A Guide to UK Data Protection: Education

Introduction

Welcome to your course on **'A Guide to UK Data Protection: Education'** written in partnership with SWGfL – a charity ensuring children benefit from technology, free from harm.

This course is aimed at all staff working within an education setting that deal with personal data.

The purpose of this course is to help you understand:

- what is meant by "personal data" and "data protection"
- the legal requirements for data protection in the UK
- the underlying principles of data protection law
- your responsibilities in an education setting
- the key risks and challenges in an education setting.

Data protection issues are increasingly at the forefront of people's minds. The media frequently cover data breaches of personal information or warn about the extent of social media control over personal information. Consumers are becoming increasingly aware of how their data is used or sold by retailers or service providers.

Parents worry about the privacy of their children in an internet age. Organisations of all types, whether large corporations, small businesses, charities, or public bodies are becoming more and more aware that data protection isn't just a legal requirement but a social responsibility.

The purpose of this course is to give you a basic understanding of data protection as well as to acquaint you with the essentials of data protection requirements in your school. We will discuss practical examples of what is expected as well as some of the key risks that are found in education settings.

The data protection landscape

The availability of information and ease of transfer has changed dramatically over recent decades. Individuals' personal data is moving to and from countries in ways people often don't realise or understand.

For example,

- a person posting a social network picture can mean that the information is transferred from their computer or phone to a server in another country immediately.

- From there, it may be disseminated to hundreds of users in countries worldwide within seconds at a tap of a screen.

- Each person who 'likes' the picture can share or resend the picture to many others with little or no restrictions. Meanwhile, the original picture can be easily modified, saved, shared, or uploaded to any number of other internet sites.

These days, information is not only easily transferred, but also difficult to control.

Whilst Tes Global Ltd have made every effort to ensure that the courses and their content have been devised and written by leading experts who have ensured that they reflect best practice in all aspects, Tes Global Ltd exclude their liability of the consequences of any errors, omission or incorrect statements to the fullest extent permitted by law and Tes Global Ltd make no warranty or representation as to the accuracy, completeness or fitness for purpose of any statements or other content in the course.

Not only is the ease of information sharing a desire for consumers, it’s also big business. Social media companies, retailers, and advertising agencies are just some of the many organisations that benefit from processing the personal data of users, customers, or potential consumers.

The UK GDPR principles

The Data Protection Act 2018 is the main law in the UK. You may also have heard of the General Data Protection Regulation or GDPR. This is a European Union law which has been fully transposed into UK law as the UK GDPR. The laws set out the main data protection obligations for schools and other organisations in the UK.

There are seven key principles which are central to the GDPR. They are fundamental elements for data protection and organisations must ensure that any processing of personal data meets the expectations set out in them. Let’s take a look at the seven principles:

- **Lawfulness, fairness and transparency**
  Personal data must be collected legally and processed in a way that is reasonable, clear and honest.

- **Purpose limitation**
  Personal data must only be collected for specified, legitimate purposes and not processed for a different purpose.

- **Data minimisation**
  This includes ensuring that only the minimal amount of personal data is processed to achieve the organisation’s purposes.

- **Accuracy**
  Personal data must be accurate and kept up to date.

- **Storage limitation**
  Personal data must not be kept for longer than is necessary.

- **Integrity and confidentiality**
  The security of personal data must be maintained to minimise the risk of loss, destruction, or damage.

- **Accountability**
  This includes taking responsibility for how personal data is processed and ensuring that compliance can be demonstrated.

These are *general principles* rather than *specific rules*. For example, ’storage limitation’ means you can only store data for as long as it is needed but the GDPR doesn’t specify how long that should be. Each organisation must determine the appropriate retention period that meets this principle. So, whether it is attendance records, CCTV images, photographs of students, staff sickness records, or the contact information of alumni, schools must decide for themselves the appropriate time limit for keeping the data.

What is meant by data protection and personal information?

Data protection is about making sure that you are being fair and responsible when processing people's personal information. Good data protection practices ensure that an organisation and the individuals within it can be trusted to collect, store, and use our personal data fairly, safely, and lawfully.

