

Data Protection Toolkit for Schools



An Coimisiún um
Chosaint Sonraí
Data Protection
Commission





Glossary

CJEU – Court of Justice of the European Union

DPC – Data Protection Commission

DPIA – Data Protection Impact Assessment

DPO – Data Protection Officer

EEA – European Economic Area

ETB – Education and Training Board

GDPR – General Data Protection Regulation

ICT – Information and Communication Technology

SAR – Subject Access Request



For more information on wording with specific legal meanings under the GDPR, read through the [Definition of Key Terms on our website](#).



CONTENTS

Foreword.....	4
Introduction	4
Background	4
Contents of the “toolkit”	6
Guidance	8
Introduction	9
Data protection and schools.....	9
What is “personal data”?.....	10
What is a “data subject”?	11
What is a “data controller”?.....	11
What is a “data processor”?.....	11
Are schools required to have a Data Protection Officer (“DPO”)?	13
What are the principles of data protection?	14
What is a legal basis?	14
What is special category personal data?	22
What are data subject rights?	24
The exercise of data protection rights by or on behalf of children.....	26
CCTV on school premises.....	30
Storage and retention of data	32
Use of technology in schools.....	34
FAQs	36
Resources.....	49
Schools and subject access requests	50
Privacy policies – What kind of information does my school need to include?	61
Data Protection Impact Assessments.....	64

Foreword


Introduction

Under data protection law, schools are considered to be “data controllers” as they process personal data in order to carry out their functions and meet their statutory obligations. This includes, amongst other things, the processing of personal data of employees, parents and students, who, for the most part, are children in the eyes of the law. The personal data of these individuals (“data subjects”) are processed for different purposes, as each processing activity arises within different contexts.

This toolkit has been specifically created for schools to assist them with their obligations as data controllers and to help them to comply with the General Data Protection Regulation (“**GDPR**”) and the Data Protection Act 2018 (“**2018 Act**”). Given the particularly challenging issues that may arise when processing the personal data of children, this resource is focused on the processing of student/children’s personal data only.

Background


In December 2021, the Data Protection Commission (“**DPC**”) published the [Fundamentals for a Child-Oriented Approach to Data Processing](#). The Fundamentals aim to assist all organisations that process children’s data (including schools), by clarifying the principles, arising from the high-level obligations under the GDPR, to which the DPC expects such organisations to adhere. The Fundamentals are anchored on the principle of the best interests of the child and the DPC highlights that this must always be a primary consideration when processing children’s personal data. The Fundamentals also recognise the evolving capacity of the child, which is something that schools, particularly secondary schools, will need to take into account as their students come closer to reaching the age of majority and become more capable of making their own decisions. These issues alone demonstrate the complexity for data controllers such as schools, in terms of protecting and vindicating the data protection rights of children.



From the perspective of its complaint-handling and consultation function, the DPC identified a number of areas, which schools, as a sector, appear to be finding challenging from a data protection compliance perspective, and decided to produce a data protection resource specifically for schools.

Before drafting this toolkit, the DPC consulted with a number of external organisations and management bodies in the education sector in order to gain a clear picture of the specific areas, which they felt merited particular attention in terms of guidance. The DPC took this feedback into account when deciding on the format and topics covered in this toolkit.

The DPC has produced this “Data Protection Toolkit for Schools” in order to further assist schools in meeting their data protection obligations. As mentioned above, this resource is primarily concerned with children as data subjects, and does not cover specific issues that may arise in the context of schools processing employee data, for example. **For advice on personal data processing more generally, the DPC has a variety of guidance available to the public on our website.**



The full range of our guidance documents and publications can be found on our website www.dataprotection.ie



Contents of the “toolkit”

This toolkit is broken down into three different sections:



- A detailed guidance piece on different aspects of data protection law in the specific context of schools
- An FAQ section containing answers to questions commonly received by the DPC from the education sector
- An appendix containing three helpful resources for schools, namely:
 - A sample template for Data Protection Impact Assessments (DPIAs)
 - An infographic on what information to include in a Privacy Policy
 - A “checklist” for schools on how to respond to a Subject Access Request (SAR)



Resources



Sample DPIA Template



Privacy Policy Infographic



SAR Checklist

All sections of this toolkit are interdependent and as such, the DPC strongly recommends that schools, as data controllers with responsibilities and obligations under data protection law, read this resource in its entirety, in order to ensure they have as comprehensive an overview as possible.



Guidance



Data protection and schools

Schools routinely collect various types of personal data in the course of carrying out their functions and statutory obligations¹. From information about prospective students in application forms, sensitive medical information about allergies or health conditions, right up to information on student's academic performance, schools are active data controllers and process personal data every single day.

The special case of children's data

Schools process the personal data of lots of different types of people, such as parents, staff members, and external service providers, however their processing activities primarily involve the personal data of students, in other words children. Given the particular focus on the importance of the protection of children's personal data under the GDPR, the DPC recognises the challenges that schools, as data controllers, face on a day-to-day basis in ensuring compliance with their data protection obligations towards children.

In December 2021, the Data Protection Commission ("**DPC**") published the **Fundamentals for a Child-Oriented Approach to Data Processing ("the Fundamentals")** which is a detailed guidance document aimed at raising the level of protection afforded to children by all organisations that process children's data, and this includes schools. The Fundamentals examine, amongst other things, the issue of when children should be entitled to exercise their various data protection rights to access, erasure and restriction of processing, both in conjunction with and independently of their parents. This is an area very much linked to the evolving capacity of the child and requires careful consideration of where the best interests of the child lie. This concept of the evolving capacity of the child is relevant for schools, particularly secondary schools where many final year students turn 18 and are therefore, in law, adults in their own right. The Fundamentals are anchored on the principle of the best interests of the child and the DPC highlights that this must always be a primary consideration when processing children's personal data.

¹) For example a "Record of Processing Activities" (RoPA). The DPC has developed separate detailed guidance on RoPA requirements which you can find on our website.



Related to this is the concept of child protection and welfare, and the DPC's position is that **"child protection/welfare measures should always take precedence over data protection considerations affecting an individual"**². While this is referenced in the Fundamentals mainly within the context of legal bases, the welfare principle applies more broadly to the processing of children's personal data. That said, the application of the welfare principle should not be construed as a means to ignore the data protection rights of the child or to simply pay lip-service to those rights when there is a welfare issue. A balancing exercise must be carried out to ensure that the data protection rights of the child are protected to the extent possible, even if welfare concerns take precedence in certain limited cases. As a matter of policy, this should be assessed on a case-by-case basis.

These issues alone demonstrate the complexity for data controllers such as schools, in terms of protecting and vindicating the data protection rights of their students. As a result, the DPC has produced this guidance for schools to further assist schools in meeting their data protection obligations. This document covers topics such as what is a data controller/processor, explanations of legal bases and how they might apply in a school setting, data subject rights, including access requests and the role of parents and children in this regard, and the use of technology in schools. As mentioned above, this guidance is primarily concerned with children as data subjects, and does not cover specific issues that may arise in the context of schools processing employee data, for example.

What is "personal data"?

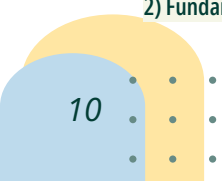
Article 4(1) of the GDPR defines personal data as:

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

The Court of Justice of the European Union ("**CJEU**") has interpreted "personal data" broadly. In most cases, it will be obvious to a school what constitutes the personal data of a child, such as their name, address and date of birth. However, a child's personal data can also include things like information pertaining to their academic progress, photos or videos of them that may be taken in the context of school activities, and may even include lesson plans specifically tailored to that child (if applicable).

Individuals may not be aware of the extent of personal data that is being collected about them, so it is important that schools are very clear in terms of explaining exactly what personal data they are collecting and why.

²) Fundamentals page 24.



What is a “data subject”?

Data subjects are individuals whose personal data is processed by a data controller. Schools process the personal data of a number of different types of data subjects, including students, employees, volunteers, legal guardians and possibly foster parents. However, this is not an exhaustive list as the personal data of others may also be processed. For example, if a school has a CCTV system in place, the personal data of individuals who enter a school premises may also be processed.

Children as data subjects

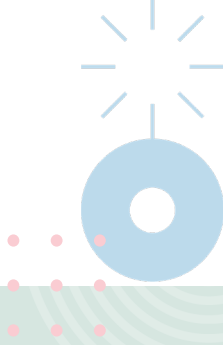
Under Section 29 of the 2018 Act, a child is an individual under the age of 18 years. The legal rights of children are considered and documented in detail in Chapter 2 of the DPC’s Fundamentals. The core message is that children of all ages, regardless of their circumstances, have the same data protection rights as adults; these rights are sourced under Articles 12-22 of the GDPR. The exercise of the rights of children are considered at a later point in this guidance.

What is a “data controller”?

A data controller determines the purposes and means of processing personal data. Schools are the data controller of the personal data they process because they determine **what** personal data they need to process and **why**. This does not mean that the Principal of the school or the Chairperson of the Board of Management, as an individual, is the data controller. The school as an entity is the data controller and it is a matter for the school to determine which individual will be addressing the data protection queries that may arise, on the school’s behalf, in the event that they do not have a DPO. It may be that the school decides the Board of Management will act as the designated point of contact for data protection matters or that the school assigns an individual to address any data protection queries which may arise. It is a matter for each school as to how they wish to structure this, however whatever is decided should be detailed in the school’s Privacy Policy.

What is a “data processor”?

A data processor carries out processing activities on behalf of and in accordance with a data controller’s instructions. In other words, the data controller can provide personal data to the data processor to carry out such processing activities on its behalf. Schools may decide to engage the services of third parties to assist them with any aspect of their function, including those that involve the processing of personal data. When this happens, the third party that is engaged to act for a specific purpose on the specific instruction of the school is known as the data processor and in most cases the school will remain the data controller.



Example 1:

Many schools use applications (apps) to streamline administrative processes so that relevant information and student data is up to date and to ensure effective communication between parents and the school. It is a matter for the school, as data controller, to decide which app they wish to use and for what purpose. Generally, the school remains the data controller for the purposes of data protection law and the platform being used for the app is likely considered the data processor (provided it is only processing personal data under the specific instructions of the school and nothing else). Parental permission is not required for the school to engage the services of a specific processor. While schools are entitled to engage with any processor they choose, they must ensure they have an appropriate legal basis for processing the personal data. The school also has a responsibility to ensure that they enter into a processing agreement with the processor in line with the requirements of Article 28(3) GDPR. Also, in accordance with Article 28(1) GDPR, the data controller must ensure that the processor has provided sufficient guarantees to implement appropriate technical and organisational measures so that the processing meets the requirements of the GDPR.

Example 2:

At Christmas time, primary schools sometimes wish to facilitate their students designing their own Christmas cards. In order to do so, they will need to send the pictures the children draw to a printer and the pictures are likely to contain some of the child's personal data, such as their name, age and class. The printing firm engaged in this instance is the data processor, as the processor is engaged by the school as data controller, for one purpose only, which is to print a certain number of cards, after which it would be expected that the personal data, which belongs to the children, is deleted. It is a matter for the school to engage with the printing firm to set out the parameters of the instructions which should include a time frame for the retention and subsequent deletion of the personal data of the children.

Are schools required to have a Data Protection Officer (“DPO”)?

There are three instances where it is a mandatory requirement for an organisation to appoint a DPO. These three instances are clearly stated within Article 37 of the GDPR;

- **Article 37(1)(a)** stipulates that all organisations that process personal data, either as a data controller or data processor, must designate a DPO where the **“processing is carried out by a public authority or body”**.
- **Article 37(1)(b)** states that where the processing operations by virtue of their nature, scope and/or purposes, require **regular and systematic monitoring of data subjects on a large scale**, a DPO must be appointed.
- **Article 37(1)(c)** states where the core activities of the controller or processor consist of processing on a **large scale of special categories of personal data (Article 9) or criminal convictions and offences (Article 10)**, a DPO must be appointed.

When defining a “public authority” within the 2018 Act, Section 2(1) explicitly excludes “a recognised school or board within the meaning of section 2 of the Education Act 1998”, but further states that this definition of a public authority includes “a recognised school established and maintained by an education and training board and a board of a school so established and maintained, and (ii) a management committee established under section 37 (3) of the Education Act 1998”.

