Inspiring Futures through Learning

Data Protection Policy

Policy name:	
Version:	V2.1
Date relevant from:	September 2025
Date to be reviewed:	As and when regulations change
Role of reviewer:	IFtL Head of Operations
Statutory (Y/N):	Y
Published on website*:	3C

Policy level:**	1
Relevant to:	All employees through all IFtL schools and departments
Bodies consulted:	
Approved by:	IFtL Board of Trustees
Approval date:	28 August 2025

Key:

**** Publication on website:***

IFtL website		**School website**	
1	Statutory publication	A	Statutory publication
2	Good practice	B	Good practice
3	Not required	C	Not required

***** Policy level:***

1. Trust wide:
   - This one policy is relevant to everyone and consistently applied across all schools and Trust departments with no variations.
     - *Approved by the IFtL Board of Trustees.*
2. Trust core values:
   - This policy defines the values to be incorporated fully in all other policies on this subject across all schools and Trust departments. This policy should therefore from the basis of a localised school / department policy that in addition contains relevant information, procedures and / or processes contextualised to that school / department.
     - *Approved by the IFtL Board of Trustees as a Trust Core Values policy.*
     - *Approved by school / department governance bodies as a relevantly contextualised school / department policy.*

3. School / department policies
   - These are defined independently by schools / departments as appropriate
     - *Approved by school / department governance bodies.*

Data Protection Policy

Introduction

In order to operate efficiently IFtL [the Trust] has to collect and use information about people with whom it works. These people may include members of the public, current, past and prospective employees, clients and customers, and suppliers. In addition, the law may require us to collect and use information in order to comply with the requirements of central government.

The Trust is committed to ensuring personal information is properly managed and that it ensures compliance with all current data protection legislation including the Data Protection Act 2018 [DPA] and the UK GDPR.
The Trust will make every effort to meet its obligations under the legislation and will regularly review procedures to ensure that it is doing so.

1. Scope

This policy applies to all employees, governors, contractors, agents and representatives and temporary staff working for or on behalf of the Trust.

This policy applies to all personal information created or held by the Trust in whatever format (e.g. paper, electronic, email, film) and however it is stored, (for example ICT system/database, shared drive filing structure, email, filing cabinet, shelving and personal filing drawers).

For the purposes of this policy, any reference to the Trust includes the Trust offices and all schools that are a part of the Trust Including our ITT provision (as a shared responsibility with Chiltern Learning Trust).

The DPA/UK GDPR does not apply to information about deceased individuals.

2. Responsibilities

The Data Controller, under data protection law, is Inspiring Futures through Learning (also referred to within this document as IFtL or the trust). Individual schools are also Data Controllers and share this role, and its responsibilities, with the trust. The Board of Trustees has overall responsibility for compliance with current data protection legislation.

The Headteachers of individual schools are responsible for ensuring compliance with the DPA, UK GDPR and this policy within the day to day activities of their Schools.

Headteachers should appoint a data lead who will be the main point of contact in school for the trust's Data Protection Officer.

Headteachers are also responsible for ensuring that any staff involved in the handling of personal data are trained in the correct procedures and are fully aware of polices relating to data protection.

Although members of staff or contractors who hold or collect personal data are responsible for their own compliance with the DPA and UK GDPR, schools should ensure that all appropriate technical and organisational measures are in place to ensure that data security is robust and that there is no opportunity for a rogue member of staff to illegally obtain and remove personal data.

Schools must have contracts in place with any organisations that process personal data on the school's behalf. Such contracts must state the processors position on compliance with data protection legislation and should include information on the adequacy and security of data stored.

The Trust's Head of Operations is the named Data Protection Officer and is responsible for appropriately advising schools and staff on the correct procedures and their obligation to comply with the legislation, to provide training opportunities to staff that require it, to monitor compliance with the legislation and to advise on corrective actions where appropriate, to conduct internal data audits and to be the main point of contact with the regulatory authorities.

