Preparing for GDPR

The 12 steps to be taken:

1. Awareness
2. Information you hold
3. Communicate privacy information
4. Individuals rights
5. Subject Access Requests
6. Lawful basis for processing personal data
7. Consent
8. Children
9. Data Breaches
10. Privacy by design and Data Protection Impact Assessments (DPIA)
11. Data protection officers
12. International

1. ***Awareness***

You should make sure that decision makers and key people in your school/ETB are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have and identify areas that could cause compliance problems under the GDPR. It would be useful to start by looking at the schools/ETBs risk register, if one exists. You may find compliance difficult if you leave your preparations until the last minute.

2. ***Information you hold***

Schools/ETB's should document what personal data is held, where it came from and with whom it is shared. Schools/ETBs may need to organise an information audit. The GDPR requires Schools/ETBs to maintain records of their processing activities. It updates rights for a networked world. For example, if Schools/ETBs have inaccurate personal data and have shared this with another organisation, they will need to inform the other organisation about the inaccuracy so it can correct its own records. Schools/ETBs won't be able to do this unless they know what personal data is held, where it came from and who you share it with. You should document this. Doing this will also help you to comply with the GDPR's accountability principle, which requires organisations to be able to show how they comply with the data protection principles, for example by having effective policies and procedures in place.

3. Communicate privacy information

Schools/ETBs should review their current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation. When schools/ETB's collect personal data they currently need to give people certain information, such as their identity and how they intend to use their information. This is usually done through a privacy notice. Under the GDPR there are some additional things schools/ETBs will be required to communicate to people; for example, they will need to explain their lawful basis for processing their data, data retention periods and that individuals have a right to complain if they think there is a problem with the way schools/ETBs are handling their data. The GDPR requires the information to be provided in concise, easy to understand and clear language.

4. Individual's rights include:

- the right to be informed;

- the right of access;
- the right to rectification;
- the right to be forgotten;
- the right to restrict processing;
- the right to data portability;
- the right to compensation & liability

Right to be Informed

The right to be informed encompasses a schools/ETBs obligation to provide 'fair processing information', typically through a privacy notice. It emphasises the need for transparency over how they use personal data.
The GDPR sets out the information that schools/ETBs should supply and when individuals should be informed. The information schools/ETBs supply is determined by whether or not they obtained the personal data directly from individuals.
Much of the information schools/ETBs should supply is consistent with current obligations under the DPA, but there is some further information they are explicitly required to provide.
The information supplied about the processing of personal data must be:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

Right to Access

Part of the expanded rights of data subjects outlined by the GDPR is the right for data subjects to obtain from the school/ETB confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the school/ETB shall provide a copy of the personal data, free of charge, in an electronic format.
Under the GDPR, individuals will have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice)

Right to Rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.
If a school/ETB has disclosed personal data to third parties, you must inform them of the rectification where possible. You must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.

Right to be Forgotten

Also known as Data Erasure, the right to be forgotten entitles the data subject to have the school/ETB erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure include the data no longer being relevant to original purposes for processing, or a data subjects withdrawing consent.
It should also be noted that this right requires schools/ETBs to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests.

If an individual contacts your school/ETB and requests that their data be removed from its databases, it will be obliged to do so, unless it has a legitimate reason to retain the data.

Right to Restrict Processing

In some situations, this right gives an individual an alternative to requiring data to be erased; in others, it allows the individual to require data to be held in limbo whilst other challenges are resolved.
If personal data are 'restricted', then a school/ETB may only store the data. It may not further process the data unless:
• the individual consents; or
• the processing is necessary for establishment etc. of legal claims; for the protection of the rights of another natural or legal person; or for reasons of important (Union or Member State) public interest.
Where the data are processed automatically, then the restriction should be effected by technical means and noted in the controller's IT systems. This could mean moving the data to a separate system; temporarily blocking the data on a website or otherwise making the data unavailable.
If the data have been disclosed to others, then the controller must notify those recipients about the restricted processing (unless this is impossible or involves disproportionate effort).
The controller must notify the individual before lifting a restriction.

Right to Data Portability

GDPR introduces data portability - the right for a data subject to receive the personal data concerning them, which they have previously provided, in a 'commonly use and machine readable format' and have the right to transmit that data to another controller. It allows data subjects to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.
The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.
It applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means

Right to Compensation & Liability

Data subjects can sue both controllers and processors for compensation for pecuniary or non-pecuniary damage (e.g. damages for distress) suffered as a result of a breach of the GDPR. Data subjects will have a right to recover material and/or non-material damages including loss of control over personal data or limitation of rights, discrimination, financial loss, damage to reputation, loss of confidentiality of personal data protected by professional secrecy and "other significant economic or social disadvantage." Data subjects can choose to sue both the controller and the processor, with the introduction of joint and several liabilities between parties engaged in the same data processing.

5. *Access Requests*

A 'subject access request' can be considered a data subject seeking information as to whether or not information concerning the subject is being processed, and usually, access to such data.

