Guidance Note: General Data Protection Regulation

Introduction

The General Data Protection Regulation ("GDPR") came into force on 25 May 2018. It is advisable for schools to achieve a good level of compliance by the end of this academic year and to be able to evidence a culture change relatively soon after that. More information is set out below.

As education settings we deal with personal data all the time and will therefore be affected by the introduction of the GDPR and the legal requirements it brings. The purpose of this note is to provide you with some initial information about the GDPR, what it means for your school and what steps you need to take and when.

What does GDPR cover?

In general terms the GDPR covers the requirements for processing personal data. This was until recently regulated by the Data Protection Act 1998 ("DPA"). The GDPR was introduced by the EU to "harmonise" individuals' rights in the processing of personal data and to ensure its free flow between Member States. The main concepts and principles remain the same, but the GDPR introduces new elements that enhance the provisions under the current DPA.

Important definitions:

Personal Data has been defined as "any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific

This *Guidance Note: General Data Protection Regulation* was prepared by Browne Jacobson in collaberation with the CES, published May 2018.

to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;"

Special category data - There is a subset of personal data referred to as ***Special Categories of Personal Data*** and this includes:

- 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 person's sex life or sexual orientation

Processing is defined as "any operation or set of operations which is performed on personal data … whether or not by automated means, such as 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;". This means anything you do with the data including deleting or archiving constitutes processing it.

Data Protection Principles under the GDPR

When processing data you need to ensure that you comply with the six Data Protection Principles which require:

(a) Data to be processed lawfully, fairly and in a transparent manner;

(b) Data to be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

(c) Processing of data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

(d) Data to be accurate and, where necessary, kept up to date; inaccurate data should be erased or rectified without delay;

(e) Data to 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;

(f) Data to be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Processing under the GDPR

The first Data Protection Principle requires that the data is to be processed lawfully. For **personal data** to be processed lawfully by schools, one of the conditions below needs to be satisfied:

6(1)(a) – Consent of the data subject (must be clear affirmation) (Article 7 and 8)

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 (this condition does not apply to public authorities in their public functions) *

It is rare for schools to be able to rely on legitimate interest (6(1)(f)) because it is designed for use by commercial entities who cannot reply on public interest. However, there are some circumstances where schools can rely on this lawful basis, such as completing the CES census, which is an example of the Bishop exercising his canonical function in relation to place planning. In relation to the CES census and a limited range of other circumstances, 'legitimate interest' can therefore be relied upon.

Consent and age of consent (6(1)(a))

Consent as a condition for processing should be the last basis a school relies on as individuals can withdraw consent just as easily as they provide it. Organisations, including schools, can no longer rely on "opt out" consent – this option is no longer legal under GDPR.

Schools must now be able to evidence that consent was freely given, specific, informed and unambiguous and a positive affirmation of the individual's agreement. Whilst most of the

processing schools do will fall under other bases of legal processing, consent is still going to be required for certain processing, such as using school photos in and around the school, on the school website and social media and on the internet more broadly. Most schools will need to revisit their current approach to consent to ensure it meets the requirements of the GDPR.

The age at which children can consent to their information being processed is not set out in the GDPR. For primary schools it is straight forward – primary school children are too young to consent and so the parents or guardians will need to consent on behalf of the child.

Secondary schools need to decide how they will obtain consent from their pupils. The GDPR does not set out at what age children are able to consent. Based on current law it is advisable for schools to consider children of 12 or older able to provide consent on their own behalf. Some schools may prefer the age of 13 and this too would be acceptable. However, schools should not set the age any higher.

So, at the normal point of entry schools should seek consent form parents on behalf of pupils. Where children join the school later and are 12/13 years old, consent should be sought from the pupil.

Consent and biometric data

Consent should always be used for biometric data. If a pupil or a parent does not wish to consent, schools must offer a real alternative. As an example, if biometric data is used to support catering management and a pupil does not wish to consent, then offering a pin number instead would be a genuine alternative.

Public task (6(1)(e))

The majority of processing in schools is done under the public task condition. This condition is used when the data is being processed in order to safely and effectively run the school. Examples would include:

- Inputting and analysing data on SIMS and CPOMS systems
- Sharing data with exam boards in order to enter children for exams
- Sharing parent contact details with a third party (such as Parentmail) to facilitate efficient and effective contact with parents

Special categories of personal data

"Special category data" is personal data which the GDPR says is more sensitive, and so needs more protection in law. Special category data is:

- racial or ethnic origin,
- political opinions,
- religion or philosophical belief, 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 person's sex life or sexual orientation

To add the required additional protection, the GDPR says that in order to lawfully process special category data, we need to identify:

1. a lawful basis under Article 6 (set out above under "Processing under the GDPR"); and
2. a separate condition for processing special category data under Article 9.