3. The Requirements

Article 5 of the GDPR states that personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals
- Collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and, where necessary, kept up to date. Every reasonable step must be undertaken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- 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 subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against

accidental loss, destruction or damage, using appropriate technical or organisational measures.

Article 5(2) requires that:

- the controller shall be responsible for, and be able to demonstrate, compliance with the principles

Personal data is information about living, identifiable individuals. It covers both facts and opinions about the individual but need not be sensitive information. It can be as little as a name and address. Such data can be part of a computer record or manual record.

4. Notification

Under data protection law, every data controller who is processing personal data is required to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence. The Information Commissioner maintains a public register of data controllers, in which the trust is registered. IFtL schools do not need to register individually.

The trust will review the Data Protection Register annually, prior to renewing the notification to the Information Commissioner.

5. Privacy Notices

Whenever information is collected about individuals, they must be made aware of the following:

- The identity of the data controller, e.g. the Trust;
- The purpose for which the information is being collected;
- The lawful basis for collection of that information;
- Any other purposes that it may be used for;
- Who the information will or may be shared with; and
- How to contact the data controller.

This must be at the time that information first starts to be gathered on an individual. Privacy notices are displayed in our schools and on our school websites.
Schools should also display relevant privacy notices near data collection points. For example, schools that use electronic visitor management systems should ensure that the system displays a privacy notice when visitors first sign in.

Specific privacy notice may be required if data outside the scope of the standard privacy notice is required. One example of this would be collecting information related to Covid vaccination status. This requires a separate privacy notice.

6. Lawful Basis for Processing

Under the terms of the GDPR, data controllers must have a valid lawful basis in order to process personal data. The following bases are the grounds on which information is processed within IFtL.

Legal Obligation – Where we are required, by law, to process data in order to fulfil our legal requirements, such as compliance with The Education Act 2011

Public Task – Where processing of data is necessary to allow us to fulfil our duty of carrying out tasks in the public interest

Performance of a Contract – where data is processed in relation to a contract, such as an employment contract

Legitimate Interest – where we have a legitimate interest that does not prejudice the rights and freedoms of the data subjects (but this cannot be used for performance of a task as a public authority)

Vital interests – In very specific and limited circumstances, it may be necessary to process data to protect the vital interests of a data subject. This may be, for example, in a medical emergency or a child protection incident

Consent – Where appropriate, we will seek consent to process data

We may share **personal data** that we hold about **data subjects**, and without their consent, with other organisations. Such organisations include the Department for Education, Ofsted, health authorities and professionals, School nursing teams, the Local Authority, examination bodies, other schools, and other organisations where we have a lawful basis for doing so.

The Trust will inform **data subjects** of any sharing of their **personal data** (usually, by means of a published privacy notice) unless we are not legally required to do so, for example where **personal data** is shared with the police in the investigation of a criminal offence.

In some circumstances we will not share safeguarding information. Please refer to our Child Protection Policy.

References provided, or received, by any IFtL school or department are classed as confidential and are excluded from any request for access (subject access request).

7. Data Subjects and Their Rights

Under the GDPR, Data Subjects have more rights than they had under the previous Data Protection Act. These rights, and how we deal with requests under these rights, are detailed within this section. If there is any uncertainty around the rights of the data subject or if further clarification is required following any communication regarding a person's rights, please contact the trust's Data Protection Officer.

Right to be informed

Organisations are required to provide fair processing information and this is done via privacy notices which are available on all IFtL websites and also available, on request, from school offices.

Right of access

Individuals have the right to request any information that we hold about them. This information should be provided free of charge, and within one month of the request. Further guidance is available in the IFtL Subject Access Request Policy.

References provided, or received, by any IFtL school or department are classed as confidential and are excluded from any request for access (subject access request).

