General Data Protection Regulation

DATE: OCTOBER 2018

FALMOUTH MAT

STAFF NEWSLETTER

GDPR—Edition 2

This newsletter is designed to raise staff awareness around GDPR. It will help you identify what a data breach looks like and what to do if a data breach occurs. It also gives an introduction to when consent needs to be obtained for data.

What is a personal data breach

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

Examples of a data breach could include the following (but are not exhaustive):

- Loss or theft of data or equipment on which data is stored, for example loss of a laptop, memory stick or a paper file (this includes accidental loss)
- Inappropriate access controls allowing unauthorised use
- Human error (for example sending an email containing personal data to the wrong recipient)

In This Edition:

Minimise the risk of a data breach

- There is lots that you can do to minimise the risk of a data breach:
- If you use a memory stick it should be encrypted
- If you send a confidential document to an external e-mail address, make sure you send it securely
- Lock your workstation when you are not at your desk
- Lock paperwork away at the end of the day
- Before giving information over the phone or in person, make sure you know who you are talking to and whether they are permitted to receive the information you are about to give

Consequences of a data breach

Data protection is everyone's responsibility. In the event of a data breach the ICO can issue warnings, reprimands, corrective orders or impose fines depending on the severity. There are also very serious consequences in terms of reputation and trust that could be hugely difficult to overcome.

Data breach procedure

There is a MAT data breach poster in the staff room and main office of each school that outlines the steps that have to be taken in the event of a suspected data breach. Each school has access to the electronic form that needs to be completed and this should be submitted to the Data Protection Officer (Claire Collins) as soon as possible. Any data breach must be reported to the Information Commissioners Office (ICO) **within 72 hours** so time is critical.

FALMOUTH SCHOOL

St. Francis C. of E. School

Sending a document securely

Think before sending any personal data to an external e-mail address and ensure it is sent securely!

If you need to send student or staff data to an external e-mail address and are not sure how to send it securely, please speak to the DPO who will be able to advise who within your school can assist you.

GDPR only applies to personal data, which is information relating to an identified or identifiable person. You don't need to worry about data that can't be specifically linked to an individual, including data that has been anonymised.

Falmouth MAT data audit

Falmouth MAT is in the process of compiling a high level data map to show what data is processed and controlled across all of its schools. There could be instances where applications are used by staff and may not be on the radar of SLT. When the mapping process has been completed, it will be shared with staff so they can ensure that nothing has been missed. Your input to this is extremely important. If you use an application/service and have received GDPR compliance information from them, please ensure this is sent to the DPO so it can be stored centrally and support the data map audit.

The audit will be kept up to date by the DPO. If you want to start using a new application/ piece of software within school please speak to IT in the first instance to ensure security and compatibility. If this is all in order, you will then need to contact the DPO to ensure it is added to your school's high level data map. If the application/ software requires staff or student data, the DPO will be able to point you in the right direction regarding to how to obtain any necessary consent.

Consent

It is often assumed that you must always have consent to be able to process personal data – this is not true. Consent is only one of the six lawful basis' for processing and, in the case of schools, consent is not likely required for the core purpose operations of running the school. Consent is, however, likely to be required for non-core operations, such as marketing. You must have a valid lawful basis in order to process personal data.

The lawful basis for processing is set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Contact Claire Collins (MAT Officer and DPO) if you have any questions relating to GDPR (DPO@falmouthmat.org.uk)