Whilst Tes Global Ltd have made every effort to ensure that the courses and their content have been devised and written by leading experts who have ensured that they reflect best practice in all aspects, Tes Global Ltd exclude their liability of the consequences of any errors, omission or incorrect statements to the fullest extent permitted by law and Tes Global Ltd make no warranty or representation as to the accuracy, completeness or fitness for purpose of any statements or other content in the course.

The people whose personal information you are processing could be employees, students, parents, or members of the public. They include people in your country as well as people in other countries. It also includes you and your colleagues, which means that your school should take steps to make sure that your personal data is processed appropriately.

What do we mean by 'personal data'?

Personal data is information that relates to an identified or identifiable individual (data subject). If it is possible to identify an individual directly from the information you are processing, then that information may be personal data.

This covers basic identifiers such as:

- name
- email address
- identification number
- online identifier
- more confidential information such as:
  - salary details
  - disciplinary records
  - bank account information.

In schools, personal data includes:

- information about pupil behaviour and attendance
- assessment and exam results
- staff recruitment information
- staff contracts
- staff development reviews
- staff and pupil references.

If you cannot directly identify an individual from that information, then you need to consider whether the individual is still identifiable. If an individual is identified or identifiable, directly or indirectly, from the data you are processing, it is not personal data unless it 'relates to' the individual.

Certain types of data are recognised under law as special category data and include:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data for the purpose of unique identification
- health
- sex life or sexual orientation.

In a school, this could include:

- a safeguarding matter
- pupils in receipt of pupil premium
- pupils with special educational needs and disability
- children in need
- children looked after.

Information about a deceased person does not constitute personal data and therefore is not subject to the UK GDPR.

Whilst Tes Global Ltd have made every effort to ensure that the courses and their content have been devised and written by leading experts who have ensured that they reflect best practice in all aspects, Tes Global Ltd exclude their liability of the consequences of any errors, omission or incorrect statements to the fullest extent permitted by law and Tes Global Ltd make no warranty or representation as to the accuracy, completeness or fitness for purpose of any statements or other content in the course.

Criminal offence data

Criminal offence data includes:

- the alleged committing of an offence
- the legal proceedings for an offence that was committed or alleged to have been committed, including sentencing.

Schools process criminal offence data in storing the outcome of a Disclosure and Barring Service (DBS) check on their employees, non-employed staff, and volunteers. As this data relates to criminal convictions, collecting and retaining it means the school is processing criminal offence data. This applies even though the check has not revealed any conviction.

Resources can be found in the Resource section of the course.

Data subject

A data subject is a person. It is an identified or identifiable living individual to whom personal data relates.

Reflective question
Can you think of examples of data subjects in a school context?

A school's data subjects include:

- *pupils and former pupils*
- *parents and carers*
- *employees and non-employed staff*
- *governors and trustees*
- *local-authority personnel*
- *volunteers, visitors, and applicants.*

Data assets

Schools store personal data in various formats, collectively known as data assets. These data assets include:

- **Data items:** Individual pieces of information.
- **Data item groups:** Clusters of data items related to the same process.
- **Data sets:** Collections of related data that can be managed as a unit by a computer.
- **Systems:** Administrative software applications.
- **System groups:** Larger infrastructures that host multiple administrative software systems.

What is meant by ’appropriate’ use of personal data?

We have already said that schools and other organisations have a responsibility to process personal data in an appropriate manner. But what do we mean by processing and appropriate?

Processing

This is simply a catch-all term to describe all the things that could be done to or with personal data.

It includes:

- collecting
- recording

- organising
- structuring
- storing
- using
- handling
- deleting or archiving, among many others.

Here are some examples of processing.

- Collecting names and addresses of people interested in hearing more about your school.
- Recording videos of people with CCTV surveillance cameras.
- Storing records of safeguarding data.
- Maintaining information in a student file.
- Transferring examination results to another organisation.
- Sending information to the personal email addresses of alumni about social events.
- Sharing vital medical records with health professionals.

In short, doing almost anything with personal data can be described as ’processing’.