Right to rectification

Individuals have the right to have any incorrect or inaccurate personal data rectified. This means that, where a request has been made, all records relating to that individual, where information is found to be incorrect, must be corrected within one month. This relates to paper records, computer files, backups of computer files and, where possible, records kept by third parties where the information has been passed on by the trust.
Requests can be extended by 2 months where the request for rectification is complex.

Right to erasure

The right to erasure is also known as 'the right to be forgotten'. This is to enable an individual, where it is appropriate, to request the deletion or removal of personal data relating to them where there is no longer a compelling reason for its continued processing.

It is important to note that this is not an absolute right and the right of erasure can be refused in many circumstances.
Where data is no longer necessary in relation to the purpose for which it was originally collected, where an individual has withdrawn consent, where an individual objects to the processing of their data and there is no overriding legitimate interest for the continued

processing of the data or where data is being unlawfully processed are some of the reasons where the right to be forgotten may be upheld.
Any case where a data subject requests to exercise this right must be referred to the trust's data protection officer.

Right to restrict processing

An individual can request that their data is no longer processed, that is, no longer used by the organisation. If this happens, the organisation retains the right to store the data, but may no longer further process it. This restriction may happen if the accuracy of data is contested, where an objection has been made against the processing, where processing is unlawful and the data subject requests restriction rather than erasure of data or where the organisation no longer requires the data but the individual requires the data to be retained in order to establish, exercise or defend a legal claim.
If this data has been passed on to third parties, there is an obligation to pass the restriction details on to them unless it is impossible, or would involve disproportionate effort, to do so.

Right to data portability

Individuals have the right to obtain and reuse their personal data for their own purposes across different services. This right should allow them to move, copy or transfer personal data easily from one IT system to another, safely and securely.
Data should be supplied in a structured, commonly used, machine readable format (An example of this format would be a .csv file) where possible.
This information must be provided free of charge within 30 calendar days.
There is no obligation to make data compatible with a proprietary format nor to convert paper records to electronic format.
This right is unlikely to be exercised within a school setting and is primarily aimed at businesses and financial institutions. Schools, however, should be aware of the right and of its implications.

Right to object

Individuals have the right to object to their data being processed based on legitimate interest or the performance of a task carried out in the public interest. They also have the right to object to direct marketing, including profiling and to the processing for purposes of scientific or historical research and statistics.

Any right to object must be referred to the Trust's DPO.

Rights related to automated decision making, including profiling

Individuals have rights with regard to automated decision making (where no human involvement is included in the making of a decision) as well as automated profiling (where

personal data is analysed to evaluate certain things about an individual).
Currently, neither the trust nor its schools undertake any automated decision making or profiling. Should any automated systems be investigated in the future, a data protection impact assessment should be undertaken prior to any systems being put into place.

8. Provision of data to children

Secondary provision within the Trust should undertake an assessment of requests from pupils to establish whether requests made by pupils are deemed appropriate, i.e. whether the pupil is of sufficient maturity to understand the nature of such a request. Under UK law, children of 13 years and older are deemed responsible enough to manage their own data. Any decisions relating to subject access requests for children must be documented and retained with the paperwork.

9. Parents' rights

The Education (Pupil Information)(England) Regulations 2005, do not apply to academies and free schools, therefore a parent's right to access their child's educational record does not apply within the IFtL trust as long as an annual report on the child's progress is provided. Schools may decide, on a case by case basis, to grant a request to access a pupil's educational record and will bear in mind any guidance issued from the ICO.

The law relating to children over 13 managing their own data also relates to this area, and schools should be aware that requests for pupil data for children aged 13 or over may need to be authorised by the child. In theory, a child aged 13 or older can prevent their parents accessing pupil data.

10. Information Security

All members of staff should be constantly aware of the possibility of personal data being seen by unauthorised personnel. For example, possibilities may arise when computer screens are visible to the general public; files may be seen by cleaners if left on desks overnight (all papers must be locked in cabinets when not in use).

The requirement of GDPR is that only people with a legitimate entitlement to access data should be allowed to do so, therefore any paperwork containing personal data should be locked away at the end of each day or offices should be locked so that persons that are not authorised to access the data are unable to do so.