The GDPR requires the provision of specific, additional information to data subjects when responding to access requests.
The time period for dealing with requests is one month. The ability to charge a fee has also been removed. However, the school/ETB may charge a reasonable fee for any further copies requested by the data subject, or where access requests are manifestly unfounded or excessive, taking into account the administrative costs of providing the information.
The GDPR says that the information you provide to people about how you process their personal data must be:

- concise, transparent, intelligible and easily accessible
- written in clear and plain language, particularly is addressed to a child, and
- free of charge

6. Lawful basis for processing personal data

For processing to be lawful under the GDPR, schools/ETBs need to identify (and document) their lawful basis for the processing. There are six lawful bases listed in Article 6:

6(1)(a) – Consent of the data subject
6(1)(b) – Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
6(1)(c) – Processing is necessary for compliance with a legal obligation
6(1)(d) – Processing is necessary to protect the vital interests of a data subject or another person
6(1)(e) – 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
6(1) (f) – Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

In the absence of a lawful reason to process personal data, that personal data must not be processed.
Data must be collected lawfully, fairly and transparently.
It must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
It needs to be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
It must be accurate, and where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate; having regard to the purposes for which they are processed, are erased or rectified without delay.
Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using inappropriate technical or organisational measures.

7. Consent

Consent must be freely given, specific, informed and unambiguous. Requests for consent should be separate from other terms, and be in clear and plain language.
A data subjects consent to processing of their personal data must be as easy to withdraw as to give. Consent must be "explicit" for sensitive data. The school/ETB is required to be able to demonstrate that consent was given. Existing consents may still work, but only provided they meet the new conditions.
Under the GDPR, additional information must be communicated to individuals in advance of processing, such as the legal basis for processing the data, retention periods, the right of complaint where data subjects are unhappy with the implementation of any of these criteria, whether their data will be subject to automated decision making and their individual rights under

the GDPR. The GDPR also requires that the information be provided in concise, easy to understand and clear language.
Consent requires some form of clear affirmative action. Silence or pre-ticked boxes will no longer be sufficient to constitute consent.
The GDPR permits data subjects to withdraw their consent at any time.
A record must be kept of how and when consent was given.

Where a data controller collects personal data for one specific purpose, the GDPR requires that data subjects give additional consent for each additional processing operation.
People will have a stronger right to have their data deleted where you use consent as your lawful basis for processing.
The GDPR requires the provision of specific, additional, information to data subjects when responding to access requests.
The timeframe for dealing with requests has been reduced from 40 days to one month.
The ability to charge a fee has also been removed. However, the controller may charge a reasonable fee for any further copies requested by the data subject, or where access requests are manifestly unfounded or excessive, taking into account the administrative costs of providing the information.

8. Processing children's data
The GDRP identifies children are identified as vulnerable natural persons, deserving of specific protection.
Processing of data relating to children is noted to carry certain risks, and further restrictions may be imposed as a result of codes of conduct.
Many of the main concepts and principles of GDPR are much the same as those in our current Data Protection Acts 1988 and 2003 (the Acts) so if a school is compliant under current law, then much of this approach should remain valid under the GDPR.
The explicit emphasis on adapting privacy notices for children goes beyond what is currently required by the DPA's. Data controllers processing children's data will need to take account of the level of comprehension of the age groups involved and tailor their notices accordingly.
What about Data Subjects under the age of 16?
Children under the age of consent can never, themselves, give consent to the processing of their personal data in relation to online services. The GDPR does not prescribe the age at which a person is considered to be a child.
Parental consent is necessary to the processing of a child's data, where the child is below the age of 16 years old. Ireland may choose to lower this age but not below 13 years old.
Parental consent will always expire when the child reaches the age at which they can consent for themselves. Schools/ETBs need therefore to review and refresh children's consent at appropriate milestones.

9. *Data Breaches*
A data breach occurs where the security or integrity of personal data is compromise. This can occur through misappropriation; loss or theft of data or equipment; unauthorised individuals gaining access; a deliberate attack on systems; equipment failure; human error of malicious acts such as hacking, viruses or deception.
Under the GDPR, breach notification will become mandatory in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals". This must be done within 72 hours of first having become aware of the breach. Schools/ETBs are required to justify any delays to the ODPC by way of reasoned justification. Data processors will also be required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach.

Controllers will also have to notify data subjects where the breach is likely to result in a 'high risk' to them. 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 transmitted, stored or otherwise processed".
Schools/ETBs also need to document any data breaches, comprising the facts relating to the personal data breach.