Data controller

For most of the personal data the school collects, stores, and uses, the school or the multi-academy trust is the data controller. This means it is responsible under the Data Protection Act 2018 for protecting data in every situation where it decides:

- whose information to collect
- what types of data it needs
- why it needs it
- whether the information can be shared with a third party
- when and where data subjects’ rights apply
- for how long to keep the data.

A data controller needs to be registered with the Information Commissioner’s Office.

Resources can be found in the Resource section of the course.

Appropriate use of personal data

There are a number of aspects involved.

First, it means being lawful.

In addition to ensuring that the school is processing data in a lawful manner, ’appropriateness’ refers to satisfying the school’s internal requirements included in its own standards, policies, and procedures.

These are often created to ensure that the school satisfies all legal requirements, but they can also go above-and-beyond what is legally required.

These may cover things like:

- how the school obtains personal data
- where it is stored
- who is allowed access to it.

The **second priority** is to ensure that processing meets the internal expectations of your organisation.

The legal requirements together with your organisation's policies will include specific, objective rules on what is expected.

But they will also have expectations that are harder to quantify, such as considerations for:

- ethics
- safeguarding
- welfare or respecting people's right to privacy.

This means that data protection can never be a 'check-box exercise'.

In practice, handling data in an appropriate manner generally means:

- Being open and transparent about how people's data is processed and why it's needed.
- Processing the minimum amount of personal data necessary to fulfil the purposes for which it was collected.
- Ensuring that appropriate security and controls are in place to prevent that data being mishandled.
- Taking responsibility for data that belongs to other people and safeguarding it while it is under your control.
- Building trust between your organisation and the people whose data is processed.
- Recognising that people have a right to control their personal data, while striking a balance with the needs of your organisation and wider society.

Data protection compliance

You might think it should be straightforward or that the law directly states what is required. But in fact, much of data protection law is principles-based which means that compliance is not mainly about adhering to prescriptive rules but about meeting overarching, broad-based principles. It means that instead of keeping specific rules, organisations must identify for themselves whether their policies and actions meet those broad objectives.

In general, it can be said that data protection law requires organisations to achieve the following goals:

- Establish and maintain broad-based standards and values.
- Focus on outcomes and evidence-based compliance.
- Accountability from the organisation’s leadership.

Of course, we should note that specific rules do exist. Data protection law is not entirely principles-based; there are also specific requirements. For example, the UK GDPR requires organisations to appoint a data protection officer (DPO) if they are a public authority or body, or if they carry out certain types of processing activities.

Risks and challenges: data privacy in practice

Now let’s consider some of the practical concerns that may be important for your school.

- **Cyber attacks**
  Increasingly, cyber attackers are targeting schools.

  According to data obtained from the UK government, in the past year:

  52% of primary schools identified a breach or attack.
  71% of secondary schools identified a breach or attack.
  86% of further education colleges identified a breach or attack.

Higher education institutions are more likely to be affected by cyber-attacks **- 97%** identified a breach or attack.

- **Reputational damage**
  Reputational damage is a serious risk because schools are expected to look after children's data in an ethical and responsible way.

- **Financial costs**
  Cyber attacks, accidental disclosures, and data breaches can lead directly to financial losses.

- **Laws and regulatory action**
  There can also be fines and penalties for data breaches or unlawful processing imposed by data protection regulators or law courts.

AI and data protection

The GDPR mandates strict compliance with data protection principles when processing personal data in educational settings.

The Information Commissioner's office has designed an AI toolkit which provides support to help reduce the risk to individuals caused by AI systems.

A link to the toolkit can be found in the Resources section.

Resources can be found in the Resource section of the course.

Practical requirements for your school

What are the main elements that a school must do to meet data protection compliance requirements? Here are nine aspects to consider.

- **Leadership and governance**
  Accountability for Data Protection compliance starts at the highest levels of the school's management. A coherent strategy and clear goals should shape the organisation's intentions and results. Well-defined roles and responsibilities should be assigned to individuals. Regular reporting and reviews enable visibility for senior leadership.

