Appendix C2 Personal Data Advice and Guidance

Data Protection Law – A Legislative Context

With effect from 25th May 2018, the data protection arrangements for the UK changed following the implementation of the European Union General Data Protection Regulation (GDPR). This represented a significant shift in legislation and in conjunction with the Data Protection Act 2018 replaced the Data Protection Act 1998.

After the end of the Brexit transition period, the GDPR is expected to be incorporated into UK law. The 'UK GDPR' will sit alongside an amended version of the DPA 2018 and means the UK will have the independence to keep the framework under review. Therefore, the key principles, rights and obligations are predicted to remain the same. However, there are implications regarding the rules for transferring personal data between the UK and the EEA.

Please be aware that the Data Protection Act 2018 (DPA2018) sits alongside the GDPR (i.e. the laws complement each other). The DPA2018 tailors how the GDPR applies to the UK and covers aspects not included in the GDPR, such as Law Enforcement processing and exemptions about how to handle education and child protection data.

In this document the term "Data Protection Law" refers to the legislation applicable to data protection and privacy as applicable in the UK.

Does the Data Protection Law apply to schools?

In short, yes. All schools process personal data and are considered a separate 'data controller' for the purposes of data protection.

Personal data is "any information relating to an identified or identifiable natural person ('data subject')". An identifiable natural person is one who can be identified, directly or indirectly, by reference to:

- an identifier such as a name, an identification number, location data, an online identifier or
- to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

Some types of personal data are known as 'special categories of personal data' and include the following:

"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"

The school must identify both a lawful basis (Article 6 of the GDPR) and a separate condition for processing special category data (Article 9 of the GDPR). These should be decided prior to any processing taking place, and further guidance is available on the Information Commissioner's Office (ICO) website

The ICO's powers are wide ranging in the event of non-compliance and schools must be aware of the huge impact that a fine or investigation will have on finances and also in the wider community for example in terms of trust.

The Data Protection Law sets out that a data controller must ensure that personal data shall be:

a) processed lawfully, fairly and in a transparent manner;
b) collected for specified, explicit and legitimate purposes ("purpose limitation");
c) adequate, relevant and limited to what is necessary ("data limitation");
d) accurate and, where necessary, kept up to date;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ("storage limitation"); and
f) processed in a manner that ensures appropriate security of the personal data

An overall principle of accountability requires the school to be responsible for and demonstrate compliance with data protection law.

Data protection law requires the school to always have a lawful basis for processing personal data. These can be summarised as:

(a) Consent:	the data subject has given clear consent for you to process their personal data for a specific purpose (see below for further guidance)
(b) 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.
(c) Legal obligation:	the processing is necessary for you to comply with the law (not including contractual obligations).
(d) Vital interests:	the processing is necessary to protect someone's life.
(e) 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.
(f) Legitimate interests:	the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks).

No single basis is 'better' or more important than the others and which basis is most appropriate to use will depend on your purpose and relationship with the data subject.

Data Mapping to identify personal data, data subjects and processing activities

The school and its employees will collect and/ or process a wide range of information concerning numerous data subjects and some of this information will include personal data. Further, the school may need to share some personal data with third parties. To be able to demonstrate and plan compliance and it is important that the school has a data map of these activities. These inform privacy notices and help put security measures in place to keep personal data secure, including steps to avoid a breach, and ensure Data Processing Agreements (i.e. contracts) are in place with the suppliers or contractors.

The data map should identify what personal data is held in digital format or on paper records in a school, where the information is stored, why it is processed, and how long it is retained.

In a typical data map for a school, the data subjects and personal data will include, but are not limited to:

- Parents, legal guardians, governors: personal data of names, addresses, contact details
- Learners: curricular / academic data (e.g. class lists, learner progress records, reports, references, contact details, health and SEN reports)
- Staff and contractors: professional records (e.g. employment history, taxation and national insurance records, appraisal records and references, health records).

The ICO have advice and guidance on keeping a Record of Processing Activities.

The school will need to identify appropriate lawful process criteria for each type of personal data, and if this is not possible, such activities should be discontinued.

A school can use the public task lawful basis if processing takes place to perform an official task as set down in UK law (e.g. Education Act 1996):

"processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller" (Article 6(1)(e) of the GDPR)

If not, the school should consider each of the other lawful bases for processing in turn to assess how they fit with the processing and relationship with the data subject. As a public authority, please remember that legitimate interests cannot be used as a lawful basis when processing personal data to perform an official task or a public function.

The rules around consent should be considered carefully, as another lawful basis may be more appropriate. GDPR sets a high standard for consent and should put individuals in charge. Consent is now defined as:

"in relation to the processing of personal data relating to an individual … 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 consent must be freely given, specific, informed, and an unambiguous indication of wishes by a statement or affirmative action. As a result, consent forms should be clear and concise;

include an opt-in, granular approach; as well as explain why information is collected and how it will be processed to inform individuals. Implied consent is no longer suitable.

The DPA2018 modifies the GDPR so that the minimum age for consent to be obtained from a child is lowered to 13 years old.