Computer screens must also be locked whenever an employee leaves their workstation in order to protect any data that is accessible from that workstation.

Portable flash drives (USB sticks) should not be used, under any circumstances, for the storage of personal data. These devices are easily lost or corrupted. (The use of such devices for non-personal information is acceptable, although all staff should be working from the IFtL Sharepoint Portal which should reduce the need for portable drives).

Laptops or tablets, where they have access to personal data, should be password protected and drives should be encrypted to minimise the risk of a data breach in event of the loss of a machine.

Schools should ensure that administrator password to networks are kept secure and only provided to persons that absolutely require access. Where possible, access should be restricted to only the areas required and each administrator should have their own password so that access can be easily revoked if required.

Schools should consider penetration testing and ethical hacking services in order to assure the security of their networks.

For further guidance on this subject, please refer to the IFtL Cyber Security Policy.

11. Maintenance of up-to-date data and disposal of data

Personal data should be checked and updated at appropriate intervals. Staff and parents should be given the opportunity to check relevant personal data and make corrections on a regular basis.

Data collection should take place via Bromcom's My Child at School App.

Out of date information should be discarded if no longer relevant. Information should only be kept as long as needed, for legal or business purposes. The attitude where data is kept 'just in case' should be avoided. In reality, most relevant information should be kept for the period during which the person is associated with a school plus an additional period determined by the records management policy. Ideally, where data is archived, a disposal date should be clearly marked on boxes or folders.

When it is time for data to be disposed of, it should be destroyed in an approved manner. For paper records, this will be by use of a cross cut shredder or by means of an approved contractor operating to current industry standards.

Where electronic information is disposed of, this must be done under contract with a supplier where the contract assures that the terms of the GDPR are complied with. This

extends to disposal of any computer equipment containing storage media (hard drives etc) that may have processed personal data during the lifetime of the equipment.

Schools should maintain a data asset register listing what data they hold, where it is held, who has access, why they have this data and for how long the data is kept. IFtL schools currently use GDPRiS to manage this.

It is a legal requirement for records to be kept of data that is disposed of. Staff destroying data should record, as a minimum;

- File reference (or other unique identifier)
- File title (or brief description)
- Number of files
- The name of the authorising officer
- Date action taken

This could be kept in an Excel spreadsheet or other database format and retained

13. Retention of Safeguarding and Child Protection Data

In January 2021, IFtL published a 'Transfer and Retention of Safeguarding and Child Protection Files' Policy which advises on how Primary Schools should transfer CP data when pupils move on their next setting.

The key points from this document include;

- Schools that use an online or electronic child protection or safeguarding system should contact the provider to check what happens to data if the child transfers to a school that does not operate the same system or if a child leaves the school with no further school placement (i.e. if they are home educated or move abroad, for example).
  Schools must ensure that they have procedures in place for these circumstances to ensure that information is retained or transferred and there is no risk of loss of information.
- All schools should compile a chronology of information as a summary of events which tell the whole story (in summary form) of the file[1]. This should record decision making, action agreed, outcomes and strategies.
- All schools should compile a vulnerable child tracker/mapping tool to map services provided to support children[1]. This could also be used to identify and monitor sibling links.

