Information Management
UK General Data Protection Regulation (GDPR)

When the GDPR comes into force on 25th May 2018, it will entirely replace our current Data Protection Act 1998 (DPA) and radically overhaul many of our existing data protection rules.

At Brownlow Fold the Headteacher, Deputy Headteacher and School Business Manager are working together to see how the data protection law is changing and how those changes will affect how our school.

The head teacher in all schools retains overall responsibility for data protection. However, at most schools the school business manager has the day to day responsibility for data protection in school. The GDPR changes will impose **significant additional compliance burdens.**

Accountability and Data Governance: One of the main features of the GDPR is that compliance alone is not enough; data controllers will also have to demonstrate their compliance and prove that they are taking data protection seriously by implementing a range of accountability measures. These measures include Privacy Impact Assessments, data protection audits, policy reviews, activity records and the mandatory appointment of a DPO.

Here is an overview of some of the accountability measures to understand:

Privacy Impact Assessments: Privacy Impact Assessments (PIA) are not new but what is new is that the GDPR will expect them to be undertaken in certain cases. PIAs will need to be carried out when we are planning a new initiative which involves "high risk" data processing activities i.e. where there is a high risk that an individual's right to privacy may be infringed such as monitoring individuals, systematic evaluations or processing special categories of personal data, especially if those initiatives involve large numbers of individuals or new technologies such as biometrics.

The idea behind a PIA is to identify and minimize non-compliance risks.

The ICO has produced a Code of Practice on PIA's which will help guide you through the process.

Pseudonymisation: This new term refers to the technique of processing personal data in such a way that it can no longer be attributed to a particular data subject without cross referencing it with other further information. The further information must be kept separate and subject to technical and organizational security measures so as to ensure that the data subject cannot be identified.

Pseudonomised information is still a form of personal data but the GDPR promotes its usage in certain circumstances in order to enhance privacy and contribute to overall compliance.

E.g. GDPR may expect pseudonymisation to be considered when personal data is processed in a way which is "incompatible" with the purposes for which it was originally obtained. Alternatively, the technique could be appropriate for schools wishing to use pupil data for historical or statistical purposes.

Data Protection Audits: As a school we need to review and document the personal data we hold, identify the source and who it is shared with. This exercise is commonly called a data protection audit and can be deployed across the entire school or confined to distinct areas within the school. Unless we know what personal data we hold and how it is being processed, it will be difficult to comply with the GDPR's accountability principles which require us to be able to demonstrate how we comply with the data protection principles in practice.

Another critical benefit of a data protection audit is that it maps the flow of personal data into and out of school and can be used to measure the degree to which we comply with the law and identify "red flags" which require urgent attention.

Data Protection Policy Reviews: The GDPR will require all schools to review their policies, particularly those relating to data protection. Data protection policies for pupils and parents are used to explain an individual's legal rights and how those rights can be exercised. As the GDPR amends those rights, our policies will also have to be amended. Any policies also intended to be read by children will have to be explained in clear non – technical language and in a way that can be readily understood by the intended audience.

Appointment of a Data Protection Officer (DPO): Due to the significant new burdens imposed on data controllers by GDPR, it is recommend that all schools now formally appoint a DPO because of the demands of the existing Data Protection Act. Under GDPR, certain data controllers and data processors MUST appoint a DPO. These include:

- Public authorities (with some minor exceptions) – this means that all maintained schools and academies will have to mandatorily designate a DPO;
- Any organization whose core activities require *"regular and systematic monitoring"* of data subjects on a *"large scale"*; or *"large scale*" processing of personal data or criminal records.

Where a DPO must be appointed the following requirements apply:

- The DPO should be an expert in their field *and* have specific knowledge of their sector. The employer must help them maintain this knowledge e.g. by making provision for specific training.
- The DPO's tasks should as a minimum include: advising colleagues and monitoring the school's compliance including via staff training and awareness raising; advising on PIAs; being the point of contact for supervisory authorities; developing policies and procedures; watching out for publication of relevant guidance and Codes of Practice; monitoring the documentation, notification and communication of data breaches.
- A DPO can be an employee or a hired contractor.
- DPO's must be able to work "independently of instruction" and not dismissed or penalized simply for doing their job. They should report to the highest level of management. This requirement will have interesting implications from a HR perspective.
- The DPO's contact details must be published and registered with the supervisory authority. They will be the point of contact for compliance matters.

Staff Data Protection Training: Schools will continue to be subject to an obligation to take organizational steps to keep personal data secure and the deployment of staff data protection training will continue to be expected. New starters will be expected to receive data protection training before they have access to personal data and existing staff should receive regular and refresher training.

Communicating Data Protection/Privacy Information: GDPR requires us to provide much more meaningful information to individuals about how we use our data. Under the current DPA, we are already legally required to provide certain minimum information to individuals (including staff, pupils and parents) about how our personal data is processed.

Under GDPR, the list of information which has to be provided to individuals will increase significantly. Some of the information has to be communicated in all cases (mandatory Privacy Notice information) whilst a second subset of information need only be provided in specific cases e.g. if the school intends to process the personal data for further different purposes than those that existed at the time of collection. Notwithstanding the sheer volume of information that now needs to be included in our Privacy Notice, we will be expected to provide this in a concise, transparent, intelligible and easily accessible way. Here is some of the information we will be expected to provide:

- Our Identity and contact details
- The Purpose of processing data and the legal basis for the processing of that data. (This later requirement is new and will require significant thought in some cases.)
- Who we share the personal data with
- Transfers outside EU and how data is protected
- Retention period or criteria used to set this
- Tell individuals' *all* their legal rights e.g. the right to withdraw their consent to their data being used for marketing or for school fundraising
- Right to complain

We have reviewed our existing Privacy Notices and updated them so they comply with the GDPR.

