of incidents




## Data Protection Incidents reported within 24 hours (2018-2020)



# DID YOU KNOW?

You must keep a record of any personal data breaches, regardless of whether you are required to notify.

It is mandatory that the organisations Data Protection Officer investigates all incidents and makes recommendations and actions as a result of any breach.

**Failure to comply with Data Protection Act can lead to enforcement action and a fine of up to £17,000,00**

The Data Protection Officer will make a decision on reporting the incident to the Information Commissioners office within 72 hours of being notified of the breach to ensure that the Council complies with the requirements of the Regulations.

Training is key!

HIGH QUALITY TRAINING FOR THE PUBLIC SECTOR

SOLUTIONS

# Individual rights

The GDPR provides the following rights for individuals:

1. The right to be informed

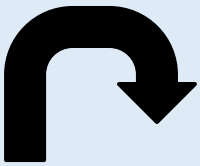
2. The right of access

3. The right to rectification

4. The right to erasure

5. The right to restrict processing

6. The right to data portability



7. The right to object

Schools should be especially aware of two individual rights:

1. The right to be informed

The right to be informed covers some of the key transparency requirements of the GDPR. It is about providing individuals with clear and concise information about what you do with their personal data.

To meet the requirements of the Data Protection Act 2018 and General Data Protection Regulation (GDPR), schools are required to issue a **Privacy Notice** to children and young people and/or parents and guardians summarising the information held on record about children and young people, why it is held, and the third parties to whom it may be passed.

2. The right of access

Individuals have the right to access their personal data. This is commonly referred to as a **subject access request (SAR)**. A SAR can be made verbally or in writing.

One of the most important points to remember about SARS is that schools must respond within one calendar month. However, an SAR can be extended by a further two months if the request is complex or if a number of requests have been received from the individual. However the individual must be notified of this within one month of receiving this request and explain why this is necessary.

For more information on SARs please see our guidance document.