- Primary schools ***MUST*** transfer CP and safeguarding files when a child leaves the school. The only legal reason for retention of CP or safeguarding information is if there is ongoing legal action.
  Having said that**, IFtL recommend that a copy of the file is retained for a period not exceeding 24 months to allow for any enquiries or referrals from the child's new school to be appropriately addressed.** This will allow for a settlement period at the new setting and an adequate time for any issues to arise which may require input from staff who may need to refer back to notes on the file.
  This retained copy should be stored securely, preferably in electronic format, and should not be otherwise processed unless an enquiry is made by the new setting or by an authority with appropriate legal justification. At the end of the 24 month period, the files should be securely destroyed[2].
- When files are transferred, written evidence of transfer should be retained. Schools should retain a copy of this form along with a copy of the chronology of information form until the child reaches the age of 25. Schools should store these securely in a designated location that is only accessible by DSLs.
- If children are classified as missing from education or are home educated, there may be a requirement to retain files at the last known school until the child reaches the age of 25. Cases should be referred to the local authority for guidance.
- Where an older sibling leaves a school and leaves a younger sibling behind, there may be a case to justify retention of the older sibling's files in order to ensure that the legal requirement to safeguard the younger sibling is met. As a minimum, the chronology in the younger sibling's file should refer to the transfer of files and cross reference to the retained chronology from the older sibling's file.
  Each case should be judged according to the circumstances of the individual case and a documented decision taken by DSLs involved. All decisions should be justified and documented on the CP file chronologies.
- Safeguarding and CP files must be retained within the school system until the child reaches the age of 25. Responsibility for transfer lies with the school that the pupil is leaving and the school should satisfy themselves that they have fulfilled their duty and obtained sufficient evidence that the complete file has been received by the new school. Responsibility for maintenance of the file then becomes the responsibility of the new school.

[1] – These items come from Learning from Serious Case Reviews (SCRs) and Serious Incident Learning Reviews (SILRs) relevant to information sharing & recording- schools, 2009-2015

14. Recording of Data

Records should be clear, concise and accurate. It should also be borne in mind that at some time in the future, the data may be inspected by the courts or some legal official. Data should, therefore be correct, unbiased, unambiguous and clearly decipherable/readable. Where information is obtained from an outside source, details of the source and date obtained should be recorded.

15. Photographs and Video

Photographs and video are considered personal data and require the same protection as any other type of personal data. Any reference to photographs in this section also relates to video.

Within IFtL, and in line with guidance from the ICO, photographs are used under the public task legal basis. Photographs are used to support educational activities, promote pupil achievements and to document school life.

Photographs may be used within school, on school websites, on social media, within communications or marketing media and in promotion of school activities to the wider community.

While we do not require consent to use photographs, parents and/or children can object to their use and request that we do not use them. If this request is made, photographs in the scope of such a request must not be used.

Schools must ensure that they follow robust procedures when using photographs, to ensure that no child where CP, safeguarding or non-contact orders exist, are used in such a way that could breach any confidentiality arrangements and potentially place the child, or their family, in danger.

In line with guidance from the UK safer Internet Centre, as far as possible, photographs should be published without names attributed, metadata should be removed from published photographs and lower resolution images should be used to help deter image manipulation.

Video or other footage of school plays that may be filmed professionally and made available for parents to purchase is generally processed under the legitimate interest basis and a legitimate interest impact assessment will be undertaken prior to any activity being filmed in this way.

17. Further rules around consent

Wherever possible, the use of consent as a legal basis for processing data should be a last resort.

Any data that is necessary to perform the tasks required of the organisation by law, should be gathered using the lawful bases for processing detailed in part 7 above of one of the other lawful bases listed under article 6 of the GDPR (or article 9 for special category data). Where data is required that does not fall within the bases stated, consent should be obtained in order to process this data prior to any processing taking place.

Where consent is required, it must be freely given, unambiguous and explicit. It also requires a positive opt-in which means that pre-ticked boxes or boxes where you must tick to opt out must not be used.

The requirement for consent to be explicit also means that consent must be given for each individual use of the data. This means that, for example, you cannot seek consent for someone's contact details to keep them informed about a particular event in school, then use those details for marketing or other activities.

Individuals should also be informed that they have the right to withdraw their consent at any time and should also be informed if the data that they are consenting to will be passed on to any third parties for processing.

There are some exceptions to withdrawal of consent. For example, if you have just printed a prospectus and consent is withdrawn for a photograph within it, it may be acceptable to continue to use these but to remove the photograph in future print runs. If this occurs, consideration would have to be given on a case by case basis.

