JMB Information note on the GDPR
Part One and Activity One

Becoming Accountable

1st May 2018

Why is data protection compliance so important for Schools?

At present, the data protection regime in Ireland is governed by the Data Protection Act 1988 and the Data Protection (Amendment) Act 2003 together with the numerous Statutory Instruments amending or extending same (collectively referred to herein as the "**Data Protection Acts 1988 and 2003**"). The Data Protection Acts 1988 and 2003 were based on EU Directive 95/46/EC.

Schools are already familiar with their legal obligations under the Data Protection Acts 1988 and 2003. The Data Protection Acts 1988 and 2003 established that there was a clear legal duty of care which every data controller owed to data subjects in respect of the collection of their personal data.

The General Data Protection Regulation

Just as the Data Protection Acts 1988 and 2003 applied to all organisations processing personal data (whether "for profit" or not), similarly the GDPR applies to all organisations processing the personal data of natural persons. GDPR will introduce changes for the way organisations collect and handle personal data. Many aspects of data protection will remain familiar, but there are significant enhancements to certain areas

Until 25th May 2018, the Data Protection Acts 1988 and 2003 apply. After 25th May 2018, GDPR applies together with whatever national implementing legislation has been enacted.

While building on familiar principles within the existing legislation, GDPR will bring new challenges our schools.

It is important for every School to understand that the law of data protection is ever-evolving, and that the School needs to keep its policies, procedures, workplace practices, training modules, contracts, and culture, under continual review to take account of the changes.

Full text of the GDPR:.
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

Roles and responsibilities

The School management team and the Board of Management have a key role in driving data protection awareness and compliance throughout the School. Their role is to build appropriate data protection policies and procedures appropriate to the School, and to review the implementation, effectiveness, and compliance with same in the School. As well as regular training for all staff, there also needs to be systematic, random inspection to ensure that members and staff are adhering to the approved protocols. Even when robust systems have been put in place, they need to be monitored and audited regularly to ensure compliance.

Everyone in the School has a role to play in ensuring people's privacy is respected. Everyone should receive data protection training appropriate to their role. In most cases, very basic (but very serious) data protection mistakes arise because of inattention, human error or a genuine misunderstanding of what the person was supposed to do. It is therefore very important that everyone involved in the School's undertaking understands the role which they play in protecting privacy.

All staff, including teaching staff, SNAs etc. must comply with the School's data protection policy, procedures and approved practices. The whole School culture should be respectful of privacy, and imbued with the principles of ethical information governance. Compliance should be audited periodically by the management team (Principal, Deputy Principal(s), Year Heads etc) to identify areas of risk and or vulnerabilities where further training is required. All members and staff must adhere to high ethical standards when handling people's data.

My school and <u>the current</u> Data Protection Acts 1988 and 2003

Schools are already familiar with their legal obligations under the Data Protection Acts 1988 and 2003.

Some of the main rules setting out the requirements for fair processing of personal data are set out in section 2 of the Data Protection Acts.

They can be summarised as follows:

- Obtain and process the information fairly;
- Keep it only for one or more specified, explicit and lawful purposes;
- Process it only in ways compatible with the purposes for which it was given to you initially;
- Keep it safe and secure;
- Keep it accurate, complete and up-to-date;
- Ensure that it is adequate, relevant and not excessive;
- Retain it no longer than is necessary for the specified purpose or purposes; and
- Give a copy of his/her personal data to any individual, upon request.

Now let's look at the changes!

What is going to change with the introduction of the European General Data Protection Regulation ("GDPR")?

While GDPR introduces significant changes to data protection law, it builds on many of the established concepts set out in the Data Protection Acts 1988 and 2003.

So many of the provisions should look and feel familiar to Schools who are already complying with the pre-existing law.