It is a school’s responsibility to determine whether or not they fall under the definition of a “public authority” as set out under the 2018 Act. While it will not be a requirement for many schools to appoint a DPO, they can voluntarily appoint one if they wish to do so. Each Education and Training Board (**ETB**) should note that they are required to appoint a DPO as they would be considered a “public authority” within the meaning of Section 2(1) of the 2018 Act.

In the event that a school is not required to have a DPO, the DPC still recommends that they have a dedicated point of contact for all data protection queries to ensure that they are addressed expeditiously. The exercise of rights under Articles 15-22 of the GDPR are subject to statutory timeframes. Therefore, as a matter of best practice, it is recommended that schools have a set procedure in place for dealing with data protection queries and issues. For example, they could have a dedicated email address that is regularly monitored, **including during school breaks and holidays**, that individuals can submit data protection-related queries to, or they could use a specific heading in the subject line so as to quickly identify emails relating to data protection. This information should be available in the school’s Privacy Policy and should be easily accessible to parents, staff and students.



What are the principles of data protection?

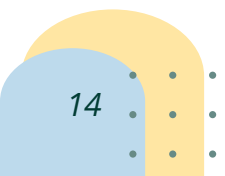
Article 5 of the GDPR covers principles relating to processing of personal data. The DPC previously issued [Guidance on the Principles of Data Protection](#). Briefly, Article 5 provides that personal data must be processed lawfully, fairly and transparently. It also sets out the principles of purpose limitation (personal data must be collected for specified, explicit and legitimate purposes) and data minimisation (data controllers must only collect what is adequate, relevant and limited to what is necessary for the purposes for which they are processed). Further, all personal data must be accurate and kept up-to-date and securely deleted when it is no longer required. Finally, data controllers are accountable and responsible for compliance with data protection law and must be able to demonstrate compliance. The principles of data protection are applicable to all data controllers, including schools.

What is a legal basis?

Article 6 of the GDPR requires that the processing of personal data be lawful, and Article 6(1) provides six such legal bases. This is a finite list and if none of these legal bases apply, then the processing cannot take place lawfully. Therefore, schools, as data controllers, must be able to identify which legal basis they are relying upon for each act of processing. Depending on the processing activities, schools may rely on different provisions under Article 6(1) of the GDPR for different acts of processing.

The legal bases under Article 6(1) of the GDPR are as follows:

1. **Consent** of the data subject, Article 6(1)(a);
2. Processing is **necessary** for the **performance of a contract**, Article 6(1)(b);
3. Processing is **necessary** for **compliance with a legal obligation** to which the data controller is subject (in other words, the data controller is obliged by law to perform a task), Article 6(1)(c);
4. Processing is **necessary** to protect the **vital interest** of a data subject or another natural person, Article 6(1)(d);
5. 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 data controller, Article 6(1)(e);
6. Processing is **necessary** for the purposes of the **legitimate interests** pursued by the data 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, Article 6(1)(f).



Legal Bases



Consent



Performance of a contract



Compliance with a legal obligation



Vital interest



Public interest



Legitimate interest



You can find more in-depth information around the [legal bases for processing personal data](#) on our website.



Preliminary point: The “necessity” requirement

The requirement of “necessity” applies to all legal bases save for the consent of the data subject. Exactly what processing is necessary to achieve a given purpose will vary from case to case, depending on the exact circumstances, and schools will need to limit processing to that which is needed for an explicit purpose. In assessing necessity, schools should consider the **reasonableness** and **proportionality** of the processing. In other words, schools must ask themselves if there is a more reasonable or less intrusive way to achieve the stated purpose without processing personal data, or if their objectives can be achieved by processing less personal data. If so, this ought to be done as otherwise there is a risk that the legal basis upon which the school is relying will be unlawful. This necessity element should be assessed on a case-by-case basis, depending on the circumstances of the processing.

The most common legal bases relied upon by schools are considered below. This is not to say that schools cannot rely on the other legal bases that have not been covered in this guidance, rather it is the DPC’s experience that the legal bases listed below are the most applicable in the context of schools.

i. Consent

Under the GDPR, consent to processing must be freely given, specific, informed and unambiguous. For children who are too young and/or lack capacity to give their own consent, consent can be provided by their legal guardian. Older children however, might be in a position to give their own consent to processing.

For example, if a school has identified that consent is the appropriate legal basis for taking and publishing photographs in a particular context, they will generally need to obtain the consent of the child’s legal guardian to do so, depending on the age and capacity of the child. It must also be possible for the legal guardian to withdraw their consent at any time, bearing in mind, that withdrawal of consent does not affect the previous use of any photos taken of that particular child before the consent was withdrawn. In the case of older children, schools may find themselves in circumstances where they need to obtain the consent of the child. For example, the parent of a 15-year old child may have given consent for photographs to be taken of their child at the school’s talent show for publication in the local newspaper – however, the 15-year old may very well have objections to this and may not wish to appear in the local newspaper. Schools themselves are in the best position to judge the age at which they believe their students are capable of understanding what exactly it is they are agreeing to and giving consent themselves. As such, depending on the context and the age of the student, it may be a case of involving both the parent/guardian and the student in the discussion about consent.

For further detail on this, see the blog on our website: [‘Taking photos at school events – Where common sense comes into play’](#).



ii. Compliance with a legal obligation

Schools, as data controllers, have statutory functions to perform under different pieces of legislation. Data protection law does not stand in the way of such processing where data controllers are mandated to process personal data for a particular purpose under other statutory provisions. Data protection law provides a legal basis under Article 6(1)(c) of the GDPR for the processing of personal data when the processing by the data controller is necessary for compliance with a legal obligation to which the data controller is subject.

Some legislation that schools may seek to rely on are as follows:

Education Act 1998, Education (Welfare) Act 2000, Education for Persons with Special Needs (EPSEN) Act 2004, Health Act 1947, Children First Act 2015, Child Protection Procedures for Primary and Post-Primary Schools 2017, Teaching Council Acts 2001-2015, Child Care Act 1991 and Children Act 2001.

This is a non-exhaustive list and schools must have consideration for the type of data they are processing when seeking to rely on such legislation.

School records

For example, under Section 20 of the Education (Welfare) Act, 2000, as amended, the principal of a school must establish and maintain a register of all students attending that school. Section 21 further provides that the principal of the school must ensure that attendance records for each student are maintained. After the end of each school year, the Board of Management must submit to the education welfare officer assigned to the school, a report on the levels of attendance at that school during the preceding school year.

Similarly, Section 9(g) of the Education Act 1998, as amended, states that a school shall ensure that parent(s) (or in the case of a student who is 18 years, the student themselves) shall have access to records kept by the school regarding the student's educational progress.

These are examples of the statutory duties that must be adhered to by schools, as data controllers. Therefore, the school's legal basis for the processing of personal data in this manner is provided for under Article 6(1)(c) of the GDPR as the processing is being undertaken for the purposes of compliance with a legal obligation under the relevant provisions of the Education (Welfare) Act, 2000, and/ or the Education Act, 1998 as amended. The school must be in a position to identify the specific provisions in the Education (Welfare) Act, 2000 or the Education Act, 1998, or any other Act upon which they are relying.

It is important that schools are aware that it is not enough to refer to an entire body of legislation when relying on Article 6(1)(c) of the GDPR. You must identify the specific section(s) of the legislative instrument that provides you with the lawful basis. The precise sections of any legislation relied upon as providing a lawful basis for data processing must be clearly provided to the data subjects also. For example, it would



not be sufficient to inform data subjects that the Education (Welfare) Act 2000 provides a lawful basis for the collecting and processing of student data for the purposes of a register of students. You would need to specify that Sections 20 and 21 of the Education (Welfare) Act 2000 are being relied upon as providing a lawful basis for the data processing.

Mandatory reporting

Schools may also need to share personal data with third parties such as the Child and Family Agency (“**CFA**”) (known as Tusla) which is the State’s child protection body. For example, the Children First Act 2015 (“**2015 Act**”) places legal obligations on “mandated persons” to report certain child protection concerns to the CFA. The provision of a student’s information or personal data by a school to the CFA constitutes processing of that student’s data and therefore must have a legal basis under data protection law.

Under Schedule 2 of the 2015 Act, a teacher registered with the Teaching Council is a mandated person. Therefore, if a teacher has certain concerns as set out under the 2015 Act, they are legally obliged to report those concerns to the CFA. Therefore, the school’s legal basis for providing this personal data to the CFA is likely to be Article 6(1)(c) of the GDPR as the request is in compliance with a legal obligation under the relevant provisions of the 2015 Act. The school must be in a position to identify the **specific** provision under the 2015 Act upon which they are relying, and it is the school’s responsibility to ensure that they are **only providing the personal data required** under the 2015 Act.

An Garda Síochána

As part of their role in preventing, detecting, investigating or prosecuting a criminal offence, An Garda Síochána may decide to contact a school for certain information relating to a student. The provision of a student’s information or personal data, by a school to An Garda Síochána, constitutes processing of that student’s data and therefore must have a legal basis under data protection law.

Section 41(b) of the Data Protection Act 2018, provides for such processing where it is **necessary** and **proportionate** for the purposes of preventing, detecting, investigating or prosecuting a criminal offence. Therefore, the school’s legal basis in this specific instance for providing this personal data to An Garda Síochána is Article 6(1)(c) of the GDPR as the request is in compliance with a legal obligation under Section 41(b) of the Data Protection Act 2018.

However, it would be expected that An Garda Síochána identify the specific provisions under which they are seeking access to this information in the first instance and the school is entitled to ask that this information be provided to them in writing so that they have a record of the request. Furthermore, the school must be satisfied that the personal data being requested is covered by the relevant provisions being quoted by An Garda Síochána and that the information being provided by the school is necessary and proportionate for the stated purposes of the processing.

Legal obligation is not a “carte blanche”

It is important that schools are aware that, while Article 6(1)(c) provides for the sharing of information where legally required, this is not a carte blanche for sharing any and all personal data. Schools must ensure that they are only providing the personal data that is specifically required under the relevant piece of legislation, and that what they are sharing is necessary and proportionate to the purpose at hand.

iii. Vital interest

Emergency situations may arise in a school which requires the school to act promptly, such as a child becoming seriously ill on the school premises. A school may already be aware that the child suffers from a health condition. If that child requires urgent medical intervention, it may be necessary for the school to disclose that information to paramedics. The disclosure of personal data to paramedics would likely constitute the processing of personal data and must have a legal basis.

Article 6(1)(d) of the GDPR provides that the processing of personal data is legal where the processing is necessary in order to protect the vital interests of the data subject or of another natural person. This legal basis is primarily for emergency situations where there is a threat to a person’s life or to mitigate against a potential risk/threat/harm to, or endangerment of, either the data subject or third party. Therefore, in such a scenario, the school would have a legal basis for such processing of personal data under Article 6(1)(d) of the GDPR.

Example 3:

At the start of the school year, a parent informed their child’s teacher that their child had a severe peanut allergy. On a school trip, the child came into contact with peanuts and went into anaphylactic shock and an ambulance was called. The child’s teacher informed the paramedics of the child’s allergy. The legal basis relied upon here would likely be Article 6(1)(d) of the GDPR as this was an emergency situation where there was a threat to the child’s life, health and welfare.

As the processing of personal data in the example above concerns the processing of health data, the data controller must also have a legal basis under Article 9(2) of the GDPR and this is discussed further below. In this particular scenario, Article 9(2)(c) of the GDPR would likely be applicable as it provides a legal basis for the processing of personal data where the processing is necessary to protect the vital interests of a data subject where that person is physically or legally incapable of giving consent.



Top tip: check out our [case studies for real life examples](#) on how data protection law is applied.



iv. Legitimate interest

Article 6(1)(f) of the GDPR may also be relied upon by schools in certain circumstances. This legal basis is applicable where processing is necessary for the purposes of the legitimate interests pursued by the data 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**.

The GDPR makes clear, at the end of Article 6(1), that public authorities cannot rely on the legal basis of “legitimate interests” to justify the processing of personal data, which is carried out in performance of their tasks. In other words, if a school falls under the definition of a “public authority” under the 2018 Act, they will only be able to rely on legitimate interest for processing activities that do not relate to their core functions. Core functions are essentially the tasks as set out under legislation for a public authority. Examples of this might include the use of CCTV in a school car park for security purposes. Schools must carefully assess whether or not they are considered a “public authority” under the 2018 Act as this will determine their ability and the extent to which they can to rely on legitimate interest as a legal basis for processing personal data.