10. Privacy by Design

The GDPR places onerous accountability obligations on data controllers to demonstrate compliance. This includes requiring them to:
(i) maintain certain documentation,
(ii) conduct a data protection impact assessment for more risky processing (DPAs may compile lists of what is caught), and
(iii) implement data protection by design and by default, e.g. data minimisation.
Privacy by design as a concept has existed for years now, but it is only just becoming part of a legal requirement with the GDPR. At its core, privacy by design calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition. More specifically - 'The controller shall..implement appropriate technical and organisational measures..in an effective way.. in order to meet the requirements of this Regulation and protect the rights of data subjects'. *Article 23* calls for controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimisation), as well as limiting the access to personal data to those needing to act out the processing. Data protection safeguards must be taken into account at the planning stages when companies re designing products or services.
'Privacy by design' means that, by default, only such personal data as is necessary for the identified purposes should be processed. Organisations should, therefore, seek to collect and retain the minimum amount of data they need for the minimum amount of time, and limit data sharing to that which is necessary.
Data controllers must ensure that privacy concerns are a key part of their decision making. The GDPR seeks to ensure that the privacy rights of data subjects are prioritised by data controllers when they make business decisions. Controllers will have to carry out privacy impact assessments for any actions that may pose a high risk for data subjects' privacy rights.
GDPR has introduced mandatory DPIAs (Art. 35) for the first time.
Under the Regulation, businesses will be obliged to conduct Data Protection Impact Assessments ("DPIA") where the processing, particularly where it utilises any new technologies, "is likely to result in a high risk" for the rights of individuals, having regard to the "nature, scope, context and purposes of the processing". The Regulation currently contains a non-exhaustive list of the situations in which a DPIA will be necessary, including where the data controller is monitoring publicly accessible areas or when sensitive personal data is being processed on a large scale. The principles of data protection by design and by default are also enshrined in the Regulation, whereby user settings will automatically be privacy friendly and the development of services and products will take account of privacy considerations from the outset.

What is a DPIA?

- A process to identify and reduce the privacy risks of new projects or practices
- An integral part of taking a privacy by design approach
- Difference to a privacy audit
- DPIAs are prospective, act as an early warning system, may affect the design/end result and are proactive

Objectives

- Minimizing risks

- Preventing unlawful processing
- Implementing privacy by design and by default

What triggers a DPIA?
DPIAs shall be conducted, where

- A type of processing is likely to result in a high risk to the rights and freedoms of natural persons
    - Taking into account: nature, scope, context and purposes of the processing
- Exemption in Article 35(10)

DPIAs are particularly required in the case of

- Systematic and extensive evaluation based on automated processing, including profiling, and on which decisions with legal or similar effects are based
- Processing on a large scale of sensitive data or of personal data relating to criminal convictions and offences
- Systematic monitoring of a publicly accessible area on a large scale
- Positive or negative lists by SAs

What is the content of a DPIA?
The school/ETB must assess the impact of the envisaged processing operations on the protection of personal data

- Minimum content
    - Systematic description of the processing and its purposes
        - Including, where applicable, the legitimate interest pursued by the controller

Assessment of the necessity and proportionality of the processing
Assessment of the risks to the rights and freedoms of data subjects
Consider expectations of the individuals
Evaluate the level of risk, based on likelihood, and impact
The measures envisaged to address the risks
Including safeguards, security measures and mechanisms (e.g., pseudonymisation, anonymisation, encryption, local storage, access restriction, limiting retention)
Compliance with approved codes of conduct shall be taken into account

Suggested Template for DPIAs:

Name of Project	**General name of the task process giving rise to risk**	**Specific description of the source and the exact nature of the risk**	**Potential privacy impact or damage**	**Level of risk based on the likelihood of occurrence**	**Alternative solutions and potential side-effects**

11. Data Protection Officers

Currently, controllers are required to notify their data processing activities with local DPAs, which, for multinationals, can be a bureaucratic nightmare with most Member States having different notification requirements. Under GDPR it will not be necessary to submit notifications/registrations to each local DPA of data processing activities, nor will it be a requirement to notify/obtain approval for transfers based on the Model Contract Clauses (MCCs). Instead, there will be internal record keeping requirements, and DPO appointment will be mandatory only for those controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences.
Importantly, the DPO:
Must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices
May be a staff member or an external service provider
Contact details must be provided to the relevant DPA
Must be provided with appropriate resources to carry out their tasks and maintain their expert knowledge
Must report directly to the highest level of management
Must not carry out any other tasks that could results in a conflict of interest.
DPO's need to be designated by:

- All public bodies (apart from courts acting in their judicial capacity)
- Where the 'core activities' of the data controller or data processor require "regular and systematic monitoring" of individuals "on a large scale", or
- Where the 'core activities' of the controller or processor consist in processing 'on a large scale' sensitive personal data (newly defined) or data relating to criminal convictions and offenses.

Does my school/ETB need to appoint a Data Protection Officer (DPO)?
DPOs must be appointed in the case of: (a) public authorities, (b) organizations that engage in large scale systematic monitoring, or (c) organizations that engage in large scale processing of sensitive personal data (Art. 37). If your organization doesn't fall into one of these categories, then you do not need to appoint a DPO.

12. International

The GDPR not only applies to organisations located within the EU but it will also apply to organisations located outside of the EU if they offer goods or services to, or monitor the behaviour of, EU data subjects. It applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location.
Increased Territorial Scope (extra-territorial applicability)
Arguably the biggest change to the regulatory landscape of data privacy comes with the extended jurisdiction of the GDPR, as it applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company's location. Previously, territorial applicability of the directive was ambiguous and referred to data process 'in context of an establishment'. This topic has arisen in a number of high profile court cases. GPDR makes its applicability very clear - it will apply to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not. The GDPR will also apply to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of

behaviour that takes place within the EU. Non-Eu businesses processing the data of EU citizens will also have to appoint a representative in the EU.