  Governors and trustees should check that the school:
  - *monitors their data protection performance*
  - *supports the data protection officer*
  - *has good network security infrastructure to keep personal data protected*
  - *has a business continuity plan in place that includes cyber security.*

- **Record of processing and data mapping**
  Understanding what, why and how personal data is processed will help the organisation establish what risks exist and provide a basis for compliance. Understanding the personal data lifecycle and what happens to personal data under your control will enable clearer visibility of what the school is doing with people's data.

- **Incident and breach management**
  A data breach programme establishes processes and procedures to help reduce risks, as well as enabling the organisation to respond and react appropriately in the event of an incident.

- **Information rights and data ethics**
  Ensuring that individuals have a general right to privacy as well as appropriate information and access to their data is an important part of an ethical data protection programme.

- **Training staff**
  Training on data protection should include training on specific school processes such as:
  - personal data breach reporting processes
  - the escalation of information rights requests.

- **Data sharing and contracts**
  Appropriate contracts and measures must be in place for any transfers to take place lawfully. Even where this isn't applicable, managing the agreements, contracts, and arrangements between your organisation and other parties is a core part of a responsible approach to data protection.

- **Information security and operations**
  Ensuring the right levels of confidentiality, integrity, and availability will protect personal data and ensure that access to it is appropriately controlled and logged. Since most personal data is stored and sent in electronic form, the underlying software, hardware, and networks should be designed and implemented with security as a central concern.

- **Risk management controls**
  Wherever possible, you should try to reduce, mitigate, or eliminate the risk of personal data being mishandled, misappropriated, or misused. Establishing and maintaining an effective data protection risk management programme is a necessary element in a compliance programme.

- **Policies and notices**
  Formal policies and procedures should be clearly written, regularly reviewed, and widely disseminated to establish and maintain the organisation's expectations for how personal data is processed. Meanwhile, information should be clear and readily available to data subjects.

Putting it into practice

We will now consider some key, practical considerations for your school that are found in UK data protection law.

- Record of processing
- Personal data breaches
- Data subject rights
- Data Protection Impact Assessment/Data Protection Officer. These are now mandatory for schools.

There is much more to data protection law than these points, but they are important aspects to get right in a compliance programme.

Record of processing

One of the specific requirements in the UK GDPR is the Record of processing. This is an internal inventory or listing of all the processing that takes place in your school. It involves identifying all the applications, systems and processes that process personal data.

Take a moment to think about the work you are involved in. Much of it will involve collecting, using, sharing, disseminating, or storing personal data. A Record of Processing is sometimes called a data map. Just remember that it is a central register or inventory of all the processing that your school undertakes, and it must be made available if requested by the UK's data protection regulator.

The Record of processing identifies, among other things, the following key aspects:

- the process or system where personal data is processed
- whose personal data is involved
- what kind of personal data is processed
- the purpose for processing the personal data
- with whom is the data shared
- how long the personal data is retained
- what security measures are in place to protect the personal data.

Each individual process or system needs a separate entry. It is common for a school to have hundreds of line items in the Record of processing.

Here are some examples.

- After-school club membership enrolment
- Emergency contact database
- Student application process
- Alumni outreach and communications
- CCTV surveillance
- Car parking access and permits
- Visitor logs
- CVs and job applicant data
- Student welfare and pastoral reporting
- Parental consent process

Personal data is involved in all the examples. Sometimes, it is special category data whereas in other cases, the data may be of a less confidential nature (such as car registration numbers and ownership). But in all cases, there is an obligation to identify and document the personal data processed.

A comprehensive Record of processing will enable your school to understand where and how personal data is processed. It will also enable you to undertake another requirement under UK data protection law: a Data Protection Impact Assessment.

Personal data breaches

A personal data breach is defined under the UK GDPR as,

"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data."

Resources can be found in the Resource section of the course.

The following are common examples of personal data breaches:

- Personal data is accidentally disclosed to the wrong party.
- An unauthorised party gains access to computer systems and obtains data.
- Mobile devices containing personal data are lost or stolen.
- Important data that must be retained is accidentally deleted.