Data controllers who seek to rely on the legitimate interest legal basis need to meet three components for this legal basis to apply:

- a. identifying a **legitimate interest** which it or a third party pursues;
- b. demonstrating that the intended processing of the data subject’s personal data is **necessary to achieve** the legitimate interest;
- c. **balancing** the legitimate interest against the **data subject’s interests**, rights, and freedoms.

For a data controller to rely on legitimate interest to process individuals’ personal data, it must consider the interests or fundamental rights and freedoms of those individuals and balance these against its own interests. The fundamental rights and freedoms of individuals include the right to data protection and privacy, but also other fundamental rights and freedoms, such as the right to liberty and security, freedom of expression and information, freedom of thought, conscience and religion, freedom of assembly and association, prohibition of discrimination, the right of property, or the right to physical and mental integrity, which may be affected by the processing, either directly or indirectly³. Further, the interests of individuals to be taken into account as part of the balancing test include any interest that may be affected by the processing at stake, including, but not limited to, financial interests, social interests or personal interests⁴.

3) See EDPB Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, page 13. Available at: [edpb_guidelines_202401_legitimateinterest_en.pdf](#)

4) Ibid page 13

A data controller must then be in a position to outline to the individual, or the DPC upon request, its rationale including the compelling grounds on which an organisational legitimate interest outweighs the interests, or fundamental rights and freedoms of individuals. The processing must also be necessary to fulfil the legitimate interests of the data controller.

Where an individual's interests or fundamental rights and freedoms outweigh the legitimate interests of the school as a data controller, then the school **cannot** rely on Article 6(1)(f) of the GDPR as providing a lawful basis. It will be for each individual school, as a data controller, to ensure they are able to demonstrate why their legitimate interest outweighs these rights and freedoms, should either the data subjects or the DPC make enquiries.

While in general terms the legitimate interests legal basis allows for a certain, proportionate level of interference with the rights of data subjects, the balancing test inherent in this legal basis should be recalibrated where the data subjects are children. As such, schools should also note that, when it comes to the processing of children's data, it is the DPC's position that controllers processing children's data in reliance on this legal basis should ensure that the legitimate interests pursued do not interfere with, conflict with or negatively impact, the best interests of the child.

Example 4:

A school is coming up to its centenary celebration and wishes to produce a special book highlighting the historic development of the school and its milestones over the previous 100 years. Publication of this book is likely to include photographs and information relating to former students (who may be alive or deceased) and current students. The school needs to consider its legal basis for the processing of data in this manner. Practically speaking, while obtaining the consent of current students might be relatively straightforward, it would be difficult for the school to rely on the legal basis of consent of former students who are still living and who attended the school over the course of decades. That said, the publication of the book could potentially be construed as a legitimate interest of the school. If relying on the legal basis of legitimate interests, the school would need to balance the rights and freedoms of the affected data subjects against its own legitimate interest and make an appropriate assessment.





What is special category personal data?

Article 9 of the GDPR covers processing of special categories of personal data. This is personal data that, by its nature, is considered to be particularly sensitive information. This type of data requires additional security measures and access considerations due to the heightened risks posed to an individual's fundamental rights and freedoms in the event of a misuse or breach of this data.

Special category data is defined as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership. It also includes genetic data, biometric data where used for the purposes of uniquely identifying someone, data concerning a person's health, and data concerning a person's sex life or sexual orientation.

When consideration is given to this complete list as set out, it is difficult to envisage how a school would not, to some extent, process some special category data about their students. While some of the terms are somewhat self-explanatory within the context of schools and are not further defined under the GDPR, such as racial/ethnic origin or religious beliefs, other terms are defined under Article 4 of the GDPR:



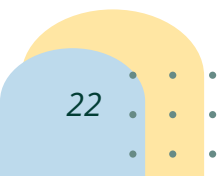
“genetic data” means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;



“biometric data” means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;



“data concerning health” means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.



Examples of special category data that a school may process might include information about a child's religious beliefs or information about any physical or mental medical conditions or allergies a child might have. The default position for the processing of special category data is that it is prohibited under Article 9(1) of the GDPR unless it falls within one of the permitted exceptions under Article 9(2). Therefore, to process special category data, the school must have a legal basis under Article 6 and fall into one of the permissible exceptions under Article 9(2) of the GDPR. It is a matter for the school to identify which special category data they process and which specific exemption under Article 9(2) they are relying upon.

Example 5:

A school needs to carry out an assessment to determine whether one of its students requires additional learning resources to aid with their learning needs (e.g. academic, social & emotional needs, physical, sensory, language and communication difficulties). The school must identify a legal basis under both Articles 6 and 9 of the GDPR to record this information as this concerns the processing of data concerning a child's health. In order to process this kind of special category data to aid in the school's assessment, the school could potentially rely on Article 9(2)(a), the explicit consent from the parent/child (based on the child's capacity). There may also be circumstances where Article 9(2)(h) may be applicable ("pursuant to a contract with a health professional") where the school needs to share information in order for an assessment to be carried out. However this processing must be carried out transparently and with the knowledge of the parents/legal guardians.

Legal Bases for Processing Personal Data

	Right of Access	Right to Rectification	Right to Erasure	Right to Restriction	Right to Portability	Right to Object
Consent	✓	✓	✓	✓	✓	Can withdraw consent
Contract	✓	✓	✓	✓	✓	✗
Legal Obligation	✓	✓	✗	✓	✗	✗
Vital Interests	✓	✓	✓	✓	✗	✗
Public Tasks	✓	✓	✗	✓	✗	✓
Legitimate Interests	✓	✓	✓	✓	✗	✓



What are data subject rights?

The rights of data subjects are set out under Articles 12 to 22 of the GDPR, however, the rights most likely to be applicable in the context of schools are those provided for under Articles 12 to 17 which are addressed below.

The right to be informed

In order to be able to exercise their rights, individuals need to understand what is happening with their personal data. The GDPR requires that individuals must be given certain key pieces of information about the use of their personal data by a data controller, including who holds it and why it is being processed. This information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The clarity of this information is particularly important where the information is being addressed to a child. With this in mind, schools should consider the types of processing they carry out and whether they need to provide specific transparency information for children. This will be a particularly important consideration for secondary schools where many students will have the capacity to understand many of the data processing activities of the school and therefore should be factored in when providing transparency information.

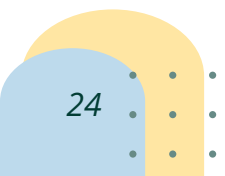
Articles 13 and 14 of the GDPR set out the type of information that must be provided by the controller, and includes: the identity and contact details of the organisation that is collecting or using the personal data; the purposes and legal basis for collecting or using the personal data; who the personal data is being shared with; how long it will be kept for; and what the individual's data protection rights are.

In order to comply with Articles 12, 13 and 14 of the GDPR, schools should ensure that they have a clear and understandable Privacy Policy in place, and that this Privacy Policy is easy for parents/guardians/students to access (e.g. in a prominent place on the school's website, handed out at the beginning of each term, etc.). For more information on what kind of information to include, please see "Privacy policies –" on page 61.

The right of access

Article 15 of the GDPR provides individuals with the right to request a copy of their personal data. They are also entitled to receive the information set out under Article 15(1) as part of their Article 15 request. This is known as a subject access request. These requests must be responded to free of charge and in an accessible form within the specific time frame. For further information on how to respond to a subject access request, please see our "SAR Checklist" on page 52.

If an access request involves the sharing of a student's health data then schools must also be aware that the Data Protection Act 2018 (Access Modification) (Health) Regulations 2022, requires an assessment be carried out, **prior** to the release of health data, as to whether it could cause harm to the data subject.



Right to rectification

Article 16 of the GDPR provides the right to have inaccurate data rectified. This is in line with the principle under Article 5(1)(d) of the GDPR that data shall be accurate and up to date.

The right to rectification is not an absolute right; in order for Article 16 to apply, the personal information being processed by a data controller must be inaccurate as to a matter of fact. Schools should note that where the information is opinion-based, or where a data subject simply does not agree with the content of information being processed, the right to rectification would likely not apply.

The right to erasure

Article 17 of the GDPR provides for the right to have data erased without undue delay in specified circumstances, namely where:

- a. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- b. the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
- c. the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
- d. the personal data have been unlawfully processed;
- e. the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
- f. the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

Recital 65 of the GDPR highlights that the right to erasure is particularly relevant where the data subject has given his or her consent to processing as a child and was not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The right of erasure can be restricted in certain circumstances, which are set out under Article 17(3)⁵ such as the controller has a legal obligation to retain the personal data.

⁵ Article 17(3) stipulates that the right to erasure does not apply where processing is necessary: for exercising the right of freedom of expression and information; for compliance with a legal obligation; for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; for reasons of public interest in the area of public health; for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes or for the establishment, exercise or defence of legal claims.



The exercise of data protection rights by or on behalf of children

The DPC previously issued guidance entitled Children, Parents and Data Protection: Can I make a complaint on behalf of my child? This guidance sets out that:

“The core message is that children have their own legal rights, separate and distinct from their parents/guardians and these include data protection rights. Children also have a right to be heard in all matters that affect them in line with their developing capacities. In addition, all decisions made which relate to the processing of children’s personal data must be underpinned by what is in the child’s best interests (“the best interest principle”).”

This guidance also notes that the main difficulty in the exercise of children’s data protection rights relates to the following questions: Who can exercise the data protection rights of children on their behalf? Up to what point can such individuals exercise those data protection rights on behalf of children?

Legal guardians can exercise the data protection rights on behalf of their child so long as it is in their child’s best interests to do so. However, it is important to realise that any personal data which relates to their child, is and remains, the personal data of their child. It does not belong to anyone else, such as their legal guardian and legal guardians do not have an automatic entitlement to that personal data.

As there is no law in Ireland setting out the age at which children can exercise their own legal rights, a child may in principle exercise their own data protection rights at any time, as long as they have the capacity to do so and it is in their best interests. Children should be able to be jointly represented with an adult if they wish when exercising their rights.

The DPC’s Fundamentals for a Child-Oriented Approach to Data Processing sets out a number of criteria that should be considered when assessing if a child can exercise their own rights, or indeed if it is in a child’s best interests for their legal guardian to exercise their rights on their behalf.



The Fundamentals can be found in the resources section of the DPC website, under ‘General Guidance’.



Factors to be taken into consideration when assessing whether a child should be capable of exercising their own data protection rights:

- The age and maturity (for example as demonstrated by interactions between the child and the organisation in question) of the child;
- The type of request (access request, erasure request, right to object, etc.);
- The context for the processing and the type of service offered by the controller (e.g. social media platform, doctor-patient relationship, online shopping platform, etc.);
- The type of personal data at issue (e.g. child seeking access to medical data, child seeking erasure of photos of themselves on social media, child seeking to update their email address on a platform). The DPC considers that in cases where the exercise of a child's data protection rights involves access to special category personal data, particularly such as medical data, or access to other sensitive types of data, such as social work data, that careful consideration should be given to whether the release of such personal data could cause serious physical or mental harm to the child in question;
- Whether enabling the child to exercise their data protection rights themselves is in the best interest of the child (i.e. do they understand the consequences of erasing certain types of personal data, will they fully comprehend what it is they are receiving as part of an access request, will receiving certain information be detrimental to their well-being?)
- Whether the child is seeking to exercise their rights with the assistance/ participation/ knowledge of a parent/ guardian or expert third party/ advocate.

Factors to consider when deciding whether it is in the best interests of the child that their parent(s)/ legal guardian(s) exercise their data protection rights:

- The age of the child – the closer the child is to the age of 18, the more likely it is that an organisation holding the child's personal data should deal directly with the child themselves, rather than involving the parent/ guardian. In this regard, the DPC considers that where a child has reached 17 years, given the closeness of this age to the age of majority (and this notably also being the age at which a driving licence can be obtained as well as the minimum age for sexual consent), other than in exceptional circumstances (i.e. where the best interests of the child demonstrably require it), the child's data protection rights should not be exercised by the parent(s)/ guardian(s). Instead the organisation should deal directly with the child;
- The nature of the personal data and the processing being carried out – this should include consideration of the sensitivity/ confidentiality of the personal data and the basis upon which it has been provided by or shared by the child with the organisation which holds it – for example is there a duty of confidence owed to the child?



