# Personal Data Advice and Guidance

## Personal Data Handling

Recent publicity about data breaches suffered by organisations and individuals continues to make the area of personal data protection a current and high profile issue for schools, academies and other organisations. It is important that the school / academy has a clear and well understood personal data handling policy in order to minimise the risk of personal data breaches. A breach may arise from a theft, a deliberate attack on your systems, the unauthorised or malicious use of personal data by a member of staff, accidental loss, or equipment failure. In addition:

- No school / academy or individual would want to be the cause of a data breach, particularly as the impact of data loss on individuals can be severe and cause extreme embarrassment, put individuals at risk and affect personal, professional or organisational reputation.
- Schools / academies are "data rich" and the introduction of electronic storage and transmission of data has created additional potential for the loss of data
- The school / academy will want to avoid the criticism and negative publicity that could be generated by any personal data breach.
- The school / academy is subject to a wide range of legislation related to data protection and data use, with significant penalties for failure to observe the relevant legislation.
- It is a legal requirement for all schools / academies to have a Data Protection Policy.

Schools / academies have always held personal data on the pupils in their care, and increasingly this data is held digitally and accessible not just in the school / academy but also from remote locations. It is important to stress that the data protection laws applies to all forms of personal data, regardless of whether it is held on paper or in electronic format. However, as it is part of an overall online safety policy template, this document will place particular emphasis on data which is held or transferred digitally.

Schools / academies will need to carefully review their policy, in the light of pertinent Local Authority / Parent Organisation regulations and guidance and changes in legislation.

## Introduction

Schools / academies and their employees must do everything within their power to ensure the safety and security of any material of a personal or sensitive nature, including personal data.

It is the responsibility of all members of the school / academy community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- have permission to access that data
- need to have access to that data.

Data breaches can have serious effects on individuals and / or institutions concerned, can bring the school / academy into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioner's Office. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to the relevant school / academy policy which brings together the statutory requirements contained in relevant data protection legislation and relevant regulations and guidance (where relevant from the Local Authority / Parent Organisation).

The Holy Spirit Catholic Primary
Personal data advice /guidance

## Legislative Context

With effect from 25th May 2018, the data protection arrangements for the UK change following the European Union General Data Protection Regulation (GDPR) announced in 2016. This represents a significant shift in legislation and replaces the Data Protection Act 1998. The UK legislation was announced on the 14th September 2017. The Data Protection Bill's (DP Bill) journey through parliament and the associated text has been published online. The EU GDPR gives members states, like the UK, limited opportunities to make unique provision for how the regulation applies. However, the GDPR and the DP Bill should not be considered separately from each other.

## Are schools / academies in England and Wales required to comply?

In short, yes. Any natural or legal person, public authority, agency or other body which processes personal data is considered a 'data controller'. Given the nature of schools / academies and the personal data required in a variety of forms to operate a School / Academys this means that an educational college in the UK is required to comply.

Guidance for schools / academies is available on the Information Commissioner's Office website including information about the new regulations.

## Freedom of Information Act

All schools / academies (including Academies, which were previously exempt) must have a Freedom of Information Policy which sets out how it will deal with FOI requests. Good advice would encourage the School / Academy to:

- Delegate to the Headteacher / Principal day-to-day responsibility for FOI policy and the provision of advice, guidance, publicity and interpretation of the school's / academy's policy
- Consider designating an individual with responsibility for FOI, to provide a single point of reference, coordinate FOI and related policies and procedures, take a view on possibly sensitive areas and consider what information and training staff may need
- Consider arrangements for overseeing access to information and delegation to the appropriate governing body
- Proactively publish information with details of how it can be accessed through a Publication Scheme (see Model Publication Scheme below) and review this annually
- Ensure that a well-managed records management and information system exists in order to comply with requests
- Ensure a record of refusals and reasons for refusals is kept, allowing the school / academy to review its access policy on an annual basis

## Model Publication Scheme

The Information Commissioner's Office provides schools and organisations with a model publication scheme which they should complete. The school's / academy's publication scheme should be reviewed annually. The ICO produce guidance on the model publication scheme for schools. This is designed to support schools / academies complete the Guide to Information for Schools.

## Personal Data

The school / academy and its employees will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school / academy community – including pupils / students, members of staff and parents / carers e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Curricular / academic data e.g. class lists, pupil / student progress records, reports, references
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

## Fee

The School / Academy should pay the relevant fee to the ICO.

## Responsibilities

Every maintained school / academy in the UK is required to appoint a Data Protection Officer as a core function of 'the business' includes:

- regular and systematic monitoring of individuals on a large scale;
- [the processing of] special categories[1] of data on a large scale and data relating to criminal convictions and offences

The Data Protection Officer (DPO) can be internally or externally appointed.

