Plymouth Catholic Schools Trust
Multi Academy Trust Notice 1712

TITLE: General Data Protection Regulation (GDPR)

Introduction

The General Data Protection Regulations (GDPR) replace the current Data Protection Act (DPA) on 25th May 2018. The new regulations represent a significant change and we need to act now and start work if we are to become compliant with the new law next May.

This MAT Notice is intended to provide a brief introduction to GDPR and outline some immediate next steps in preparation for compliance. Further communication will take place as we count down to May 2018.

Plymouth CAST is a Multi-Academy Trust; this means Plymouth CAST is responsible for schools' compliance with the GDPR. If a school belonging to the Trust breaches GDPR then the Trust is responsible as the "data controller". Under the new regulations, Multi-Academy Trusts must appoint a Data Protection Officer (DPO) and schools should appoint a Data Protection Co-ordinator (DPC). Schools may share one if geographically convenient.

What is Changing in General?

Keeping personal data safe. This is the most important area of compliance. The DPA requires you to implement technical and organisational measures to keep personal data secure. These obligations are significantly expanded under the GDPR.

The GDPR will explicitly require you to consider a number of privacy enhancing techniques, including the following: Privacy by Design; Data Minimisation; Using encryption where appropriate and Privacy impact assessments (PIAs).

Data breach obligations. Under the GDPR it becomes a legal requirement for you to report most security breaches to the Information Commissioner's Office (**ICO**) within 72 hours. You are also required to notify data subjects if the breach is likely to be a "high risk" to the individual.

Document Title:	1712 – General Data Protection Regulation	Sponsor:	COO
Version:	Final	Date:	1 Sep 17
Approved by:	iCEO	Review:	28 Feb 18

Consent as a legal basis for processing. For most uses of personal data you will rely on legal grounds other than consent, e.g. that it is necessary to comply with your legal obligations. The GDPR requires a very high standard of consent which must be given by a clear affirmative action (freely given, specific, informed, and unambiguous).

Record keeping. There is a general obligation under the GDPR to "demonstrate" compliance with the data protection principles. Each school is required to have a document of processing activities which must include: A description of the personal data processed; the purposes of the processing; the categories of recipients and the retention periods.

Privacy notices. Under the DPA, you must be transparent when handling personal data and, as part of this, you must give individuals (e.g. pupils, parents and staff) certain information about how their personal data is used. This information is normally provided in a document known as a privacy notice or fair processing statement. With the introduction of the GDPR the privacy notice will require significantly more information. The GDPR explicitly requires privacy notices aimed at children to be age appropriate.

Subject access requests. You may be familiar with Subject Access Requests under the DPA. Individuals are entitled to receive a copy of their personal data and supplemental information such as classes of recipients and sources. The timescale for this information to be given to the individual/s changes from 40- days to one month, the time period does not stop during school holidays.

New and enhanced rights. The GDPR gives individuals new rights in their data and also enhances existing rights. You should familiarize yourself with these new rights to understand when and how they apply.

Using contractors. Under the DPA, there must be a written contract in place between you and any contractor who is able to access the personal data which you hold. This includes cloud storage providers and external payroll providers, for example.

What does this mean for Schools in practical terms?

Retaining Information. Schools can no longer assume the right to gather and retain data. Specific permission is now required - usually in the form of specific clause in a Home/School or Parent Contract. The principle here is that the person(s) whom the data 'belongs' to must 'opt-in' with their permission for schools to hold it.

Recruitment. It is no longer permissible to make unsolicited approaches to third parties for general or marketing purposes – even if you have a pre-existing relationship with them. In most cases the renewal of a Home/School agreement will cover provided it contains an explicit clause and is signed. A useful method of compliance is for marketing material or brochures to state 'by responding to this phone/email you are granting permission for us to contact you' or words to that effect.

Electronic Backup. All schools must maintain a system of electronic backup and restore for data storage in their management information systems. The backup system must be checked and proved by actual activation on an annual basis. Best practice suggests annually at a remote site.

Getting it wrong

The DPA already gives good reasons to take data protection seriously. Failure to observe data protection legislation could result in fines of up to £500,000. Under the GDPR, the potential fine is the greater of up to €20 million or 4% of annual turnover.

As well as having financial consequences there can be serious reputational damage caused by data protection breaches. The ICO will often make enforcement action public on its website.

What do Academies Need to Do Next?

Plymouth CAST's overall accountability for compliance with GDPR rests with the Chief Executive Officer (CEO) as the Trust's Data Protection Officer (DPO). The CEO delegates responsibility for day to day management to the Chief Operating Officer (COO) who will plan and manage activity to ensure compliance.

The following actions need to be completed by the dates shown:

By 15 October 2017

The attached notice should be displayed in staff rooms to increase awareness of GDPR.

Every Plymouth CAST Academy Head Teacher is to nominate a Data Protection Coordinator (DPC) and notify admin@plymouthcast.org.uk

By 15 November 2017

The COO will amend the current Plymouth CAST Data Protection Policy.

Academy nominated DPC's to revise the following documents (as applicable) to ensure 'opt-in' for holding of data. In most cases this is a simple check box to give permission.

- Staff consent forms (or equivalent)
- Pupil consent forms (or equivalent)
- Home/School Agreement or Parental Contract
- Promotional literature for prospective parents

Academy nominated DPC's to confirm electronic backup arrangements at their school and determine if additional resources or processes are required.

By 30 November 2017

Academy DPC's will be invited to complete an electronic survey regarding completion of the above.

Regional conferences for DPC's will be scheduled for the Spring Term.

By 28 February 2018

Regional conferences for DPC's complete.

For further information and support please contact admin@plymouthcast.org.uk