There are ten conditions for processing special category data under Article 9. They are:

Article	Condition
9(2)(a)	Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law
9(2)(b)	Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement
9(2)(c)	Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
9(2)(d)	Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent
9(2)(e)	Processing relates to personal data manifestly made public by the data subject
9(2)(f)	Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
9(2)(g)	Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards
9(2)(h)	Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional
9(2)(i)	Relates to public interest in the area of public health
9(2)(j)	Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)

*****It is likely that the new Data Protection Act 2018 will introduce additional conditions and safeguards*****

So, to process special category data we need a lawful basis under Article 6 **and** a specific condition under Article 9. This is very similar to what we were used to when processing sensitive personal data under the superseded Data Protection Act 1998.

Your choice of lawful basis under Article 6 does not dictate which special category condition you must apply, and vice versa.

For example, if you use consent as your lawful basis, you are not restricted to using explicit consent for special category processing under Article 9. You should choose whichever special category condition is the most appropriate in the circumstances – although in many cases there may well be an obvious link between the two - if your lawful basis is vital interests, it is highly likely that the Article 9 condition for vital interests will also be appropriate.

School based example:

Safeguarding matters may well include relevant information about ethnicity, sex life and health. All three are special categories of data and therefore we need a lawful basis under Article 6 **and** a separate condition under Article 9 in order to lawfully process the data.

Under Article 6 we are likely to be able to rely on either 6(1)(c) – legal obligation, or 6(1)(e) – public interest task. In this case, we decide to opt for 6(1)(e).

Now we need an Article 9 condition, and we have 10 to choose from. On these facts, we could certainly rely on:

9(2)(a) – Explicit consent (assuming the individual does consent)
9(2)(g) – Substantial public interest

We only need one Article 9 condition and given that express consent could be withdrawn, it would be safer to rely on substantial public interest.

So to lawfully process this safeguarding data, we reply on Article 6(1)(e) and Article 9(2)(g).

Individual's rights under the GDPR

As a school the children, parents/carers, staff, volunteers, Governors/Trustees/Members can all request that the school complies with a request to exercise their rights, which are:

1. Right to information - Fair processing notice
2. Subject access rights
3. Right to rectification
4. Right to erasure (right to be forgotten)

5. Right to restrict processing
6. Right to data portability
7. Right to object
8. Rights in relation to automated decision making and profiling

Accordingly, the individuals mentioned above should be provided with the following, usually through a Fair Processing Notice which sets out the information to which they are entitled, including:

a) the identity and the contact details of the controller and, where applicable, of the controller's representative

b) the contact details of the Data Protection Officer

c) the purposes and legal basis for the processing of the personal data

d) the recipients or categories of recipients of the personal data, if any

e) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or where required reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

f) the rights they have including the right to make a complaint to the ICO

The information to be provided will depend on whether you obtained the personal data from the data subject or elsewhere and which of this information the individual already has in their possession.

Practical Steps Schools should be taking now to ensure compliance with GDPR

1. Ensure that your Governors and SLT are aware of the upcoming changes and legal requirements and what needs to be done
2. Review the information you hold and how and why you process (data audit)
3. Check contracts you have with third parties who will be processing data on your behalf and any data sharing contracts to ensure they are GDPR compliant
4. Review policies including privacy notices and retention and destruction policy
5. Review procedures for individual rights and Subject Access Requests

6. Review how you obtain consent from individuals including where appropriate from children
7. Review or introduce a data breach management procedure
8. Ensure that you apply Privacy by design
9. Take the opportunity to review staff practices and consider the training/re-education needs of staff
10. Appoint a Data Protection Officer (as you fall within the category of a public authority)

Timeframes

25 May 2018 is not a hard deadline; it is the date when a new regime of data protection exists and the new laws come into force. Schools should not rush to be compliant for 25 May and should instead focus on the quality and strength of compliance in a sensible time frame. We suggest the following;

By the end of this academic year:

1. Carry out your data audit so you know what information you process and why

2. Review, redraft and implement new policies, procedures and other documents to include your Data Protection Policy, CCTV policy, privacy notices, consent forms, breach procedures, subject access request procedures and template letters

3. Appoint your Data Protection Officer and ensure they receive adequate training from a reliable and knowledgeable provider

The GDPR makes no changes to the substance of your CCTV policy, but it may well require rewording to refer to the new law and to ensure the language used within it complies with the requirements of the GDPR with regards to clarity and transparency.