- The nature of the relationship between the child and the parent/ guardian – e.g. are there any court orders relating to parental access/ responsibility/ custody/ child protection etc. in existence?;
- The purpose for which the parent(s)/ guardian(s) seek(s) to exercise the child's data protection rights – for example is this purpose wholly in the best interests of the child or is there another purpose or interest (i.e. that of the parent/ guardian or a third party, as opposed to the child) pursued in seeking to exercise these rights?;
- Whether the child would, or does in fact, consent to the parent(s)/ guardian(s) exercising their data protection rights and any views or opinions expressed by the child;
- Whether allowing the parent(s)/ guardian(s) to exercise the child's data protection rights would cause harm/ distress to the child in any way;
- Whether there are any sectoral rules or laws which apply to the particular context in which the parent(s)/ guardian(s) is/ are seeking to exercise the child's data protection rights.

It is a matter for the school, as a data controller, to satisfy themselves that the person exercising the data rights of the child is their legal guardian and that fulfilling the request is, amongst other things, in the best interests of the child. If the child is exercising their own data protection rights, the school must be satisfied that the child has the capacity to do so and it is in their best interests. In addition, the school must consider the child's right to be heard in all matters that affect them in line with their developing capacities⁶.



6) Article 12 of the UN Convention on the Rights of the Child requires that any child who is capable of forming his or her own views has the right to express those views freely in all matters affecting them and that those views are given due weight in accordance with the child's age and maturity.

Children in the care of the state

The DPC has received numerous queries from foster parents regarding the data protection rights of children in their care. A difficulty that may arise for schools regarding children who are in foster care, is that their foster parents are not their legal guardians.

The issue of legal guardianship of foster carers is not one with which the DPC can assist as this issue is separate and distinct from data protection. However, from a data protection perspective, it is open to schools to conduct a case-by-case risk-assessment with the welfare and best interests of the child being paramount, carefully considering whether disclosing or indeed withholding the information could give rise to identifiable harm(s). Should the school then decide to release the data to a foster parent, who is in fact a third party as they are not the child's legal guardian, the school, as data controller, would need to be able to demonstrate how they carried out that risk assessment, what issues they considered as part of the assessment and how they came to their conclusion.



Restrictions on data subject rights

While the GDPR affords a number of rights to data subjects, it also prescribes that such rights can be lawfully restricted by a data controller in certain circumstances. In other words, there are some instances where data controllers can decide **not** to grant a data subject request. However, this is in very limited circumstances. Article 23 of the GDPR sets out a range of circumstances under which a data controller can lawfully restrict data subject rights, and Sections 59, 60 and 61 of the 2018 Act give further effect to the provisions of Article 23. However, the GDPR highlights that any measure used to restrict the rights of a data subject must be of limited scope and applied in a strictly necessary, proportionate and specific manner. In other words, schools should not routinely rely on exemptions to avoid having to engage with data subject requests, and must only apply restrictions in limited circumstances where it is absolutely necessary to do so.

The DPC's guidance on [Limiting Data Subject Rights and the Application of Article 23 of the GDPR](#) provides further information on the restriction of rights.

Therefore, if a school wishes to restrict the rights of a data subject, it must specify the precise restriction it is relying upon (quoting the precise provision/s of the legislation), how they have come to this decision, and inform the data subject accordingly. It is open to the data subject to revert to the school and seek further clarity on the restriction and data controllers ought to respond accordingly.



CCTV on school premises

Queries are often raised with the DPC regarding the use of CCTV in schools. The DPC has published comprehensive guidance on the use of [CCTV for data controllers](#), which schools should consult in the first instance.

Broadly speaking, the principles set out in this CCTV guidance apply equally to schools, save that schools must be particularly mindful that where CCTV is capturing images of children, a higher threshold of protection would be required owing to the fact that children merit specific protection under the GDPR. While this toolkit is focused on the processing of children's personal data in particular, schools must also be mindful that they are a workplace. The impact that CCTV may have on a school's employees and visitors must also be considered when determining if a CCTV system should be implemented in a school. All such processing of personal data must be in compliance with data protection law.

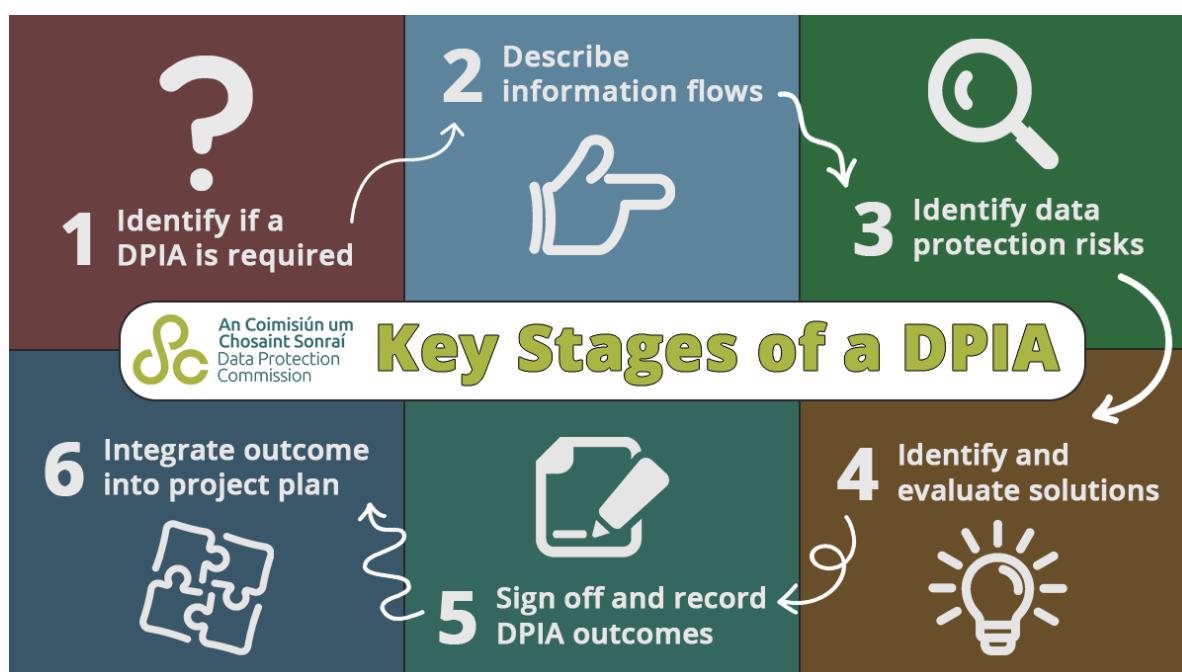
When considering the implementation of CCTV, schools must:

- ✓ Have a clearly defined purpose for installing CCTV in or around the school;
- ✓ Have a legal basis for the use of CCTV;
- ✓ Be able to demonstrate that the CCTV is necessary to achieve its stated purpose(e.g. they must be able to show that the purpose **cannot** be achieved by less intrusive means than CCTV. If the purpose can be achieved using less intrusive means, then the processing of personal data through the use of CCTV would not be lawful as it could not be deemed to be necessary);
- ✓ Be able to demonstrate that the use of CCTV is proportionate for its stated purpose;
- ✓ Be able to demonstrate that appropriate measures are in place to ensure that the CCTV recordings are safe and secure, both technically and organisationally, including who accesses and views CCTV recordings;
- ✓ Have retention policies in place;
- ✓ Have appropriate signage in place to inform people CCTV is taking place;
- ✓ Have an up-to-date CCTV Data Protection Policy in place, which should be brought to the attention of everyone whose data is captured or likely to be captured (for example, making the policy available on the school's website).
- ✓ Ensure that CCTV is not in operation in areas where students, staff or visitors would have an increased expectation of privacy (e.g. changing rooms).

Data Protection Impact Assessments

Schools can demonstrate that they have considered in detail the above-mentioned criteria by carrying out a Data Protection Impact Assessment (DPIA). Article 35 of the GDPR states that a DPIA must be carried by a data controller where a type of data processing, in particular using new technologies, is likely to result in a high risk to the rights and freedoms of individuals. The GDPR also sets out a number of specific instances in which controllers **must** conduct a DPIA. A DPIA describes a process designed to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible. If required, a DPIA must be completed before the data processing has begun. DPIAs are important tools for negating risk, and for demonstrating compliance with the GDPR. In addition to the CCTV system example outlined above, a school may need to carry out a DPIA in other circumstances such as using third-party platforms to process student data (new EdTech platforms etc.) or in circumstances where student health data is being processed (e.g. health monitoring apps used by a school's football team).

The DPC has separate [guidance on DPIAs available on our website](#). It is the DPC's position that where the processing of children's personal data is at issue, a data controller should carry out a DPIA given that children are a particularly vulnerable group. For further assistance on how to carry out a DPIA, please see our "DPIA Template" on page 66 of this toolkit, to see a sample template DPIA that we've created for schools to use.





Storage and retention of data

Schools should ensure that any personal data they process is stored safely and retained for no longer than is required.

Storage

Article 24 of the GDPR obliges the data controller to ensure that appropriate technical and organisational measures are in place in their organisation and to be able to demonstrate that the processing of personal data is performed in accordance with the GDPR. This applies to all personal data which forms part of a filing system, including the personal data of the children enrolled in the school. The responsibility also rests with the data controller to ensure the storage of personal data by its processors, including cloud-based processors, conforms with these requirements.

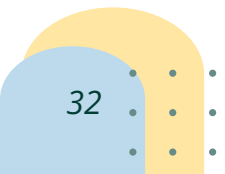
Note: While most schools are familiar with their wider obligations regarding the storage of data in the broader sense, this also relates to handwritten incident reports that may be taken by teachers during the course of the school day. Any handwritten notes/logs or journals which contain the personal data of children, in whatever form they arise, should be locked away at the end of each school day.

Retention

As data controllers, schools have an obligation to only keep personal data for as long as is **necessary** for the reason it was originally collected. This is highlighted under Article 5(1)(e) of the GDPR, which states that personal data shall be:

(e) 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 may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ("storage limitation");

The GDPR does **not** set specific time limits for different types of data. This is a data controller's responsibility to determine, and the time limits for categories of data will depend on how long the controller needs the data for each specified purpose. For example, if a child did not accept the offer of a place in a school and is not a pupil of the school, it would be expected that the retention period for that data relating to that child would be short, unless otherwise specified. On the other hand, schools may need to retain certain records, e.g. accident reports, for the purposes of being able to defend themselves against potential legal claims in the future. In this instance, it is reasonable to expect that the school will need to apply a longer retention period.



However, personal data should not be processed forever or indefinitely just in case it might be useful in the future. Schools will need to ensure they can demonstrate the necessity and proportionality of any retention periods they set. Schools also need to be aware of and understand the statutory frameworks within which they, as data controllers, operate and must be aware of any relevant time periods (if any) for retaining personal data that may be specified in other legislation to which the school is subject.

Retention policies

Schools should have a retention policy made available on their website so that individuals are aware of how long their data is being retained for. A retention policy is a document that sets out a list of all of the different types/categories of personal data that you hold, how long you intend to keep it, and why.

Schools should have a system in place for making sure that they are adhering to these retention periods in practice, e.g. having appropriate procedures in place for disposing of records, ensuring that data is promptly securely deleted upon reaching the defined retention, etc. If your school engages a third party to securely destroy the personal data on the school's behalf, it would be advisable to request (and retain) a certificate of destruction.

Retention policies should also be reviewed at regular intervals to make sure the policy is fit for purpose – for example, if you find that you are not actually using a particular category of data that you routinely collect, you should reconsider whether you need to retain it at all.





Use of technology in schools

Schools use technology on a daily basis to assist them in carrying out their duties. This technology ranges from email, online education platforms, knowledge management systems, and external communication systems, to name but a few.

Technology is an intrinsic part of how schools operate, and data protection law does not prevent schools from using various platforms and systems. However, schools do have obligations as data controllers when it comes to the protection of the personal data that they process and should be mindful of their obligations when using technology to carry out their functions.

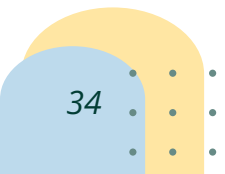
Third-party service providers

Schools are entitled to use third-party service providers to assist them with aspects of their duties and functions. For example, a school may have engaged the services of an online education platform to facilitate remote learning during the pandemic, or they may use an application to help them track attendance of students and academic performance. As a preliminary point, schools, as data controllers, are not obliged to rely on permission/consent from data subjects in order to engage the services of a data processor (e.g. a software provider). In other words, so long as the school has a clear legal basis to do so, it is for schools to determine which data processors they wish to work with.

