Data Breach

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Personal data breaches can include:

- access by an unauthorised third party.
- deliberate or accidental action (or inaction) by a controller or processor.
- sending personal data to an incorrect recipient.
- computing devices containing personal data being lost or stolen.
- alteration of personal data without permission.
- loss of availability of personal data.

A data breach must be reported to the ICO immediately and no later than 72 hours from becoming aware of the breach.

The GDPR states that you must provide the following information when reporting a breach:

- description of the nature of the personal data breach including, where possible:
    - the categories and approximate number of individuals concerned.
    - the categories and approximate number of personal data records concerned.
- the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained.
- a description of the likely consequences of the personal data breach.
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

The GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. Article 34(4) allows you to provide the required information in phases, as long as this is done without undue further delay. In the first instance, you must report this to the senior person within your school responsible for GDPR - either Sarah Manning or Faye Dennis.

Failure to notify a breach can result in a significant fine for your organisation

Data Breach Reporting

Complete the sections below even if you do not have all the answers as soon as possible – It must be done within 72 hours of being made aware of the breach!

Date	
Name of Data Protection Officer	The Onto Group (GDPR@theontogroup.com / 0161 504 6921)
Name of senior member of staff with GDPR responsibility	
Description of breach: a) the categories and approximate number of personal data records concerned b) the categories and approximate number of individuals concerned	
Consequences of the breach	
Measures to be taken or proposed as a result of the breach	
Measures taken to mitigate the breach	