The Information Commissioner's Office (ICO) gives clear advice on when it's appropriate to use consent as a lawful base. It states:

"Consent is appropriate if you can offer people real choice and control over how you use their data and want to build their trust and engagement. But if you cannot offer a genuine choice, consent is not appropriate. If you would still process the personal data without consent, asking for consent is misleading and inherently unfair."

The school should only use consent if none of the other lawful bases are appropriate. If you do so, you must be able to cope with people saying no (and/or changing their minds). Therefore, it's important that you only use consent for optional extras, rather than for core information the school requires in order to carry out its function. The below are examples where consent may or may not be appropriate;

- consent should be obtained when publishing a child's photo in any way (i.e. a school website, newsletter, prospectus, or social media).
- the school is required to hold learner and parent/carer details in an Management Information System (MIS.) Therefore, it would not be appropriate to rely on consent, as the individual(s) would then have the right to opt out of the processing. In this case, the school could apply the 'public task' lawful basis.
- The school is required to share information for the purposes of child protection issues. As a result, it would not be appropriate to rely on consent, as the individual(s) would have the right to opt out of the processing. The school could also alert an individual about an allegation made against them. In this case, the school could apply the public task lawful basis.

Content of Privacy Notices

Privacy Notices are a key compliance requirement as they ensure that each data subject is aware of the following points when data is collected/ processed by a data controller:

- the identity and contact details of the data controller
- what categories of personal data are being processed
- the purposes and lawful basis for processing the personal data
- where and how the personal data was sourced
- to whom the personal data may be shared with
- whether any personal data is transferred to a country outside of the EEA
- how long the personal data will be stored and retained
- the contact details of the Data Protection Officer

- the existence of automated decision making, including profiling
- data subject's rights and how to exercise them
- details of how to make a complaint to the school or ICO.

The right to be informed is closely linked to the fair processing and transparency requirements of data protection principles. In order to comply, the school must provide parents/carers and learners with the above information when collecting personal data from individuals and ensure a privacy notice is easily accessible throughout the processing. For example, privacy notices could be passed to parents/carers and learners in the school prospectus, newsletters, or a specific letter/communication. The school could publish privacy notices on the school website. Parents/carers and learners who are new to the school should be provided with the privacy notice through an appropriate mechanism. Please be aware, however, that different forms of processing require a Privacy Notice, such as when processing visitor information or using personal data for employment purposes.

A school should ensure that privacy notices are available for learners as data subjects. Children and young people have the same rights as adults when it comes to their personal data. These include the rights described below and policies that explain this should be clear and age appropriate.

Data subject's right of access

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

- Right to be informed how personal data is collected, stored, managed, protected, and processed.
- Right of access to request a copy of personal information held of yourself. However, please be aware that information can sometimes be legitimately withheld.
- Right to rectification of inaccurate or incomplete personal data.
- Right to erasure where you have the right to have your personal data erased in certain circumstances. This does not include any personal data that must be retained by law.
- Right to restriction, which allows you to limit the way we use your personal data in some circumstances.
- Right to portability gives an individual the right to receive copies of data provided to a controller in a portable format.
- Right to object to the processing of one's personal data.
- Rights in relation to automated decision making and profiling.

Several of these are likely impact schools, such as the right of access. Therefore, the school should put procedures in place to deal with Subject Access Requests and other individual rights requests (e.g. erasure and rectification).

Subject Access Requests are probably the most common individual right request made to any organisation. These are written or verbal requests to access all or a part of the personal data held by the Data Controller in connection with a living individual. Controllers have one calendar month to provide the information, unless the case is unusually complex and an extension can be obtained.

A school must consider all information requested for disclosure. However, there are instances where personal data must not be disclosed to the applicant, even if requested:

- the personal data of any third parties (not relating to the data subject)
- if doing so would cause serious harm to the individual
- child abuse data
- adoption records
- Individual Development Plans for learners with Additional Learning Needs (ALN).

Your school must provide the information free of charge. However, there are occasional instances where a reasonable fee can be charged, for example if the request is clearly unfounded, or excessive.

Personal data breaches and how to manage them

Schools are "data rich" and hold a large volume of personal data on the learners in their care. This data can be in paper (i.e. manual records) and electronic format (e.g. shared drives, electronic databases, and Cloud solutions). Personal data is increasingly being held digitally with the introduction of electronic storage solutions (e.g. Google Drive) and the digital transfer or sharing of information. As a result, personal data is more accessible and the potential for data loss has increased significantly, especially where staff are working from remote locations (such as at home, other schools, or even public spaces).

Data protection law applies to all forms of personal data, regardless of whether it is held on paper or in electronic format. However, this document will place emphasis on data that is held or transferred digitally due to being part of an overall Online Safety Policy template.

A personal data breach is described as a *"breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"*. As a result, there is more to a personal data breach than simply losing personal data, and breaches can be the result of both accidental and deliberate causes. For example, 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 or a pupil, accidental loss of equipment or paper records, or equipment failure.