Within the next 6/8/10 months:

1. Focus on changing the culture of your staff and governors to ensure that they understand the importance of managing personal data correctly and identify behaviours that need to change in order to ensure GDPR compliance.

The Data Protection Officer

All schools, academies and MATs need to appoint a Data Protection Officer "DPO"). The DPO is responsible for:

- Monitoring GDPR compliance and implementation and application of data protection policies
- Informing and advising school and staff about GDPR obligations
- Advising whether and how to carry out DPIA
- Being the point of contact for the ICO
- Training staff
- Carrying out internal data audits

There are no specific credentials required, but the DPO needs to have expert knowledge of the GDPR relevant to the setting. To put that in context, the skills, experience and abilities of a DPO for a major bank will be very different from those required for a DPO of a school.

When appointing the DPO you can consider appointing someone already within your setting or organisation. If you take this approach you should ensure that they will not have any conflict with their current role and their role as DPO. The mere fact they process data will not be sufficient to mean a conflict. You will need to take account of their usual role and day to day tasks.

Most schools should be able to appoint a DPO from their existing staff and it is not envisaged that the role would be outsourced. Once appointed, the DPO will require training to ensure they have the skills and knowledge they require. A one-day Foundation Course should suffice, as long as it is delivered by a reliable and knowledgeable provider. The Archdiocese may wish to consider arranging training for the DPOs in its schools to ensure consistency and quality of training.

Application of the GDPR to Catholic Schools

To help you understand how GDPR impacts on processing data in Catholic Schools, we have set out below some examples of everyday data processing activities and the lawful bases for that processing.

Care should also be taken when explaining to parents that their child (when aged 12/13 years old) is able to provide or withhold consent. Parents may not appreciate (or indeed accept) that their child has control over those issues and may be unhappy when faced with this realisation.

Example 1 - Casework relating to pupils

A Catholic Primary School receives a complaint from a parent of a current pupil relating to alleged ongoing bullying. The allegations involve acts within and outside of school at the hands of two other pupils. The complaint is detailed and complex, setting out the alleged events and the impact the parent says those events have had on her child's health.

It is possible that this complaint also raises issues which are relevant to the Catholic character of the school and potential reputational damage to the school and wider church.

Sharing (processing)

The school requires the additional support of the Diocese to investigate and advise upon the merits of the complaint and the steps to take to manage it. To do so, the school will need to share:

- Personal data relating to the mother, child, two alleged bullies; and
- Special category data (the health impacts set out in the complaint) relating to the child

Lawful bases

For sharing the personal data, the school requires one lawful basis under Article 6. The school is sharing with the Diocese so that it can investigate an allegation relating to a child and receive advice as to next steps. Given that a school is expected to keep its pupils safe and also has a legal duty to keep pupils safe, it has a lawful basis for sharing – Public Task (6(1)(e)).

To share the special category data, an Article 6 basis is required along with an Article 9 condition. Here, the school could rely on the substantial public interest condition (9(2)(g)).

In this example, there could also be safeguarding reasons which would provide additional support for the lawful bases and the Article 9 conditions

Example 2 - Personnel issues

A member of support staff at a Catholic High School is facing a disciplinary investigation relating to a number of performance issues. The school seeks the support of the Diocese to investigate and present the school's case at the disciplinary hearing.

Sharing (processing)

The school requires the support of the Diocese to investigate the issue and present the case at the hearing. To do so, the school will need to share personal information and, if special category data is also relevant to the issue, it too will need to be shared.

Lawful bases

For sharing the personal data, the school requires one lawful basis under Article 6. The school is sharing with the Diocese so that it can investigate a disciplinary matter and present the case at a disciplinary hearing.

One of the school's tasks is to educate children. To do so it needs good staff. If staff are underperforming, which in turn could be to the detriment of the children, then the school could rely on Public Task (6(1)(e)).

If special category data is also contained within the disciplinary information to be shared, then an Article 9 condition is also required. Here, the school could rely on the substantial public interest condition (9(2)(g)) or the establishment, exercise or defence of legal claims condition (9(2)(f)).

Example 3 - Inspections

As part of its role in supporting its schools and exercising the Bishop's responsibilities (including oversight of the provision), the Diocese carries out Canonical Inspections under Canon 806 and section 46 Education Act 2005. In doing so, the Inspectors are likely to see personal data and special category data of staff and pupils.