The UK GDPR sets out high expectations for organisations when data breaches occur. This is because the consequences for data subjects can be high, especially if it involves special category data, such as health data or safeguarding records. There is mandatory reporting of personal data breaches under UK law. In the event of an incident, you may need to notify both the Regulator (the ICO) and the affected data subjects.

What breaches do we need to notify the ICO about?

When a personal data breach has occurred, you need to establish the likelihood of the risk to people's rights and freedoms. If a risk is likely, the school must notify the ICO. If a risk is unlikely, then this does not have to be reported. If this decision is made, the school will need to justify this decision, so it should be documented.

If there is a risk to data subjects, your school is required to inform the Regulator within 72 hours. If it is determined that the risk is not likely, no reporting is required.

If there is a high risk to data subjects, your school is also required to inform the affected individuals without undue delay.

Organisations must decide for themselves whether there is a risk or a high risk and to document the facts and decisions surrounding the incident. Moreover, the 72-hour notification requirement means that you must act quickly. Internal reporting mechanisms within a school are therefore critical to ensure that the right individuals (such as the Data Protection Officer) are informed immediately. A data breach policy and associated procedures are an important part of a school's data protection programme.

You can read more about Data Breaches at the ICO's website.

Resources can be found in the Resource section of the course.

Data subject rights

'Data subject rights' are also known as 'Data subject access rights', 'Subject access rights', or 'Individuals' rights'. In short, data subject rights give people legal control over their personal data.

The rights are set out in the UK GDPR as follows:

The right to be informed involves telling people what personal data is collected and how it is further processed. It concerns communication and requires organisations to be open and honest about how they process people's information.

The right of access allows people to discover what personal data an organisation holds concerning them. There are strict time limits on how long organisations have to respond.

The right to rectification enables people to request that organisations correct any inaccurate or incomplete information about them. As with the right of access, organisations must respond to the request within a specified time limit.

The right to erasure grants people the right to have their personal information deleted in certain, specific situations. It is sometimes known as the 'right to be forgotten'.

The right to restrict processing allows for people to request that organisations limit or suppress the processing of their personal data in certain, specific situations.

The right to data portability allows individuals to obtain and reuse their personal data with another organisation. It allows people to have their information moved from one IT system to another.

The right to object means that people may object to an organisation processing their data. Where it applies, it means that organisations must cease processing the individual's data, even if they had previously consented.

Rights in relation to automated decision making and profiling provides for particular rights in situations where no human involvement takes place in the processing of a person's data. Rights include the possibility of requesting human intervention or challenging a decision.

Schools must be prepared to respond quickly and appropriately to all of these data subject rights requests. At a minimum, carefully thought-out processes and procedures for responding to such requests should be maintained.
It is important to note that in many cases, data subject rights are not 'absolute rights'. In other words, they do not apply in every situation. There are times, for example, when a data subject may want their data deleted but the school has a legitimate reason or legal obligation to retain it. In such circumstances, the request to erase the data can be lawfully denied.

One important exception must be made about safeguarding. Although the UK data protection law provides for strong data subject rights, as well as a general right to privacy, schools should be mindful about statutory guidance on safeguarding.

Rights to access for schools

The right to access means that people are entitled to know what personal data the school holds about them and also to obtain a copy of that information. As a general rule, data protection law requires schools to meet any request for copies of personal data. The request can be made by parents or children but the school should always remember that a child's personal data is their own. This means that schools must be careful to consider several factors if the request comes from parents.

You will usually need to get the pupil's consent to share their data if they are aged 13 or over. If they are under 13, you must get consent from whomever holds parental responsibility for the child. A child should not be considered to be competent if it is evident that he or she is acting against their own best interests.

In Scotland, a child aged 12 or over can give consent unless the contrary is shown.

For more information on subject access requests in the education sector, there is useful guidance from the Data Protection Regulator (the ICO) at the ICO website.

Resources can be found in the Resource section of the course.

It is important to highlight another reason under which subject access requests may be denied. This is if they are "manifestly unfounded or excessive". This can be relevant for staff, parents, children, or any other data subject requesting data.

For example, if a school has reason to believe that a request has malicious intent, it may refuse to comply.

There is further information on this topic at the ICO website.