They must have:

- Expert knowledge
- Timely and proper involvement in all issues relating to data protection
- The necessary resources to fulfil the role
- Access to the necessary personal data processing operations
- A direct reporting route to the highest management level

The data controller must:

- Not give the DPO instructions regarding the performance of tasks
- Ensure that the DPO does not perform a duty or role that would lead to a conflict of interests
- Not dismiss or penalise the DPO for performing the tasks required of them

As a minimum a Data Protection Officer must:

- Inform, as necessary, the controller, a processor or an employee of their obligations under the data protection laws
- Provide advice on a data protection impact assessment
- Co-operate with the Information Commissioner
- Act as the contact point for the Information Commissioner
- Monitor compliance with policies of the controller in relation to the protection of personal data
- Monitor compliance by the controller with data protection laws

[1] • 'Special categories of data' is the type of data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; genetic data, biometric data or data concerning health or sex life and sexual orientation

The school / academy may also wish to appoint a Data Manager. Schools / academies are encouraged to separate this role from that of Data Protection Officer, where possible. This person will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's / academy's information risk policy and risk assessment
- oversee the System Controllers

The school / academy may also wish to appoint System Controllers for the various types of data being held (e.g. pupil / student information / staff information / assessment data etc.). These Controllers will manage and address risks to the information and will understand:

- what information is held, for how long and for what purpose,
- how information has been amended or added to over time, and
- who has access to the data and why.

Everyone in the school / academy has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

## Information to Parents / Carers – the Privacy Notice and Consent

In order to comply with the fair processing requirements in data protection law, the school / academy will inform parents / carers of all pupils / students of the data they collect, process and hold on the pupils / students, the purposes for which the data is held and the third parties (e.g. LA, DfE, etc.) to whom it may be passed. This privacy notice will be passed to parents / carers for example in the prospectus, newsletters, reports or a specific letter / communication. Parents / carers of young people who are new to the school / academy will be provided with the privacy notice through an appropriate mechanism.

More information about the suggested wording of privacy notices can be found on the DfE website.

The DFE only publishes documents for England. But these template privacy notices may be suitable for amendment by schools / academies in other UK nations.

Consent under the regulation has changed. Consent is defined as:

"in relation to the processing of personal data relating to an individual, means a freely given, specific, informed and unambiguous indication of the individual's wishes by which the individual, by a statement or by a clear affirmative action, signifies agreement to the processing of the personal data"

This means that where a school / academy is relying on consent as the basis for processing personal data that consent has to be clear, meaning that pre-ticked boxes, opt-out or implied consent are no longer suitable. Pupils / students aged 13 or over (the age proposed in the Data Protection Bill, subject to Parliamentary approval) may be able to consent to their data being processed for the purposes of information society services. The GDPR does not specify an age of consent for general processing bur schools / academies should consider the capacity of pupils / students to freely give their informed consent.

Schools / academies should satisfy themselves that their consent forms are clear and written in plain language. Consent should also detail in a very clear and specific way why this is necessary, what will happen to the data, and, how and when it will be disposed of.

Consent is just one of the six lawful bases for processing data:

1. Consent:
2. Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
3. Legal obligation: the processing is necessary for you to comply with the law
4. Vital interests: the processing is necessary to protect someone's life.
5. Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
6. Legitimate interests: processing is necessary for the purposes of the legitimate interests pursued by the 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. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Previously maintained schools / academies were able to rely on the 'legitimate interests' justification. But under the new laws, this has been removed for Public Bodies (which includes schools as defined in Schedule 1 of the Freedom of Information Act 2000 and referenced in the UK Data Protection Bill 2017). This now means that should you wish to process the personal data of a child a risk assessment must be completed and justification documented.

## Parental permission for use of cloud hosted services

Schools / academies that use cloud hosting services are advised to seek appropriate consent to set up an account for pupils / students.

## Data Protection Impact Assessments (DPIA)

According to the ICO, Data Protection Impact Assessments (DPIA): "help organisations to identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy."

These will be carried out by Data Managers under the support and guidance of the DPO. These are intended to be carried out before processing activity starts, although some may need to be retrospective in the early stages of compliance activity.

The risk assessment will involve:

- Recognising the risks that are present
- Judging the level of the risks (both the likelihood and consequences)
- Prioritising the risks.

According to the ICO a DPIA should contain:

- A description of the processing operations and the purpose.
- An assessment of the necessity and proportionality of the processing in relation to the purpose.
- An assessment of the risks to individuals.
- The measures in place to address risk, including security and to demonstrate that you comply.

Or more simply and fully:

- Who did you talk to about this?
- What is going to happen with the data and how – collection, storage, usage, disposal
- How much personal data will be handled (number of subjects)
- Why you need use personal data in this way
- What personal data (including if it's in a 'special category') are you using
- At what points could the data become vulnerable to a breach (loss, stolen, malicious)
- What are the risks to the rights of the individuals if the data was breached
- What are you going to do in order to reduce the risks of data loss and prove you are compliant with the law

DPIA is an ongoing process and should be re-visited at least annually to verify that nothing has changed since the processing activity started.

## Special categories of personal data

The following list is a list of personal data listed in the GDPR as a 'special category'.
"revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"

In order to lawfully process special category data, you must identify both a lawful basis and a separate condition for processing special category data. You should decide and document this before you start processing the data.