However, under Article 28 of the GDPR, data controllers are obliged to only use processors that provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR. Controllers are also required to have in place a contract with any processors they engage, and this contract must set out the following information:

- the subject matter and duration of the processing
- the nature and purpose of the processing
- the type of personal data and categories of data subjects
- the obligations and rights of the controller

In other words, if a school is engaging the services of a processor (e.g. a software provider) to process personal data on its behalf, they are free to select whichever processor they choose, provided that processor has sufficient technical and organisational measures in place to protect the personal data, and provided they have a contract in place with this processor. You may wish to consult the DPC's guidance on this matter ("[A Practical Guide to Controller-Processor Contracts | Data Protection Commissioner](#)").



While schools do not need permission to use a specific processor, they must ensure that they have an appropriate legal basis under Article 6 GDPR to process the personal data that will be stored/used by the data processor. Therefore, it is important that schools give due consideration to the processors they engage, and that they are aware that they still carry responsibility for how the personal data that they instruct the processor to collect, is processed.



Top tip: follow our social media accounts for the most up-to-date guidance and information!



Use of personal email, laptops and devices

While teachers are not prohibited from using their personal devices to carry out their work, an enhanced level of consideration and security must be considered.

Article 24 of the GDPR requires a school to implement appropriate technical and organisational measures in order to safeguard personal data. For this reason, schools should promote the use of school devices and work email accounts, as opposed to personal devices and personal email accounts, as the school retains a level of control over such devices.

Issues can arise with the use of personal devices when responding to individual data protection requests under Articles 15-22 of the GDPR. Teachers are often not aware that their personal devices and personal email accounts will also need to be reviewed when responding to individuals and this can put a school in a compromising position if teachers are on leave, moved schools etc.

In the event personal devices are going to be used by teachers it is best practice for a school to have a “Personal Devices Usage Policy” so teachers are aware of their obligations and responsibilities when using such devices.

FAQs

1. What does “transparency” mean under GDPR?

Individuals have a right to know that their data is being processed and by whom, and this right to be informed, under Articles 13 and 14 GDPR, is a key part of any organisation’s obligations to be transparent. The principle of transparency requires that any information given to a data subject about the processing of their personal data is easily accessible and easy to understand, and requires that clear and plain language be used. This information is usually provided in written form in a Privacy Policy, and can also be supplemented using non-textual measures, where appropriate (e.g. signs highlighting CCTV, infographics depicting who data is shared with, etc.). Schools should also note that given that children merit specific protection under the GDPR, any information and communication, addressed specifically to a child should be in such a clear and plain language that the child can easily understand. For further information on the transparency obligation in the context of children’s data protection rights, please see the Data Protection Commission’s [“Fundamentals for a Child-Orientated Approach to data processing.”](#)

2. What kind of information do schools need to include in a Privacy Policy?

A privacy policy should clearly explain to individuals in language they can easily understand what personal data the school is collecting and why. It should also specify, amongst other things, the school’s lawful basis for processing under Article 6(1) of the GDPR, who the information is shared with and how long the individual’s data is held before being deleted securely. A privacy policy should be supplemented with a Retention Policy.

A privacy policy should also inform data subjects on how to exercise their rights under the GDPR, including by providing the name and contact details of the school’s DPO or dedicated point of contact for data protection matters. For more information on what to include in a privacy policy, see “Privacy policies” on page 61.

3. How long should we keep personal data for?

Article 5(1)(e) of the GDPR stipulates that personal data shall 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 processed⁷.

In line with this, a school should specify retention periods for each category of personal data it holds, and outline same in a Retention Policy. A retention period is best described as the period of time a data controller will hold personal data before it is securely deleted. The GDPR does **not** set specific time limits for different types of data. This is a data controller's responsibility to determine, and the time limits for categories of data will depend on how long the controller needs the data for each specified purpose.

Schools should note that personal data should not be processed forever or indefinitely just in case it might be useful in the future. Schools need to ensure they can demonstrate the necessity and proportionality of any retention periods they set, and they must be aware of relevant time periods (if any) for retaining personal data that may be specified in other legislation to which the school is subject.

As a matter of best practice, schools should carry out regular audits of the personal data they collect and the procedures they have in place to protect this data, and they should ensure they are adhering to their own Retention Policy. It is important to note a school must consider **all** records held, including physical and digital copies.

If records are deemed to no longer be necessary, a school must follow a method of secure deletion. It is important that schools opt for secure methods such as shredding or engaging with a third-party disposal company. Disposing of records in public bins is not considered a secure method of deletion.

4. I have a consent form that covers all scenarios where parental consent may be required during the year, is this sufficient for lawful processing?

The first thing to note is that schools need to be sure that consent is an appropriate legal basis for them to rely on for a particular processing activity. In line with Article 7 of the GDPR, in order for consent to be valid it must be **freely given** and **possible to withdraw**.

While a school may seek consent from parents at the start of the school year for certain processing activities, for example taking photographs, processing information in order to attend P.E. classes provided by a third party, a school must consider whether those processing activities are likely to change during the year and whether further consent from parents may be required.

⁷ There are exceptions to the rule on Storage Limitation as provided for in Article 5(1)(e). A data controller may hold personal data for longer than is necessary if it is keeping it for the public interest, archiving, scientific or historical research, or statistical purposes. However, controllers must be able to justify their reliance on these provisions.



Remember – under the GDPR there is no such thing as bundled consent.

For example: A school has organised a trip to an adventure centre. They must be aware that the written consent a school receives for the child to attend the trip is **not** the same consent required to disclose the child's personal data to that adventure centre, should information be required by them. As provided for in Article 7(2) of the GDPR, consent must be clearly distinguishable and schools must consider this in order to comply with its obligations under the GDPR.

Specifically, Article 7(4) of the GDPR seeks to ensure that the purpose of personal data processing is not disguised nor bundled with the provision of a contract of a service for which these personal data are not necessary. This is not to say that a single document cannot be used to cover consent, rather that the form must very clearly distinguish between each individual topic the parent/data subject is consenting to. For example the consent to attend a school trip does not also imply consent to post photographs taken of that child on the school trip online. Separate, explicit consent (possibly acquired with separate signatures for each topic that requires consent) should be required even if a single consent document is issued.

If a school is seeking to rely on consent as its lawful basis for processing under Article 6 of the GDPR, the school must ensure consent is obtained in accordance with Article 7 of the GDPR.

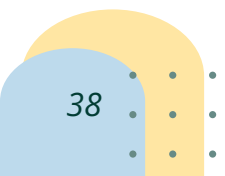
If it is not possible for a parent or where applicable the child to withdraw consent, then consent is not the correct legal basis to be relying upon in the first place. Schools must give careful consideration to their legal basis for processing.

5. What constitutes a data breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Schools should be aware that a personal data breach can cover a lot more than just 'losing' personal data. Personal data breaches include incidents that are the result of both accidents (such as sending an email to the wrong recipient) as well as deliberate acts.

A personal data breach occurs in incidents where personal data are lost, destroyed, corrupted, or illegitimately disclosed. This includes situations such as where someone accesses personal data or passes them on without proper authorisation, or where personal data are rendered unavailable through encryption by ransomware, or accidental loss or destruction.

A school is obliged to notify the DPC of any personal data breach that has occurred, unless they are able to demonstrate that the personal data breach is unlikely to result in a risk to the rights and freedoms of the individual. This places the obligation on the school to assess the risk associated with the personal data breach that has occurred. If a school establishes that a breach may result in a risk to the rights and freedoms of



data subjects, the school must notify the DPC without undue delay, not later than 72 hours from when it became aware of the breach. NB: This 72-hour time-period applies even in instances where schools are closed for holidays.

For more information please see our guidance note, ["A Quick Guide to GDPR Breach Notifications"](#).

6. A data breach has occurred in our school, what do we do?

Firstly, the school must assess the risk associated with the personal data breach and consider whether the personal data breach is likely to result in a risk to the rights and freedoms of individuals. If the school establishes that a breach may result in a risk to the rights and freedoms of data subjects, the school must notify the DPC without undue delay, not later than 72 hours from when it became aware of the breach. It is important to note that once a risk is identified, whether high or low, the school must notify the DPC without undue delay.

[The DPC's breach notification form can be found on our website.](#)

Example:

We've accidentally sent the school report of a child to another child's parents – what should we do?

In assessing the risk associated, a school should consider factors such as:

- When did the school become aware that a personal data breach occurred?
- What information was shared with the incorrect recipient i.e. did it contain any sensitive data relating to a child (like a psychological report)?
- Has the school contacted the incorrect recipient about the personal data breach and requested deletion?
- Has the school followed up with the incorrect recipient to confirm deletion of the email?
- Has a risk to the rights and freedoms of the affected individual been identified? If yes, the DPC must be notified
- If such risk was identified as a high risk to the rights and freedoms of the individual whose personal data was breached, the individual must be notified by the school.



It is important to note this distinction – if any form of risk has been identified, be it high or low, the DPC **must** be notified (in other words, this is a legal requirement which schools must adhere to). However, if a **high** risk is identified, the school is obliged to notify the individual affected as well.

Schools will likely have additional considerations to those highlighted in the example above and it is therefore best practice for schools to draft a **Data Breach Procedure Policy** to ensure procedures are in place for reporting and responding to a data breach.

7. We have experienced repeated incidences of anti-social behaviour on the school premises and are considering installing CCTV cameras – can we do this?

Schools should be aware that footage or images containing identifiable individuals captured by CCTV systems are personal data for the purposes of data protection law. Before making the decision to implement a CCTV system, schools should consider, amongst other things:

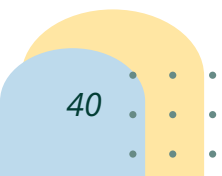
- whether they have a clearly defined purpose for installing CCTV in or around the school;
- What their legal basis is for the use of CCTV under Article 6;
- Whether they can demonstrate that the CCTV is necessary to achieve its stated purpose
- Whether they can demonstrate that the use of CCTV is proportionate for its stated purpose;

Schools must be particularly mindful that where CCTV is capturing images of children, a higher threshold of protection would be required owing to the fact that children merit specific protection under the GDPR.

A Data Protection Impact Assessment (DPIA) should be carried out before any processing commences. By conducting a DPIA, a school can identify and mitigate against any data protection related risks arising from the installation of CCTV, which may affect the school or the individuals it engages with, and in turn can ensure and demonstrate that the school is in compliance with the GDPR.

[For more information on DPIAs, please find the link to our guidance on our website](#) and additionally, please see our “DPIA Template” on page 66

[For more information on CCTV for data controllers, you can find guidance on our website.](#)



8. The Gardaí have contacted our school requesting a child's personal data, are we obliged to provide this information?

Schools have a mandatory obligation under certain legislation to share personal data with third parties under specific circumstances.

Section 41 of the 2018 Act provides for processing for a purpose other than the purpose for which data has been collected. Section 41(b) permits a data controller to disclose personal data to a third party for a purpose other than the purpose for which it was collected where “**necessary** and **proportionate** for the purposes of preventing, detecting, investigating or prosecuting criminal offences”. In line with our guidance, in order for a school to determine what is necessary and proportionate to provide the requested data, it is likely that the school will need to know the legal basis being relied upon and the purpose for which the data is being requested in the first instance. Additionally, in order to ensure compliance with Section 41 of the 2018 Act, it is best practice for the school to seek the Gardaí's request in writing.

The school must be satisfied that the personal data being requested is covered by the relevant provisions being quoted by the Gardaí and that the information being provided by the school is necessary and proportionate for the stated purposes of processing.

9. How long does a school have to respond to a subject access request?

Article 12(3) of the GDPR states that a data controller shall provide information, to the data subject, on action taken under an Article 15 request without undue delay and within one month of receipt of the request.

The GDPR does allow for this period to be extended by a further two months where necessary, taking into account the complexity and number of the requests. If a school is seeking to extend the period, they must inform the data subject of same within one month of receipt of the request along with reasons for the delay.

It is important to note that the one-month timeframe specified in Article 12(3) of the GDPR applies to all data subject rights under Articles 15 to 22 of the GDPR, not just to subject access requests.

For more information please see our “SAR Checklist” on page 52. Please see also our detailed guidance piece on [Subject Access Requests: A Data Controller's Guide](#).