There are certain privacy enhancements introduced by GDPR, specifically greater rights for data subjects. Some examples include (but are not limited to):

- shifting the onus onto the organisation to "demonstrate compliance";
- greater emphasis on the principles of transparency and accountability;
- enhanced data subject rights (access, right to be forgotten, right to object, etc) and shortened time-frames within which to deal with these requests;
- extensive record keeping obligations (Article 30);
- the legal requirement to appoint a mandatory Data Protection Officer ("**DPO**") in certain circumstances;
- a requirement to conduct data protection impact assessments ("**DPIAs**") for certain types of data processing;
- a requirement to adopt internal policies and implement measures which meet the principles of "privacy by design"/"privacy by default";
- mandatory notification of certain data breaches to the DPC within 72 hours (in certain situations), and mandatory notification of certain data breaches to the affected data subjects;
- enhanced requirements in relation to "consent" (and in certain circumstances, data controllers may no longer be entitled to rely on "consent" as a lawful basis for the processing of personal data – discussed further in this paper);
- the right for an individual to seek compensation (judicial remedy) for material or non-material damage; and
- increased financial penalties and fines for non-compliance.

Where can I access the European General Data Protection Regulation?
https://www.dataprotection.ie/docimages/documents/The%20GDPR%20and%20You.pdf

Is there a quick access link to the Articles?
https://gdpr-info.eu/

Understanding Key Terms

A **data controller** is the body (or natural or legal person) who alone or jointly with others determines the purposes and means of the processing of personal data. For example, in a Schools context, the data controller in a School is **not** the Principal!! The School is managed by its Board of Management, and the Board of Management determines the purposes and means of processing the personal data.

Occasionally, a data controller will contract with another organisation to process data on its behalf and at its direction (a "**data processor**"). In a Schools context, this may be the School's cloud-based administrative software (VSware, Aladdin, Advance, etc), it may be third parties retained to undertake certain actions (payment solutions for receipt of school fees and money for school trips, bookkeeping, payroll, HR, IT technical support, shredding companies, etc).

"**Personal Data"** is any information relating to an identified natural person, or identifiable natural person who can be identified by reference to their "name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

There are so-called "**special categories**" of personal data (previously part of the "sensitive personal data" category), which refers to personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Significantly more rigorous requirements apply to the fair processing of such special category personal data.

The living natural person to whom the personal data relate is a "**data subject**".

"Processing" means doing anything with the data, including "collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction". It is difficult to conceive of anything that could be done to personal data that could fall outside this definition.

For further details please see **Article 4: Definitions**.

What are the new GDPR Principles relating to the processing of personal data?

Article 5 of GDPR sets out the principles relating to the processing of personal data, many of which will be familiar to schools from the Data Protection Acts 1988 and 2003.

Lawfulness, fairness, transparency: Article 5(1)(a) of GDPR sets out the principles that must be adhered to when processing personal data. It provides that personal data shall be "*processed lawfully, fairly and in a transparent manner in relation to the data subject*". Schools will already be familiar with this legal requirement, as there is a similar legal requirement already in existence under the existing laws: section 2(1)(a) DPA 1988 and 2003.

Purpose Limitation: Article 5(1)(b) of GPD requires personal data to be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes. Any school already complying with existing laws (and in particular section 2(1)(c)(i) and (ii) DPA 1988 and 2003) should be in a good position to demonstrate it is complying with this principle.

Data Minimisation: Article 5(1)(c) requires that the data be adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed. This will be familiar to schools, who are already bound by the existing legal provision: Section 2(1)(c)(iii) data shall be "*adequate, relevant and not excessive in relation to the purpose or purposes for which they were collected or are further processed*". This principle should serve as an important reminder to Schools of the importance of collecting only that data they absolutely require to deliver education, and to ensure they only collect same at the correct time.

Accuracy: Article 5(1)(d) requires that the data be accurate and kept up to date. Furthermore, it requires that every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay. This is similar to the existing legal requirement in section 2(1)(b) that the data be accurate, complete, and kept up to date.