## Use of Biometric Information

The Protection of Freedoms Act 2012, included measures that affect schools / academies that use biometric recognition systems, such as fingerprint identification and facial scanning:

- For all pupils in schools / academies under 18, they must obtain the written consent of a parent before they take and process their child's biometric data
- They must treat the data with appropriate care and must comply with data protection principles as set out in the Data Protection Act
- They must provide alternative means for accessing services where a parent or pupil has refused consent

New advice to schools / academies makes it clear that they are not able to use pupils' biometric data without parental consent. Schools / academies may wish to incorporate the parental permission procedures into revised consent processes.

## Training & awareness

All staff must receive data handling awareness / data protection training and will be made aware of their responsibilities, through opportunities such as:

- Induction training for new staff
- Staff meetings / briefings / INSET
- Day to day support and guidance from System Controllers

## Secure storage of and access to data

The school / academy should ensure that systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

Good practice suggests that all users will use strong passwords made up from a combination of simpler words. User passwords must never be shared.

Personal data may only be accessed on machines that are securely protected. Any device that can be used to access personal data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data should only be stored on school / academy equipment. Private equipment (i.e. owned by the users) must not be used for the storage of school / academy personal data.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected,
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school / academy policy once it has been transferred or its use is complete.

The school / academy will need to set its own policy as to whether data storage on removal media is allowed, even if encrypted. Some organisations do not allow storage of personal data on removable devices.

The school / academy should have a clear policy and procedures for the automatic backing up, accessing and restoring all data held on school / academy systems, including off-site backups.

The school / academy should have clear policy and procedures for the use of "Cloud Based Storage Systems" (for example Dropbox, Microsoft 365, Google drive) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school / academy will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data. The ICO produced guidance about cloud storage for organisations in 2012.

As a Data Controller, the school / academy is responsible for the security of any data passed to a "third party". Data Protection clauses must be included in all contracts where personal data is likely to be passed to a third party.

All paper based personal data must be held in lockable storage, whether on or off site.

## Subject Access Requests

Data subjects have a number of rights in connection with their personal data:

- Right to be informed – Privacy notices
- Right of access – Subject Access Request

- Right to rectification – correcting errors
- Right to erasure – deletion of data when there is no compelling reason to keep it
- Right to restrict processing – blocking or suppression of processing
- Right to portability – Unlikely to be used in a School / Academy context
- Right to object – objection based on grounds pertaining to their situation
- Rights related to automated decision making, including profiling

Clearly several of these have the opportunity to impact on schools / academies, one being the right of access. Procedures must be in place to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. The school must provide the information free of charge, however a 'reasonable fee' may be charged where the request is manifestly unfounded or excessive, especially if this is a repetitive request. See later information on Records of Processing Activity.

## Secure transfer of data and access out of school

The school / academy recognises that personal data may be accessed by users out of school / academy, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school / academy or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school / academy
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event.

## Disposal of data

The school / academy should implement a document retention schedule that defines the length of time data is held before secure destruction. The Information and Records Management Society Toolkit for schools provide support for this process. The school / academy must ensure the safe destruction of personal data when it is no longer required.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely disposed of, and other media must be shredded, incinerated or otherwise disintegrated.

A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

## Audit Logging / Reporting / Incident Handling

Organisations are required to keep records of processing activity. This must include:

- The name and contact details of the data controller
- Where applicable, the name and contact details of the joint controller and data protection officer
- The purpose of the processing
- To whom the data has been/will be disclosed
- Description of data subject and personal data
- Where relevant the countries it has been transferred to
- Under which condition for processing the data has been collected
- Under what lawful basis processing is being carried out
- Where necessary, how it is retained and destroyed
- A general description of the technical and organisational security measures.

Clearly, in order to maintain these records good auditing processes must be followed, both at the start of the exercise and on-going throughout the lifetime of the requirement. Therefore audit logs will need to be kept to:

- provide evidence of the processing activity and the DPIA
- record where, how and to whom data has been shared
- log the disposal and destruction of the data
- enable the School / Academy to target training at the most at-risk data
- record any breaches that impact on the data

It then follows that in the event of a data breach, the school/ college should have a policy for reporting, managing and recovering from information risk incidents, which establishes:

- a "responsible person" for each incident
- a communications plan, including escalation procedure
- and results in a plan of action for rapid resolution
- a plan of action of non-recurrence and further awareness raising

All significant data protection incidents must be reported through the DPO to the Information Commissioner's Office based upon the local incident handling policy and communication plan. The new laws require that this notification should take place within 72 hours of the breach being detected, where feasible.

## Data Mapping

The process of data mapping is designed to help schools / academies identify with whom their data is being shared in order that the appropriate contractual arrangements can be implemented. If a third party is processing personal data on your behalf about your students then this processor has obligations on behalf of the school / academy to ensure that processing takes place in compliance with data protection laws.

## Privacy and Electronic Communications

Schools / academies should be aware that they are subject to the Privacy and Electronic Communications Regulations in the operation of their websites.