If there is any doubt around this, please contact the trust's data protection officer.

18. Breach of the policy

Non-compliance with the requirements of the DPA/UK GDPR by members of staff is a serious matter. Fines under GDPR can be up to £17.5 Million or 4% of annual turnover, whichever is the greater. Staff can also be personally convicted of criminal offences, for example, obtaining or disclosing personal data for their own purposes or without the consent of the data controller can lead to criminal prosecution. Non-compliance by a member of staff is therefore considered a disciplinary matter which, depending on the circumstances, could lead to dismissal.

19. Procedure in the event of a data breach

A data breach can be any loss, destruction, unofficial alteration, unofficial access, theft or disclosure of personal data.
Any potential breach of data MUST be notified to the trust's data protection officer as soon as it is discovered.

For further guidance, please refer to the Trust's Data Breach Policy.

20. Transferring data outside of the UK/EEA

The majority of general data processing within schools will not involve transferring data outside of the UK. However, many software providers host data in other countries so transferring data outside the UK needs to be given due consideration.

The UK government has made adequacy regulations to allow data to be transferred between the EU and the UK so this is permitted. This arrangement is under regular review.

If data is being transferred to other countries, checks should be made on whether there are adequacy arrangements, standard contractual clauses or other conditions under which transfers may be made.

In all cases, the trust's data protection officer should be consulted about transfers outside the EEA/EU.

21. Provision of online services to children

Where online services that collect personal data are offered to children, explicit parental consent must be obtained. This is particularly significant where children's personal information is used to create online profiles or for marketing. (Preventative or counselling services do not necessarily require parental consent.) Children aged 13 years or older may provide their own consent.

It is unlikely that these services will be offered by the trust or its schools, but schools should ensure that any apps or websites used for educational purposes are compliant with GDPR before putting them to use in the classroom.

22. Use of email and document security

Email has evolved over the years and the email systems that are currently in use across the Trust are Outlook/Office 365 and Google Mail. Both systems have Transport Layer Security (TLS) embedded by design.
TLS is a protocol designed to provide privacy and data integrity between two or more communicating computer applications. This means that, by default, email between any IFtL staff using their work email account is secure and no further steps are necessary to ensure secure transfer of information.

If extra security is required, for communicating outside the trust, products such as Egress Switch or Trend Encryption can be used.
Azure Information Protection can also be enabled in Outlook which enables encryption or emails and controls such as 'do not forward'.

All staff, governors and trustees should be issued an IFtL email address for their use with regard to work matters. Use of personal email addresses for work matters should be

avoided wherever possible.

Where agendas and papers for meetings are issued, these should be hosted on systems such as SharePoint or Governor Hub and links distributed by email as opposed to sending out documents attached to an email. This helps ensure the security of the documents and also helps with version control as there will only be one copy of the document in use rather than various copies which may not pick up any modifications made.

Particular attention should be paid to permissions when sharing documents and you should consider whether to send documents with read only rights or whether editing is necessary.

23. DPIAs and Data Protection (Privacy) by Design

It is critical that any new systems take data protection into account at the planning stage. When looking into any new systems that handle personal data, a Data Protection Impact Assessment (DPIA) should be undertaken to ensure that the security, protection and privacy of data held within the new system is assured prior to any purchasing taking place.
For information regarding DPIAs, please see the ICO guidance on Privacy Impact Assessments or refer to the trust's data protection officer.

Further guidance on all matters relating to data protection is available from the trust's data protection officer or from the Information Commissioners Office.