Retention/storage limitation: Article 5(1)(e) requires that the data be kept in a form which permits identification of data subjects for no longer than is necessary. This is similar to the existing legal provision in section 2(1)(c)(iv) requiring data not to be kept "*for longer than is necessary for that purpose or those purposes*".

Integrity, confidentiality (security): Article 5(1)(f) requires that the data be processed in a manner than "*ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against unlawful loss, destruction or damage, using appropriate technical or organisational measures*". Organisations processing people's data are required to ensure that the data are kept safe and secure. Article 5(1)(f) is similar to and is in-keeping with the pre-existing legal obligations set out in the Data Protection Acts 1988 and 2003, specifically Section 2(1)(d) and Section 2C(1).

What is meant by the lawful basis for processing?

Article 6 sets out the grounds for lawful processing of personal data ("lawful basis").

Schools process personal data on a variety of lawful bases. Under the Data Protection Acts 1988 and 2003, it has always been important for Schools to understand the lawful bases upon which they are relying for each processing operation. The importance of understanding the organisation's lawful bases for processing becomes even more critical under GDPR.

Schools are required to explicitly inform data subjects what lawful basis is being relied upon for each data processing operation as part of the transparency requirements (see Article 13(1)(c) which provides that the data controller must inform the data subject of "*the purposes of the processing for which the personal data are intended as well as the legal basis for the processing*").

Please note that separate rules apply to processing special categories of personal data (Articles 9 and 10), and the list below deals only with processing of personal data (Article 6):

Article 6(1)(a): the data subject has given consent to the processing.
In certain limited circumstances, Schools might process some limited personal data on the basis of a person's consent. Under the GDPR, in order to provide a lawful basis for processing, the consent of a data subject must be: a) freely given: b) specific; c) informed: and d) an unambiguous indication of the data subject's wishes by a statement or clear affirmative action – evidence of consent. In order for consent to be valid, four additional criteria must be complied with: a) onus of proof; b) independent consent clauses; c) right of withdrawal.

Article 6(1)(b): the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

Article 6(1)(c): the processing is necessary for compliance with a legal obligation to which the controller is subject.

Article 6(1)(d): the processing is necessary in order to protect the vital interests of the data subject or of another natural person; Recital 46 of GDPR provides that processing on the lawful basis of "vital interests" should "*in principle take place only where the processing cannot be manifestly based on another legal basis*". The recital goes on to state that "*some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters*".

Article 6(1)(e): the processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller. Example: where a School is legally obliged to perform a function conferred on it by or under an enactment, or other function of a public nature performed in the public interest, this may constitute a lawful basis, so long as it is strictly necessary.

Article 6(1)(f): the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection

of personal data, in particular where the data subject is a child. Under the existing Data Protection Acts 1988 and 2003, a School was permitted to process personal data on the basis of "legitimate interests" (ie the legitimate interests of the School, except where the processing was unwarranted in any particular case by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject). However, GDPR **withdraws** the availability of "legitimate interests" as a lawful basis for **public authorities** in the performance of their tasks.

Special categories of processing – Article 9 and Article 10
The list above sets out lawful basis for processing relates to personal data only (excluding sensitive personal data). When considering the lawful basis for processing special categories of personal data (*what was previously called "sensitive personal data under the Data Protection Acts 1988 and 2003,* a School must analyse **Articles 9 and 10** to ascertain the appropriate lawful basis.

Special categories of processing (processing of medical information, or information relating to race, religion, political beliefs, etc.), receive an additional level of protection under the GDPR. Such processing must be justifiable with reference to at least one condition from Article 9 of the Regulation – if this cannot be done, then the organisation should not be processing such information. For example, when processing these special categories of personal data, the consent of the Data Subject needs to be explicit and cannot be implied or assumed.

Understanding "Consent" Article 6(1)(a):

As stated above under **Article 6(1)(a),** consent is one possible lawful basis for the processing of personal data. However, the general view is that consent should only be utilised where it is absolutely appropriate, and where there is no other legal ground for the processing.