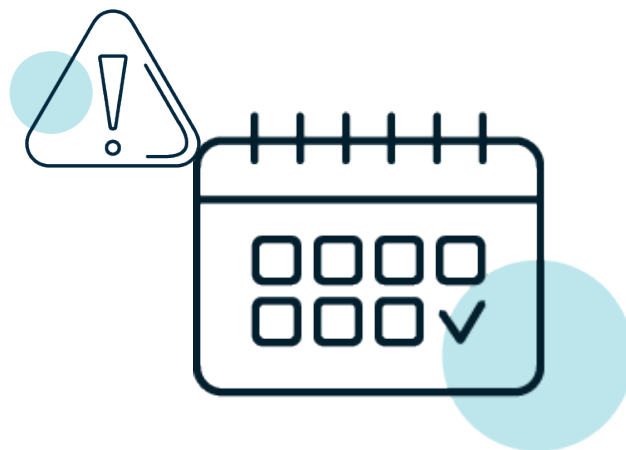


10. The school is closed for holidays and we cannot respond to Subject Access Requests during this time – is this ok?

No. As specified in Article 12(3) of the GDPR, the maximum time limit to provide information on the action taken on an access request, is one calendar month from receipt of the access request from data subjects. This applies even if the request was received on a weekday or holiday.

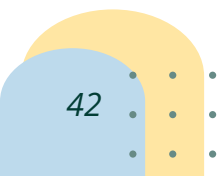
This time limit can be extended by up to two further months, however the data subject must be notified of such extension within one month of receipt of the request along with the valid reasons for the delay.

For this reason and to ensure a school does not fail to fulfil its obligations under Article 12(3) of the GDPR during school holidays, it is best practice that the school's inbox/post is checked regularly even during school holidays.



11. Can a child submit a SAR, or do we need permission from their parent/guardian?

Yes, in principle a child can submit a SAR and schools can respond to the child directly provided they are satisfied that the child understands what exactly it is they are asking for, and provided the school is satisfied that giving them this information would be in their best interest. As a matter of best practice, schools should consider encouraging children to make SARs with the support of a parent/guardian, where possible. For more information on children exercising their own rights, see Chapter 4 of the DPC's [Fundamentals for a Child-Oriented Approach to Data Processing](#).



12. A Leaving certificate student submitted an access request to the school for their results the day after one of their exams. The results won't be prepared within the statutory timeline. What do we do?

Schools might find it useful to be aware of the provisions of Section 56 of the Data Protection Act 2018 ("**2018 Act**") which provides for the right of access to results, examination scripts and results of an appeal. This is likely to be more relevant to secondary schools.

Article 15 access requests made in relation to examination results (or scripts completed during the course of an examination), are taken to be made on the later of (a) the date of the first publication of the results **or** (b) the date of the request. An Article 15 request for the result of an appeal against an examination is also taken to have been made on the later of (a) the date of the first publication of the results of the appeal **or** (b) the date of the request.

In practical terms, the Leaving Certificate State Examinations are usually held during the month of June and the results released during August. Therefore, if a student made an Article 15 request in June, the request would be taken to have been made in August, when the results were released (as this was the later of the two dates).

For more information regarding Subject Access Requests, please see our "SAR Checklist" on page 52.





13. We have a parent who has withdrawn consent for processing and requested the erasure of their child's personal data from an app used by the school to track their attendance and academic performance – can they do this?

As per Article 7(3) of the GDPR, an individual has a right to withdraw their consent to processing at any time.

In the first instance, schools must carefully consider whether consent is the appropriate legal basis to rely upon for such processing. If the school is not in the position to facilitate the withdrawal of consent for a certain processing activity, then consent is not the appropriate legal basis upon which to base this type of processing. The school should consider whether one of the other five legal bases under Article 6 is more appropriate and be able to demonstrate this.

The right of erasure applies in the following specific scenarios:

- Where personal data are no longer necessary in relation to the purpose for which it was collected or processed.
- Where a data subject withdraws their consent to the processing and there is no other lawful basis for processing the data.
- Where a data subject objects to the processing and there is no overriding legitimate grounds for continuing the processing;
- Where a data subject objects to the processing and their personal data are being processed for direct marketing purposes;
- Where a data subject's personal data have been unlawfully processed.
- Where a data subject's personal data have to be erased in order to comply with a legal obligation.
- Where a data subject's personal data have been collected in relation to the offer of information society services (e.g. social media) to a child.

Schools should note that the right to erasure under Article 17 of the GDPR is not an absolute right and does not apply where processing is necessary for reasons specified in Article 17(3)⁸ of the GDPR and Section 60 of the 2018 Act. If, having assessed the request and determined that one of the exemptions under Article 17 apply, the school must inform the data subject of same along with reasons for that decision.

For the reasons outlined above, a school must assess Article 17 requests on a case-by-case basis.

⁸ The right to erasure does not apply where processing is necessary for: exercising the right of freedom of expression and information; compliance with a legal obligation; the performance of a task carried out in the public interest or in the exercise of official authority; reasons of public interest in the area of public health (See Article 9(2)(h) & (i) and Article 9(3), GDPR); archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; establishment, exercise or defence of legal claims.

14. We have a parent who is seeking rectification of their child's school report, how do we respond to this?

Under Article 16 of the GDPR, if personal data is inaccurate, an individual has a right to have the data rectified, by the controller, without undue delay. Furthermore, if an individual's personal data is incomplete, they have the right to have the data completed, including by means of providing supplementary information.

However, the right to rectification is not an absolute right and will depend on the specific circumstances of each request for rectification and the "purposes of the processing" of the personal data as defined under Article 16 and 5(1)(d) of the GDPR.

In order for Article 16 to apply, the personal information being processed by a data controller must be inaccurate as to a matter of fact. Where the information is opinion-based, or where a data subject simply does not agree with the content of information being processed, the right to rectification would likely not apply.

As with all rights, the right to rectification can be lawfully restricted by the data controller, for example, under Section 60 of the 2018 Act. However, data controllers must ensure they specify precisely which provision they are relying upon to restrict this right and the data subject has a right to be informed of the relevant provision restricting their rights in the event they wish to raise further queries on the restriction.

For the reasons outlined above, a school must assess Article 16 requests on a case-by-case basis.



Top tip: any students looking for clarification on their own data protection rights can avail of our [comprehensive collection of guidance for children!](#)





15. As a school, what kind of policies should we have in place that would help us with our data protection obligations?

It is important that a school's policies and procedures provide individuals with clarity and consistency, by communicating what people need to do and why. The GDPR requires the implementation of appropriate data protection policies but does not expressly state which policies apply.

The most important policies for schools to consider are its Privacy Policy and its Retention Policy. Other policies a school may consider drafting are:

- CCTV Policy
- ICT Policy
- Personal Devices Usage Policy (where appropriate)
- Subject Access Request Policy
- Admissions/Enrolment Policy

When drafting any of the policies outlined above, a school must consider the data protection principles under Article 5 of the GDPR. Data controllers should also be aware that such policy documents which relate to the processing of personal data are live documents. For that reason they ought to be kept under regular review and updated accordingly.



16. Are teachers allowed to use their own personal devices to conduct their work?

While teachers are not prohibited from using their personal devices to carry out their work, an enhanced level of consideration and security must be considered.

Article 24 requires a school to implement appropriate technical and organisational measures in order to safeguard personal data. For this reason, schools should promote the use of school devices and work email accounts as opposed to personal devices and personal email accounts as the school retains a level of control over such devices.

For more information, please see "Use of Technology in Schools" on page 34. Please see also the [DPC's guidance on Data Security](#).

17. Is there anything under data protection law that prevents children from taking photos of each other in school and posting them online?

Data protection law does not prohibit the taking of photographs or video recordings. However, it's what you do with that photo or video that can potentially become a data protection issue.

Article 2(2)(c) of the GDPR states that data protection law does not apply to the processing of personal data where data is kept by an individual and is concerned solely with the management of his/her personal, family or household affairs or kept by an individual for recreational purposes. This is more commonly known as the **"household exemption"**. In other words, GDPR does not apply when a person processes personal data (for example, a photograph of someone) in the course of a purely personal or household activity, e.g. with no connection to a professional, business, official or commercial activity.

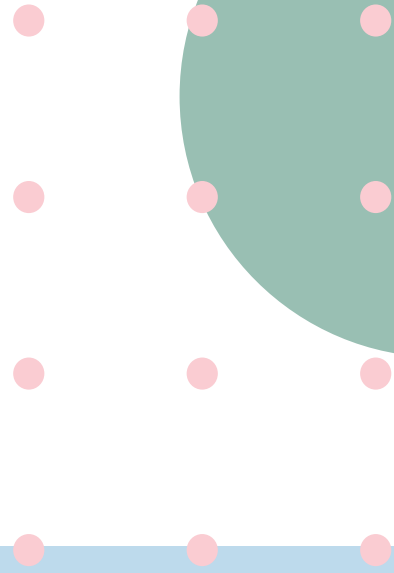
A lot of the time students taking photographs of themselves or with friends in schools are simply doing so for social purposes. However, the ubiquitous nature of the social media means that many photos like these will inevitably wind up on someone's social media profile. And in fact, the GDPR doesn't strictly prohibit this either, with Recital 18 stating that personal or household activities could include "social networking and online activity". However, if a student published a photo of their classmate online and the other student or parent of the other child was uncomfortable with this and asked that the photo be taken down, common courtesy would suggest that they should take the photo down.

In an effort to maintain a sense of control over this situation, some schools are implementing an outright ban on the taking of photographs at school. It is at the discretion of schools to create their own policies on these matters, and it may be beneficial for such policies to outline the school's position on the use of devices on the premises and to inform students of risks, rights and routes for redress available to them in these situations.

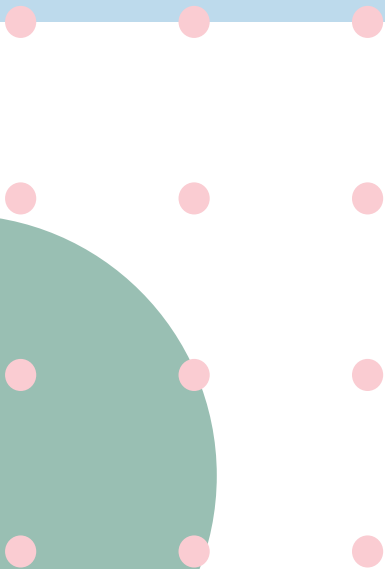
For more information on data protection in relation to children, please see:

- [Guidance for children on their data protection rights](#)
- [Children, Parents and Data Protection: Can I make a complaint on behalf of my child?](#)
- [Fundamentals for a child-oriented approach to data processing](#)
- [Guidance on Taking photo's at school events – Where common sense comes into play](#)
- [Guidance on My Child's Data Protection Rights](#)
- [A Consultation by the Data Protection Commission on the Processing of Children's Personal Data and the Rights of Children as Data Subjects under the General Data Protection Regulation](#)

[illegible]



Resources



Schools and subject access requests

Article 15 of the GDPR gives individuals (data subjects) the right to **request a copy of any of their personal data** which are being processed by data controllers. These requests are often referred to as “subject access requests” or SARs for short.

The DPC receives many queries from schools each year in relation to SARs and how to deal with them. As this appears to be an area of uncertainty, the DPC has developed this brief guide to assist schools in responding to SARs but it should not be viewed in isolation. Schools should still consult the primary legislation when drafting any internal policies for responding to these requests, specifically Articles 4, 12 and 15 of the GDPR. The DPC also recommends schools familiarise themselves with the DPC’s detailed guidance on [Subject Access Requests: A Data Controller’s Guide](#).

Guidance on Subject Access Requests: A Data Controller’s Guide



Subject access request (SAR) policy

As a matter of best practice, schools should consider having a SAR Policy in place and setting up a dedicated inbox through which they can receive GDPR requests. This contact information should feature in the school's Privacy Policy and should be readily accessible to students, parents and staff members.

It is important that a school, as a data controller, takes a consistent approach when responding to SARs, which is why having a SAR policy in place is so important. At a **minimum**, the SAR policy should include information on:

- how individuals can go about submitting a SAR,;
- who in the school is responsible for dealing with SARs;
- the procedure for gathering the information requested by the individual, and;
- the procedure for providing that information to the individual.

While a school may choose to provide a standardised form for making a SAR, an individual does not have to complete that form if they do not want to. Schools must remember there is no prescribed format for submitting a SAR under the GDPR or the 2018 Act and such requests can be received by post, email or even made verbally. Schools cannot refuse to respond to a SAR because it was not submitted in their preferred format.