Resources can be found in the Resource section of the course.

As we have seen, there are strong provisions preventing organisations from processing data that infringe on the rights of individuals. However, in the UK, it does NOT prevent the sharing of information for the purpose of keeping children safe. Sharing information effectively is essential to help identify any safeguarding issues early and to put appropriate provisions and measures in place.

There is statutory guidance titled ‘Working Together to Safeguard Children’ which states that:

The Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR) supports the sharing of relevant information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of safeguarding and promoting the welfare of children.

Resources can be found in the Resource section of the course.

Data Protection Impact Assessment/Data Protection Officer in a school context

The GDPR expects an effective approach to risk management and key elements of this are the Data Protection Impact Assessment and the Data Protection Officer role.

Schools need to consider the risks to Data Subjects of different processing activities they undertake (or plan to undertake).

A Data Protection Impact Assessment (DPIA) is performed for this purpose, and the GDPR (Article 35) expects a DPIA where processing:

- will use new technologies
- is systematic and extensive and involves automated Processing
- is on a large scale and of Special Category Personal Data or
- is systematic monitoring of a publicly accessible area on a large scale.

A DPIA contains (at least):

- a description of the Processing operations and the purposes of the Processing, including the legitimate interests pursued by the Data Controller (if applicable)
- a review of the necessity of the Processing in relation to the purposes
- an assessment of the risks to the rights and freedoms of the affected Data Subjects; and
- the measures the Data Controller will take to address the risks, including safeguards, security measures and mechanisms to ensure the protection of the Personal Data.

In undertaking a DPIA and indeed in establishing and overseeing many of the processes required to comply with the GDPR, a school will require a source of expertise.

The Data Protection Officer (DPO) role is set out in the GDPR (Article 37) as being required where:

- Processing is carried out by a public authority or body
- Processing entails regular and systematic monitoring of data subjects on a large scale as part of the main activities of the Data Controller or Data Processor; or
- Processing Special Category Personal Data (or Personal Data relating to criminal convictions and offences) on a large scale as part of the main activities of the Data Controller or Data Processor.

Given that schools are considered public authorities for the purposes of the GDPR (as public authorities are defined as those subject to the Freedom of Information Act 2000 (FOIA) or the Freedom of Information Act (Scotland) 2002 in Scotland), it is the case that schools will need a DPO.

As per the ICO guidance the governing body of a maintained school, further education institution or university is considered a public authority under FOIA.

The GDPR states that the primary function of the DPO is to assist the Data Controller or Data Processor with compliance with the GDPR, and that:

- the DPO must have expert knowledge of data protection law and practices
- the DPO may be employed by or alternatively contracted by the Data Controller or Data Processor
- the Data Controller or Data Processor shall publish the contact details of the DPO and
- the DPO should be able to perform their duties independently (Recital 97).

Schools will need to appoint a DPO, and:

- the DPO must be expert in data protection
- the school must publish the details of the DPO
- the DPO must be independent (and not have a conflict of interests); and may be an employee or a contractor

The UK Data Protection Regulator

The UK's data protection authority is the Information Commissioner's Office (ICO). The ICO is an independent body that exists to uphold information rights.

The website of the ICO provides invaluable information and help to all organisations, large and small. There is information for schools and the education sector with examples of scenarios explained throughout.

The ICO also provide a helpline and live chat service along with a free online advisory check-up for small organisations.

Summary

In this course we have looked at what UK data protection law requires and how it affects your college, school or nursery with some practical examples.

You are now ready to complete the corresponding questionnaire. Click **'Questionnaire'** to begin the questions.

When you have completed the questionnaire, there is the opportunity for you to leave feedback on the course and we would be very grateful if you would take a minute to do so.

Whilst Tes Global Ltd have made every effort to ensure that the courses and their content have been devised and written by leading experts who have ensured that they reflect best practice in all aspects, Tes Global Ltd exclude their liability of the consequences of any errors, omission or incorrect statements to the fullest extent permitted by law and Tes Global Ltd make no warranty or representation as to the accuracy, completeness or fitness for purpose of any statements or other content in the course.