It has always been the case that data protection bodies have cautioned organisations from relying on consent where there was an imbalance of power between the data controller and the data subject. GDPR solidifies this position. There may be a small number of areas where "Consent" will be used as a lawful basis for processing within a School. It is advised that "Consent" be reserved for processing operations that are truly optional in terms of the student's core educational experience (eg. photos on the school website, entering a prize-draw, direct marketing/fundraising, etc). For all other educational data processing operations there is generally another more appropriate lawful basis, eg: contract, legal obligation, vital interests, public interest etc. However, it is important to fully understand "Consent" and how it will operate in GDPR.

In the case of GDPR, "*Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement",* and furthermore: *"Silence, pre-ticked boxes or inactivity should not therefore constitute consent*". So it is abundantly clear that where an organisation is relying on "Consent" for any form of processing, that Consent must be informed, freely given, capable of being withdrawn without detriment. The individual must be given a genuine choice in the matter.

Schools must analyse what processing operations take place on the basis of Consent, and processing proceeds in reliance on another lawful basis. It would be completely inappropriate and legally incorrect to purport to gather "Consent" for certain processing operations where Consent is not the lawful basis.

What is meant by the Digital Age of Consent?

Article 8 establishes a "Digital Age of Consent" in respect of children engaging with information society services. It must be noted that this digital age of consent reference relates to children's engagement with information society services **only**. For the avoidance of any doubt, Article 8's Digital Age of Consent **does not have any wider application beyond information society services**.

Activity One: Becoming Accountable - Carry out a Data Audit

Carrying out a data audit is a good starting point for getting started and being prepared for the GDPR. This is a manageable task and is the first of many activities the school will engage in an evolving landscape with respect to the GDPR.

Going Forward

The JMB will continue to expand on the GDPR principles and articles in forthcoming information notes so as to capture what our schools need to do in an evolving manner.

John Curtis,
General Secretary, JMB

Issue date: 1st May 2018

Activity One: Becoming Accountable – Carry out a Data Audit

Schools will already be familiar with the fairly obtaining data principle. This data protection principle applies to your school when the school initially gathered any personal data.

You are required to notify your school community, i.e parents, students, employees, BOM members - of your identity, your reasons for gathering the data, the use(s) it will be put to, who it will be disclosed to, and if it's going to be transferred outside the EU.

Under the GDPR, we see the introduction of an 'accountability principle'. This requires a school to demonstrate compliance with the GDPR by being accountable for the personal data it collects.

Article 30 https://gdpr-info.eu/art-30-gdpr/ sets out the processing activities of a data controller. Applying Article 30 to your school's processing activities will allow you to account for all the data your school processes.

Accountability can be achieved by creating an inventory of all the personal data your school holds by asking, for example, the following questions:

- Why are we holding data on students, parents, employees, past pupils?
- How did we obtain the data?
- Why was it originally gathered?
- Where is the data kept?
- Who has access to it?
- How long will we or do we retain the data?
- How secure is it, both in terms of encryption and accessibility?
- Do we ever share the data with third parties and on what basis might we do so?

Engaging in this exercise will allow your school to demonstrate and document the ways in which it complies with the current data protection principles and is future proofing against the GDPR. The following link might be of help: http://dataprotectionschools.ie/en/GDPR/

Other ways of describing this inventory exercise is to map out all the personal data you hold or to carry out an internal audit of the personal data so that you have a data audit trail.

By carrying out this obligation, your school will be able to amend incorrect data or respond quickly to a data subject access request as you will have a complete picture of the personal data you hold.

Another benefit of this inventory is that it might show up gaps in compliance or it might highlight data which needs greater levels of security and is at high risk if it were lost.

The key objective is that your school can demonstrate it carried out an inventory of the personal data it holds. The exercise also builds into developing or amending your Data Protection Policy.

Quick access links to the Articles: https://gdpr-info.eu/