24. Technical and Organisational Measures

One of the requirements of the GDPR is that organisations implement appropriate technical and organisational measure to ensure the appropriate protection of data and information. All schools should consider that they have appropriate measures in place.
Some of the measures we have in place as a Multi Academy Trust are;

- A suite of data protection policies that all schools are required to comply with
- All schools protected by firewalls, internet filtering, anti-virus and anti-malware software
- Use of Outlook and Office 365 with in-built protection
- Azure Rights Management and Microsoft Secure Score used to maximise protection
- Multi Factor Authentication on all portal admin accounts
- Appropriate permissions set to ensure access to information is secure
- Business Continuity Plans are in place across schools

- Staff are trained through Smartlog or through the IFtL portal and this is supplemented by refreshers at Inset and twilight sessions
- Annual data protection audits are undertaken
- GDPRiS is being used across the trust to monitor compliance
- School buildings are secure with efficient visitor management in place
- Schools have effective procedures in place for secure disposal of paperwork and of redundant IT equipment

Schools should consider their own measures to ensure that they are as secure as possible and to highlight where they may need to make improvements.
As a trust, we work to the NCSC Cyber Essentials standards to ensure that our IT security is as robust as possible.

25. Additional Considerations

Certain events and incidents may occur which fall outside of the scope of our general processing activities. For example, the processing of data related to the Covid-19 pandemic was an unexpected occurrence and some of the use of this data may not be covered by our usual practices.

In these circumstances, IFtL will issue central guidance and/or additional privacy notices to ensure that we continue to process data in a legal manner.

If you are in any doubt about any data processing and whether or not additional justification is necessary, please speak to your school Data Lead or contact the IFtL DPO at dpo@iftl.co.uk

26. Vulnerable Children and Adults

Certain children, and adults, may have individual circumstances which mean they are at a greater risk if their personal data is used in a way that it shouldn't be.
Schools must ensure that anyone with a responsibility for handing data for these categories of people, particularly those responsible for publishing data, managing websites or managing social medial accounts, must have an understanding of who is affected and how critical it is that data is used appropriately.

The individual circumstances around each case do not need to be shared, but the importance of not sharing data inappropriately, including understanding that photos or

names of anyone under these circumstances should not have photos or names published anywhere, needs to be communicated and understood.

27. Staff Training

All staff must undertake annual data protection training. This must follow guidance issued by the DPO and will usually take the format of an online course. It is the responsibility of school senior management teams to monitor the uptake and completion of training, and to ensure staff complete this training in a reasonable timeframe.

Online training should be supplemented with school specific training, for example, all staff should know who the school data lead is, how to identify a data breach or a subject access request, who to report these to and where to find the relevant policies governing these. This can be via a staff briefing and does not have to be in-depth.

For colleagues requiring a deeper understanding of data protection, such as data leads or SLT members, courses available through the GDPRiS Data Protection Management System should be allocated. For example, Data Leads should undertake the 'Introduction to the role of the Data Protection Officer' course.

Abbreviations

Abbreviation	**Description**
DPA	Data Protection Act 2018
EIR	Environmental Information Regulations 2004
FoIA	Freedom of Information Act 2000
GDPR	General Data Protection Regulation

Glossary

Data Controller	A person or organisation that determines the purposes for which, and the manner in which, personal data is processed
Data processor	A person, other than an employee of the data controller, who processes the data on behalf of the data controller

Data Subject	The person whose personal data is held or processed
Educational record	The educational record is confined to information that comes from a teacher or other employee of a local authority or school, the pupil or their parents. Communications about a particular child from head teachers and teachers at a school and other employees at an education authority will therefore form part of that child's official educational record, as will correspondence from an educational psychologist engaged by the governing body under a contract of services. It may also include information from the child and their parents, such as information about the health of the child. Information kept by a teacher solely for their own use does not form part of the official educational record.
Information Commissioner (ICO)	The supervisory authority for data protection in the UK
Personal Data	Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identified
Processing	Obtaining, recording or holding data
Sensitive Personal Data	Data such as: • Contact details • Racial or ethnic origin • Political opinions • Religious beliefs, or beliefs of a similar nature • Where a person is a member of a trade union • Physical and mental health • Sexual orientation • Whether a person has committed, or is alleged to have committed, an offence Criminal convictions
Subject Access Request	An individual's request for personal data under the Data Protection Act 2018 or the GDPR.