Legal Grounds for Processing Personal Data: GDPR sets out conditions (or Grounds) that must be met for the processing of personal data to be lawful. These grounds broadly replicate those in the current DPA. For example, personal data may be processed with consent or where the processing is necessary for a contract or where the processing is necessary for compliance with a legal obligation.

Most organizations, including schools, may not have had cause to think about their legal basis for processing personal data before. This is largely because under the current DPA there are very few circumstances where this is relevant. However, under the GDPR schools need to be aware of their legal grounds for processing personal data and in some cases explain it to our pupils and parents. For example, it is likely that our legal ground for processing pupil images for identification purposes will be because the processing is necessary for the contract. In contrast, the legal ground for using pupil images for school marketing and on the school website is likely to be consent. Schools are now required to explain our legal grounds for processing personal data in our Privacy Notice and when answering a Subject Access Request. This is new. In addition, under the GDPR, some individuals' rights are modified depending on our legal basis for processing their personal data. For example, individuals will have a stronger right to have their data deleted where we use consent as our legal basis for processing.

Consent: We needed to review how we seek and record consent for the processing of personal data and consider if any changes were required under the GDPR. Just as with the current DPA, we can still rely on "consent" as a legal ground to process personal data e.g. to use pupil images on the website, to send fundraising and marketing messages to parents or to publish pupil news on social networking platforms. However, satisfying the criteria for valid legal consent is harder under GDPR.

Under GDPR, consent of a data subject means ***any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to personal data relating to him or her being processed.***

Freely given: The consent must be freely given and capable of being withdrawn at any time. It must be as easy for an individual to withdraw their consent as it was to provide it in the first place.
Where the performance of the Parent Contract is made conditional on consent to the processing of personal data that is not necessary for the performance of that contract, this is likely to result in consent not being freely given.

Specific: Separate consents must be obtained for different processing operations. It must be distinguishable from other matters and not "buried" in wider written agreements. Under GDPR there is a presumption that consents should be separable from other written agreements.

Fully informed: We should clearly explain to individuals what they are consenting to and of their right to withdraw consent.

Consent must be unambiguous and be a positive indication of agreement: It cannot be inferred from silence, inactivity or pre-ticked boxes.

Individuals' Rights: The legal rights that individuals have under GDPR are very similar to those they currently enjoy under the DPA. However, there are some significant enhancements and amendments which we need to be aware of.

The main legal rights under the GDPR include:

- The right of subject access (see below)
- To have inaccuracies corrected
- To have information erased (the so called "right to be forgotten")
- To prevent direct marketing (i.e. where marketing is directed to specific individuals)

- To prevent automated decision-making and profiling, and
- Data portability (This is a new enhancement to the right of subject access. In brief schools will have to provide requested information electronically and in a commonly used machine readable format)

Right of Subject Access: As under current data protection law, the GDPR will continue to allow individuals to ask school to give them a copy of their personal data together with other information about how it's being processed by school. (This is known as a Subject Access Request or SAR for short). However, under GDPR the rules for handling SARs has changed and has updated our procedures accordingly.

Under GDPR, the main changes are:

- Now free in most (but not all) cases (used to be £10)
- Manifestly unfounded or excessive requests can now be charged for or refused
- Deadline reduced from 40 calendar days to "within 1 month". This deadline can be extended in certain cases.
- Additional information to be supplied e.g. school data retention periods and the right to have inaccurate data corrected.
- If we want to refuse a SAR, we will need to have policies and procedures in place to demonstrate why refusal of a request meets these criteria.

Personal Data Breaches: All schools have to adopt internal procedures for detecting, reporting and investigating a personal data breach. The reason for this is that the GDPR introduces mandatory breach notification to the Data Protection Authority (the ICO) and in some cases also to affected individuals. Only those breaches which are likely to result in an individual suffering damage will need to be reported e.g. breaches that could result in identity theft or where an individual's confidentiality has been breached. However, even though not all breaches will be subject to mandatory notification, we will still be under an obligation to have systems in place to detect and investigate all breaches. We should also maintain an internal breach register. If we detected a breach which is subject to the mandatory reporting rules then we must report the breach to the supervisory authority without "undue delay" and not later than 72 hours after becoming aware of it. This in itself could pose significant challenges given that it can take organizations several hours or even days to identify where the breach took place, which individuals have been affected and the data that has been compromised. Where a breach has to be reported to affected individuals this will have to be done without "undue delay".

Non-compliance can lead to administrative fines* of up to €10,000,000 or in the case of an undertaking, up to 2% of the total worldwide annual turnover or the preceding financial year, whichever is higher.

Children: The GDPR identifies children as "vulnerable individuals" deserving of "special protection". To that end, we need to be aware that the new rules introduce some child-specific provisions, most notably in the context of legal notices and the legal grounds for processing children's data. The GDPR do not prescribe the age at which a person is a child and in this context, all schools will need to address the new requirements when writing notices aimed at teenagers and young adults. In any event, any legal notice addressed to a child (whether relating to online or off line services) must be child-friendly.

The main provision in respect of children is that where information society services are offered directly to a child and the legal ground for processing personal data is consent, then parental consent will be required for children aged under 16. Ultimately though, under 13's can never themselves consent to the processing of their personal data in relation to online services. This rule is subject to certain exceptions such as counselling services.

The school as data controller would also be required to make reasonable efforts to verify that consent had been provided. Offline processing of personal data will continue to be subject to the usual Member State rules on capacity to consent.