Sharing (processing)

The school is required by law to carry out the inspections and it would not be possible for a suitable inspection to be carried out without some personal and special category data being considered as part of that inspection. The Inspectors should only have access to personal/special category data required to complete their inspection.

Lawful bases

For sharing the personal data, the school requires one lawful basis under Article 6 and an additional condition under Article 9 for special category data. Given the inspections are a legal requirement, schools can rely on compliance with a legal obligation (6(1)(c)). For an additional condition under Article 9, the school can rely on substantial public interest (9(2)(g)).

Example 4 – Catholic Certificate in Religious Studies (CCRS)

Some roles within Catholic schools require a CCRS. The Dioceses keep a central record of CCRS holders.

Storing (processing)

The CCRS central record is maintained because a CCRS is a requirement for the roles undertaken by the Certificate holders and the Diocese needs to evidence that the CCRS has been seen.

Lawful bases

The school can rely on Public Task (6(1)(e)) because the CCRS is required for those specific roles to ensure the school is employing teachers that can ensure the Catholic faith is taught to a high standard.

Example 5 – Recruitment into senior Catholic posts

Some posts such as substantive headteachers, deputy headteachers, head of RE and other posts which directly affect the Catholic mission of the school must be filled by practising Catholics. This information needs to be collected and processed in order to consider an applicant for a job/offer a job to an applicant.

Sharing (processing)

Information regarding an applicant's religion is shared with the Diocese, particularly for senior posts where a diocesan official must be present on the interview panel. Schools are required to comply with the requirements of the Bishops' Memorandum on Appointment of Teachers in Catholic Schools which includes a requirement that schools facilitate the attendance of the Diocesan Director (or his or her nominee), either by affording them advisory rights or otherwise.

Lawful bases

Personal data and special category data (religious beliefs) are being shared and so an Article 6 basis for processing is required along with an additional condition under Article 9.

Under Article 6, the school could rely on consent, given that for the individual to be considered for the role their personal data needs to be shared. However, consent should always be the last basis to rely upon because it can be withdrawn as easily as it is given (a requirement under GDPR). Therefore, an alternative basis should be considered.

The school could rely on performance of a contract (6(1)(b)) because the applicant cannot be offered the role without the personal data first being shared. This legal basis applies not only to the performance of existing contracts, but also to allow the individual to take steps to enter into a contract, as is the case here.

Under Article 9, the school could rely on explicit consent of the individual (9(2)(a)) or substantial public interest (9(2)(g)).

Example 6 – School level pupil data

The Dioceses may wish to monitor school performance to ensure appropriate standards of education are being provided in order to meet the Bishop's obligation under Canon 806 §2. The information may also be needed for the census.

Sharing (processing)

The purpose for sharing the data with the Diocese is the maintenance of education standards generally within the school (outside of the legal duty to carry out Canonical Inspections

under Canon 806 and section 48 Education Act 2005 for schools in England and section 50 for schools in Wales).

Lawful bases

To meet this purpose it may not be necessary to share personal data and where this is possible, the GDPR requires schools to avoid sharing personal data. So if the purpose – the maintenance of education standards – can be achieved without sharing personal information, then the school must avoid doing so.

If the school decides that personal information needs to be shared in order to meet the purpose, then it is most likely that the school could rely on Public Task (6)(1)(e)) because the sharing would enable the Diocese to ensure the standards of education received by the pupils is at least as outstanding as other schools in the area.

To be GDPR compliant, thought should first be given to not sharing personal information if the purpose can be achieved in another way.

Example 7 – Appointment of Foundation Governors

Dioceses appoint Foundation Governors and need to liaise with schools to ensure their appropriate placement, matching their skills with skills audits provided by the schools. The Diocese shares the personal data of the applicant with the school when the school has a vacancy on its governing body and a potential match is identified.

Sharing (processing)

The Diocese appoints the Foundations Governors and so to be considered for appointment onto a particular governing body, it is necessary to share the applicant's personal information with the school.

Lawful bases

Under Article 6, the Diocese can rely on consent (6(1)(a), given that for the individual to be considered for the role their personal data needs to be shared with the school and consent to do so will have been sought when the applicant put themselves forward.

Special category data relating to the applicant's religion will feature as part of the application and so an Article 9 condition is also required. The Diocese can rely on explicit consent of the applicant (9(2)(a)) as it's Article 9 condition.