How long do we have to respond to a SAR?

Schools who receive a SAR must respond to the request without undue delay and at the latest **within one month of receiving the request**.

Schools can extend the time to respond by a further **two months** if the request is **complex** or they have received a **number of requests** from the **same individual**, but they must still contact the individual within one month of receiving their access request and explain to them why they consider the extension is necessary. Please note, the fact that schools might be closed for holidays **is not a valid reason** for not responding to an access request within the required one-month timeframe. It is the responsibility of the school to ensure that email inboxes, post or phones are regularly monitored so as to ensure that no SARs or other data protection requests go unanswered.

If a school is unsure about the particulars of a request, they can revert to the individual to ask what specific data they are requesting. This will not be necessary in all cases but if an access request is vague or particularly broad, etc. the school can seek clarity from the requesting individual.

Essentially schools have one month, from the date of receipt to respond to the individual, be it a substantive response to the SAR or an acknowledgement of receipt and explanation of why additional time is needed to respond.

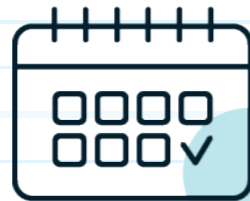
SAR Checklist

Below is a "checklist" for schools to assist them when responding to a SAR but please note, it is **not a definitive list**. Each request will have considerations that are unique to that request which must be taken into account.

1) We've just received a SAR - what are the first things we need to consider?

✓ *When was the SAR received?*

➤ *A response must be issued within one month of the date of receipt.*



✓ *Are there any reasons why the school won't be able to respond to the SAR within one month?*

➤ *If not, you must ensure to meet the one month time-frame*

➤ *If yes, you must contact the individual to notify them of the two-month extension and also provide them with a reason for the delay, which is only permissible under very limited circumstances e.g. either the complexity of the request and/ or the number of requests made by an individual.*

✓ *Who is making the request?*



➤ *If an individual is making a SAR on behalf of a child⁹, you should ask yourself the following questions –*

* *Does that individual have a right to act on behalf of the child? E.g. are you satisfied that this individual is the child's legal guardian and should receive the child's personal data?*

* *Are you satisfied that the individual submitting the request is acting in the child's best interests? Or is the individual pursuing another purpose or interest in seeking to exercise these rights?*

* *Are you satisfied that the release of the data to the individual would be in the child's best interests¹⁰? E.g., would allowing the parent(s)/ guardian(s) to exercise the child's data protection rights cause harm/ distress to the child in any way?*

Continued

9) The DPC notes that Section 9(g) of the Education Act 1998 states that a school shall ensure that parent(s) (or in the case of a student who is 18 years, the student themselves) shall have access to records kept by the school regarding the student's educational progress. This should be taken into account when a SAR relates to documents relating to educational progress.

10) The DPC notes that as a matter of Irish law, there is a rebuttable presumption that a parent/ guardian is acting in the best interests of their child unless there is evidence to the contrary.

* Was the information that is being sought, provided or shared by the child to the school in confidence and is there a duty of confidence owed to the child?

* Are there any court orders relating to parental access/ responsibility/ custody/ child protection etc. in existence that might prevent a parent acting on behalf of their child?;

* In the event of doubt in terms of the identity of the individual making the request, you should consider what reasonable steps need to be taken to verify the identity of the individual.



➤ If it is a child¹¹ making the request themselves, you should consider the following criteria when deciding whether to provide the child with the information themselves:

* The age and maturity of the child: do you consider that the child has the capacity to understand their data protection rights and what they are requesting?

* The type of personal data at issue: the DPC considers that in cases where the exercise of a child's data protection rights involves access to special category personal data, particularly such as medical data, or access to other sensitive types of data, such as social work data, that careful consideration should be given to whether the release of such personal data could cause serious physical or mental harm to the child in question.

* Whether enabling the child to exercise their data protection rights themselves is in the best interest of the child (i.e. will they fully comprehend what it is they are receiving as part of an access request, will receiving certain information be detrimental to their well-being?)

For more detailed guidance on what to do when a child seeks to exercise their own data protection rights, please see the DPC's guidance on [The Fundamentals for a Child-Oriented Approach to Data Processing](#)



11) There is no national law in Ireland which specifies the age at which children have a legal right to exercise their rights as a data subject. The DPC does not consider that it is appropriate to set a general age threshold as the point at which children should be able to exercise their rights on their own behalf. That being said, while age alone is not the most appropriate benchmark, it should certainly be taken into consideration in conjunction with a number of other criteria.

✓ How was the SAR received?



- This will be important to determine the way in which the school responds to a SAR. It is best practice to respond to a SAR in the same manner it was received. E.g. if a SAR was received by email, you should reply via email as opposed to post.
- Having regard to the above, you should consider how to securely disclose information to the individual e.g. password-protected email/USB stick/registered post.



2) What do we need to consider when conducting a search?

✓ Firstly, do you hold personal data in relation to the data subject?

✓ Is personal data held in hard and/or soft copy?

✓ Do you need to conduct a search of school email inboxes?

✓ Do admin staff need to manually go through files in the office to extract the relevant materials?

✓ How many teachers will you need to contact in order to comply with this SAR? (Note, this will differ between primary schools (possibly 2/3 teachers maximum interacting with the child in question) and post-primary schools (likely to be one teacher per subject))

✓ Ask teachers to consider all places where personal data may be held e.g. work phones, laptops, filing cabinets, notebooks, applications.

3) What kind of information is the individual entitled to receive in response to their SAR?

- ✓ Look at each document and determine whether it is personal data under Article 4 of the GDPR – make this decision on a case-by-case basis.



- ✓ If a document is deemed not to contain personal data, then it does not need to be considered further.

- If a document is deemed to contain personal data, it should be provided to the requesting individual, unless an exemption applies.



4) Are any of the restrictions under Section 60 of the 2018 Act applicable?

- If you are relying on such restrictions, the reasons for that refusal must be set out in a written notice to the individual.

- The DPC's detailed guidance on Subject Access Requests: A Data Controller's Guide provides information on when a SAR can be refused or restricted.

5) Does the request include information about other people?

Article 15(4) of the GDPR highlights that an individual's right to access relates to their personal data **alone** and does not provide the individual the right to access full copies of documentation, which contains the personal data of others. In other words, if a child (or a legal guardian on behalf of their child) makes a SAR, they are only entitled to receive the child's personal data and not the personal data of others (e.g. other students or teachers).



The right to obtain a copy of one's personal data should not adversely affect the rights of others and it is therefore important that schools consider the below.

✓ Does any third-party information need to be redacted?

✓ Is it necessary to carry out manual redactions where soft copy files are subject to release as part of a SAR?



Each SAR must be assessed on an individual basis. Each request will have unique factors that schools must give due regard, but the above "check-list" can be consulted and used to guide you to help you respond to these requests and draft internal policies.



Privacy policies –

What kind of information does my school need to include?

Schools have an obligation under data protection law to **provide individuals**, whose personal data they collect, **with specific information** such as what personal data they are collecting, the reasons why, their lawful basis for doing so, and how long they will keep this information, amongst other things. This information is often provided in the form of a "privacy policy".

A privacy policy is an accountability tool that helps a data controller, e.g. a school, demonstrate that it is compliant with data protection law, in particular in respect of its obligations under the transparency principle (Articles 12 to 14 of the GDPR), and to fulfil the right of data subjects to receive certain information in relation to a data controller's processing operations.

Privacy policies should be written in clear, plain language that is easy for the reader to understand. The GDPR specifically highlights the importance of using simple language where privacy information is addressed to children. Given that schools process children's personal data, they should ensure that their privacy policies are as clear and easy to understand as possible.

The DPC has provided below an overview of the kind of information that schools **must** communicate to individuals in their privacy policies. Please note, the level of detail necessary may vary between schools and additional information may need to be provided to data subjects depending on the individual circumstances of the school and processing activities they engage in. Privacy policies should cover information about **all** data processing activities by the school, including information collected through things like extra-curricular activities, sports, afterschool clubs, school trips, etc.

Who is the data controller?



You must provide information about **who** the data controller is and their **contact details**. Schools as an entity are data controllers, and should designate an official point of contact for data protection queries.

You must also provide contact information for your school's **Data Protection Officer**, if you have one.

What kind of personal data are you processing?



You must provide information on the **types of personal data** that you are processing, e.g. personal data about academic performance, health information, emergency contact information, etc. Be clear about all types of information you're collecting, particularly if it's information that people wouldn't necessarily expect you to be collecting.

Also, if you didn't get the personal data directly from the data subject themselves, you need to tell them where the data came from.

Why are you processing data?



You need to explain the **reasons** why you are processing personal data, and the **legal basis** you are relying on under Article 6 (and Article 9 where applicable) of the GDPR. You may be relying on more than one basis, so make sure to include them all.

If your school is relying on **legitimate interest**, you need to explain what exactly this legitimate interest is.

If your school is relying on consent as a legal basis for any processing activity, you must make it clear to parents/children that they can withdraw this consent at any time, and you must tell them how they can do this.

What about consent?



If your school is relying on consent as a legal basis for any processing activity, you must make it clear to parents/children that they can **withdraw this consent at any time**, and you must tell them **how** they can do this.

Consent should be as easy to withdraw as it was to give in the first place, so schools must ensure they have a mechanism in place for handling these requests.

Who will this data be shared with?

You must provide individuals with information about the **recipients** of any personal data you collect.

In other words, you have to clearly state if you will be disclosing this personal data to anyone, and if so, to whom? For example, another public authority, agency or other body.



Will this personal data be transferred outside the EEA?



You must inform individuals if their personal data is going to be transferred outside the EEA, either by your school or by any third party service providers your school might use.

You also must provide details on the safeguards being applied to protect this personal data.

How long will data be kept for?



You must inform individuals **how long** you are going to keep their data for, and importantly, **why**. Sometimes the reasons for this might be set out under other law to which schools are subject. It's important to be really clear about this and why you are keeping data for a specified period of time.

This information can be further explained in your school's Retention Schedule that should outline the different time periods for retaining different types of data.

What rights do data subjects have?



You must inform individuals of their data protection rights, e.g. their right of access, their right to rectification, their right to erasure, etc.

You must also explain how they can go about exercising these rights. For example, you can provide them with a contact name and email address where they can submit data protection requests. You could also provide a link to your school's Subject Access Request Policy, where applicable.

Are you profiling or making automated decisions?

You need to tell individuals if your school will be processing their personal data to profile them or make any automated decisions about them, and what impact this will have on them.

Processing is "automated" where it is carried out without human intervention and where it produces legal effects or significantly affects an individual.



Individuals have the right to not be subject to a decision based solely on automated processing.

Making a complaint to the DPC



You must inform individuals that they have a right to lodge a complaint with the Data Protection Commission if they have any concerns about how you are processing their personal data.

So consider adding the DPC's phone number and a link to our website in your privacy policy to make things easier for individuals.

Data Protection Impact Assessments



What is a Data Protection Impact Assessment?

A Data Protection Impact Assessment (DPIA) describes a process designed to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible. If required, a DPIA must be completed **before** the relevant data processing has commenced. Article 35 of the GDPR states that a DPIA **must** be carried by a controller where a type of data processing, in particular using new technologies, is likely to result in a **high risk** to the rights and freedoms of individuals. The GDPR also sets out a number of specific instances in which controllers must conduct a DPIA.

DPIAs are important tools for negating risk, and for demonstrating compliance with the GDPR. As a controller, your school needs to make sure that a DPIA is carried out where this is appropriate. An initial assessment of the risk arising from data processing, using the checklist on the next page, can indicate whether a DPIA is likely to be necessary before introducing a new technological solution or method of working. When making this assessment, schools should take into consideration that the vulnerability of children is often indicative of a higher level of risk arising from the processing of their personal data.

While DPIAs may not always be mandatory for all types of processing that a school may carry out, they may still serve as a useful tool for schools to demonstrate compliance with the GDPR. DPIAs can help schools to document how their processing is both necessary and proportionate, and demonstrate that they have considered the risks involved in their processing of personal data and taken relevant steps to mitigate against these risks.

An example of a scenario that would likely trigger the need for a DPIA is the implementation of a CCTV system in a school, covering more than just public areas.



What kind of information should a DPIA cover?

The DPC has included on the following pages a sample template of the kind of information that a DPIA should include and how to record it. This template should be read alongside our dedicated [DPIA guidance](#), as well as the [criteria for an acceptable DPIA](#) set out in European guidelines on DPIAs.

You should start to fill out the template at the **beginning** of any major project involving the use of personal data, or if you are making a significant change to an existing process.

PLEASE NOTE, THIS TEMPLATE HAS BEEN PROVIDED BY THE DPC FOR ILLUSTRATIVE PURPOSES ONLY. THIS TEMPLATE DPIA IS NOT TAILORED FOR EVERY INSTANCE IN WHICH A DPIA MAY BE REQUIRED. SCHOOLS ARE ULTIMATELY RESPONSIBLE FOR ENSURING THAT ALL APPROPRIATE, RELEVANT INFORMATION IS INCLUDED IN ANY DPIA THEY CARRY OUT.



School information

Name of school	St Mary's National School, Co. Longford.
Title of DPIA	<p>E.g.</p> <p>DPIA for use of new CCTV system in St Mary's National School</p> <p>DPIA for the use of new software for tracking incidents/accidents on school premises</p>
Name of DPO/school contact for data protection issues	John Smith
Contact no./email	<p>087 – XXX XXXX</p> <p>dataprotection@stmarysns.com</p>
Third parties involved/associated with the project (e.g. other schools, agencies, departments, service providers, etc.)	

Does my school need to do a DPIA?

Does your project involve any of the following¹²: The DPC has highlighted below in green the scenarios most likely to trigger the need for a DPIA in the context of schools, but this does not mean that the other criteria do not apply . It is for schools to make that assessment.	Yes	No
Evaluation or scoring of personal data (including profiling and predicting)		
Processing that aims at taking automated decisions about data subjects producing “legal effects concerning the natural person” or which “similarly significantly affects the natural person” (Article 35(3)(a))		
Systematic monitoring, including of a publicly accessible area		
Sensitive data or data of a highly personal nature (including special categories of data {Art. 9(1)} and criminal data {Art 10})		
Data processed on a large scale (criteria to take into account could include the no. of data subjects, volume of data, duration of processing, geographical extent)		
Datasets that have been matched or combined		
Data concerning vulnerable individuals (including children, the mentally ill, asylum seekers, the elderly, patients)		
Innovative use or applying new technological or organisational solutions		
Processing that prevents data subjects from exercising a right or using a service or contract		
Use of personal data on a large-scale for a purpose(s) other than that for which it was initially collected pursuant to Article 6(4) GDPR		

¹²) This checklist is based on criteria provided by the European Data Protection Board in its guidelines on [Data Protection Impact Assessments](#), as well as criteria set down by the Data Protection Commission in its [List of Data Processing Operations which require a DPIA](#).



Profiling vulnerable persons including children to target marketing or online services at such persons		
Use of profiling or algorithmic means or special category data as an element to determine access to services or that results in legal or similarly significant effects		
Systematically monitoring, tracking or observing individuals' location or behaviour		
Profiling individuals on a large-scale		
Processing biometric data to uniquely identify an individual or individuals or enable or allow the identification or authentication of an individual or individuals in combination with any of the other criteria set out in WP29 DPIA Guidelines		
Processing genetic data in combination with any of the other criteria set out in WP29 DPIA Guidelines		
Indirectly sourcing personal data where GDPR transparency requirements are not being met, including when relying on exemptions based on impossibility or disproportionate effort		
Combining, linking or cross-referencing separate datasets where such linking significantly contributes to or is used for profiling or behavioural analysis of individuals, particularly where the data sets are combined from different sources where processing was/is carried out for different purposes or by different controllers		
Large scale processing of personal data where the Data Protection Act 2018 requires "suitable and specific measures" to be taken in order to safeguard the fundamental rights and freedoms of individuals		

Step 1: Give an overview of the purpose of this project

What is your school aiming to achieve with this project?	
What type of processing is involved?	
Why have you identified the need for a DPIA ? (See checklist above). E.g. are you processing children's personal data? Is there a high risk involved? To whom? Why? Is processing being carried out on a large-scale?	
Links to supporting documenting (if any) (e.g. project proposals, reports, pieces of legislation that require this high-risk processing, etc.)	



Step 2: Describe the processing (nature/scope/context/purpose)

Nature of the processing	
How will your school collect, store, use and delete personal data as part of the project? Please provide details.	
Where has the data been sourced from /collected from? E.g. directly from parents/children, from the Dept of Education, from another database?	
Will your school be sharing this data with anyone else? E.g. other schools, government departments, agencies, third party providers, etc. If so, who and for what purpose?	
What types of processing identified as likely to be high risk are involved?	
Scope of the processing	
What categories/types of personal data will be collected? E.g. data relating to admissions, data relating to a child's attendance/progress at school, photos/videos of children, etc.	
What type of data subjects are involved? E.g. children, parents, school employees, the general public, etc.	
Does the project involve the processing of any special category data (Article 9 GDPR) or data relating to criminal convictions or offences under Article 10 of the GDPR? E.g. medical information about students, personal data revealing religious beliefs of individuals, results of Garda vetting, etc.	
How much data will you be collecting and how often will you be collecting it?	
How long will you keep the data for? And why ? (e.g. if you have to keep information for a specific number of years because a piece of legislation requires this, please explain this and reference the section of the legislation)	
How many individuals are affected by this processing?	
What geographical area does the project cover? (e.g. are you using any third-party providers who store personal data outside the EEA?)	
What kind of technology will be involved with processing the data? Is it novel in any way?	

Context of the processing

What is the nature of the school's **relationship** with the data subjects whose data is being processed? E.g. are the data subjects pupils/staff of the school?

How much **control** will these individuals have over their data? E.g. will there be any restrictions on their ability to exercise their data protection rights?

Would they **expect** the school to use their data in this way?

Do the data subjects include **children** or other **vulnerable groups**?

What **technical measures** will be in place to secure the data? (e.g. laptops/desktops encrypted and password-protected, restricted access to databases/systems, hard copy files/handwritten notes securely stored away in locked filing cabinets at the end of each day)

What **organisational measures** will be in place to secure the data? (e.g. GDPR training for all staff, data breach protocols in place, ICT usage policy, access management policy)

Are there any **prior concerns** over this type of processing (e.g. in terms of security) or **issues of public concern** that your school needs to factor in?

Purposes of processing

What does your school **want to achieve** by processing this personal data?

What **impact/effect** will this processing have on individuals?

What are the **benefits** of the processing? Both to your school and to data subjects more generally?

What is your **legal basis** for processing this personal data? E.g. which of the 6 legal bases under Article 6 GDPR (and Article 9 if you are processing special category personal data) are applicable in this case? If you are processing data to comply with a legal obligation, please specify the specific provisions/sections of the primary legislation.

Does processing this personal data help you to **achieve your intended purpose**? Please explain how you've come to this decision.



Is there any other way you could achieve this purpose that does not involve processing this personal data? Please explain.	
How will you ensure that this personal data is not used for any other purpose than the one for which it was originally processed? (e.g. if you are processing personal data to create a school yearbook and you told students this was the reason why you were collecting their information, how will you make sure that you don't use this same personal data for another project?)	
How will you ensure that the data remains accurate and up to date ?	
How will you ensure that you only collect the minimum amount of data required for the purposes of the project?	
What information will you give individuals about the processing of their data and their data protection rights (e.g. in the context of a Privacy Policy)? If the data subjects are children, schools should note that children have a right to this information and it should be provided to them, where feasible taking into account their age and capacity, in clear, concise language that they can easily understand.	
What measures do you take to ensure processors (e.g. third-party software providers) comply with their obligations?	

Step 3: Consult with stakeholders

You should consult with internal stakeholders with a view to identifying the technical aspects of information collection, storage and processing, and how the different elements of the project will fit together in operation. You may also want to consult with external partners, who may be engaged by your organisation as a data processor, or to whom information might be disclosed as part of a project.

It is also advisable to consult with children and parents as appropriate. Seeking their views at the DPIA stage can give parents and children an opportunity to voice their concerns about a particular project before it goes live and gives the school the opportunity to mitigate any risks that might be highlighted by them. It can also greatly assist the school with its transparency obligations.

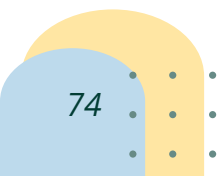
How and when will you consult with individuals (data subjects) to obtain their views?	
Is there anyone else internally within the school that needs to be consulted?	
Are there any external stakeholders that should be consulted ? (E.g. service providers engaged by the school as a data processor, or other organisations to whom information might be disclosed as part of the project?)	



Step 4: Identify the risks posed and the mitigating measures to be applied

This section identifies the potential risks posed to individuals (or more broadly) as a result of your school's proposed processing activities. Article 35 GDPR requires data controllers to **identify** and **assess** any potential risks to the rights and freedoms of data subjects and to **identify the measures** envisaged to **address these risks** (e.g. safeguards and security measures and mechanisms). The DPC has provided an example below for assessing risk, which schools can feel free to adjust as they see fit (e.g. add more categories, adjust the weighting, etc.). However, please be advised, this is just an example.

Likelihood of risk occurring	
	Highly unlikely - 1
	Unlikely - 2
	Possible - 3
	Likely - 4
	Highly likely - 5
Severity of risk	
	Negligible - 1
	Minor - 2
	Moderate - 3
	Major - 4
	Critical - 5
Overall risk score	
	Very low - 1-5
	Low - 6-10
	Medium - 11-15
	High - 16- 20
	Very high - 21- 25





Risk assessment template

FOR ILLUSTRATIVE PURPOSES ONLY, the DPC has provided an example of **two** risks that **may** occur in the specific context where a school is considering the deployment of a 24/7 CCTV system in a school gym for the purposes of preventing antisocial behaviour. There are a number of additional risks that schools would need to consider, document, assess and for which they would need to implement mitigation measures. **THIS EXAMPLE IS PROVIDED FOR ILLUSTRATIVE PURPOSES ONLY AND DOES NOT PURPORT TO BE COMPLETE, NOR DOES IT IMPLY THAT THE DPC ENDORSES THE DEPLOYMENT OF CCTV IN SCHOOL GYMS.**

Risk No.	Description of risk and the potential impact on individuals	Inherent risk (e.g. without any controls in place): (Likelihood of risk occurring x Severity of risk, e.g. 3 x 4 = 12 = Medium risk)	Description of mitigating measures to prevent risk/reduce risk	Residual risk (e.g. after mitigating measures have been implemented) (Likelihood of risk occurring x Severity of risk, e.g. 2 x 3 = 6 = Low risk)
1	There is a risk that the collection of personal data may extend beyond the confines of the gym to areas where students may have a stronger expectation of privacy (e.g. gym changing rooms).	Likelihood (4) x Severity (4) = 16 – High risk	The school will ensure that cameras are only installed in parts of the gym where changing rooms cannot be captured by CCTV Cameras in the gym will only be turned on during specific periods of the day where there has been a documented track record of serious incidences of antisocial behaviour. Cameras will only be turned on when students are not under the direct supervision of teachers.	Likelihood (2) x Severity (3) = 6 – Low risk
2	The deployment of a 24/7 CCTV system could amount to a level of personal data processing that is excessive, disproportionate and unnecessary.	Likelihood (5) x Severity (5) = 25 – Very high risk	Instead of a 24/7 recording system, cameras in the gym will only be turned on during specific periods of the day where there has been a documented track record of serious incidences of antisocial behaviour. Cameras will only be turned on at times when students are not under the direct supervision of teachers.	Likelihood (2) x Severity (5) = 10 – Low risk



Step 5: Document outcomes and recommendations from DPIA

Item	Name/Title/Date	Comments
Measures to mitigate risks approved by:		Timelines for implementing these measures, parties involved, deadlines
Residual risks approved by:		If your school is accepting any residual high risk (e.g. mitigating measures haven't sufficiently reduced the risk), you will need to consult the DPC before proceeding with your project.

DPO advice (where applicable)

[Provide a summary of the advice received from your DPO on this project and whether you have taken this advice on board. If you haven't, please provide details as to why not.]

Step 6: Sign off on DPIA

Approval decision:	Approved Not Approved Consult with the Data Protection Commission
Approval by:	[Name and title]

Notes

[illegible]



www.dataprotection.ie



21 Fitwilliam Square South
Dublin 2
D02 RD28
Ireland



01 7650100 or 1800 437 737



**An Coimisiún um
Chosaint Sonraí**
Data Protection
Commission