An important part of managing a personal data breach is for the school to have a clear and well understood procedure for reporting breaches so they can implement actions and minimise any further risk. The school should have a policy for reporting, logging, managing and recovering from incidents, which establishes:

- a "responsible person" for reporting and investigating incidents
- how to manage personal data breaches, including an escalation procedure
- criteria for determining incident level and timescales, which should help to:

The school may find it useful to develop an incident report form template for staff to complete if a personal data breach is discovered. These forms support the school to record all the information required to analyse the incident and comply with the accessibility principle. An example form should include the following.

All 'high risk' breaches must be reported to the Information Commissioner's Office through the DPO based upon the school procedure for reporting incidents. Data protection laws require this notification to take place within 72 hours of becoming aware of the breach (where feasible).

Schools must consider whether an incident discovered poses a risk to the individuals (i.e. data subjects) involved, including the likelihood and severity of any risk to people's rights and freedoms. If the assessment suggested a high risk is unlikely, the incident does not need to be reported. However, there is a legal duty under data protection law to document the facts relating to a breach, its effects, and the remedial action taken by the organisation. The school should, therefore, maintain a log of all incidents.

Data Protection Impact Assessments (DPIAs)

Data Protection Impact Assessments (DPIAs) identify and assess privacy risks early on in a project that processes personal data to enable the school to mitigate them before the project launches.

DPIAs should be carried out by project leads under the support and guidance of the DPO. Schools should conduct a DPIA before processing activity starts and run alongside the planning and development process.

- Step 1: Identify the need for using personal data
- Step 2: Describe the information flows
- Step 3: Identify the privacy and related risks
- Step 4: Identify privacy solutions
- Step 5: Sign off and record the DPIA outcomes
- Step 6: Integrate the DPIA outcomes back into the project plan

Data protection law requires a DPIA to be completed where processing is likely to result in a high risk to the rights and freedoms of individuals and for the below types of processing:

1. Systematic and extensive profiling with significant effects
2. Large scale use of sensitive data (i.e. special category or criminal data)
3. Public monitoring (i.e. CCTV)

For more information about DPIAs, please see this guidance on the ICO website.

A DPIA should contain the following:

- a description of the processing 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

and could be laid out in this way:

Describe source of risk and potential impact on individuals	**Likelihood of harm** Remote, possible or probable	**Severity of harm** Minimal, significant, or severe	**Overall risk** Low medium high*	**If medium or high, options to reduce or eliminate risk**	**Effect on risk** Eliminated, reduced, or accepted	**Residual risk** Low medium high*	**Measure approved** yes/no

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

Secure storage of and access to data

The school should ensure that systems are set up so that the existence of protected files is hidden from unauthorised users and those processing personal data will be assigned appropriate access. For example, 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, numbers, and special characters. 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 equipment. Private equipment (i.e. owned by the users) must not be used for the storage of school 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 offer approved virus and malware checking software
- The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

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

Clear policies and procedures should be in place for the use of "Cloud Based Storage Systems" (e.g. Dropbox, Microsoft 365, Google Drive). Please be aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school must ensure that it is satisfied with controls put in place by remote/cloud-based data services providers to protect the data. In Wales, all schools have access to Microsoft Office 365 and G-Suite for Education via Hwb. For more information please visit the Data Governance section of Hwb.

As a Data Controller, the school is responsible for the security of any data passed to a "third party". Specific data processing clauses must be included in all contracts where personal data is likely to be passed to a third party. These require a Data Processor that is processing personal data on behalf of the school to:

- only act on the written instructions of the school
- ensure that staff processing the personal data are subject to a duty of confidence
- take appropriate measures to ensure the security of processing
- only engage sub-processors with the prior consent of the controller, and under a written contract
- assist the controller in providing subject access to information and allowing data subjects to exercise their rights under the GDPR
- assist the controller in meeting its data protection obligations in relation to the security of processing, including the notification of personal data breaches and carrying out DPIAs
- delete or return all personal data to the controller as requested at the end of the contract
- provide the controller with whatever information it needs to ensure that they are both meeting their data protection obligations
- tell the controller immediately if it is asked to do something infringing the GDPR, Data Protection Act 2018.

Secure transfer of data and access out of school

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

- Users may not remove or copy sensitive/restricted/protected personal data from the school or authorised premises without permission. Media should be encrypted and password protected and transferred 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.
- Secure remote access to a management information system or learning platform is preferable when personal data (particularly special categories of personal data) is required by an authorised user from outside the organisation's premises (e.g. by a member of staff to work from their home). 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 transferred to another country (particularly outside Europe) and advice should be sought from the Data Protection Officer in this event.

Disposal of personal data

The school should implement a retention schedule that defines the length of time personal data is held before secure destruction. The Information and Records Management Society Toolkit for schools provides support for this process. The school 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 record of destruction log (i.e. Schedule for Disposal/Destruction) should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

Demonstrating Compliance - Audit Logging / Reporting / Incident Handling

Organisations are required to keep records of processing activity. The data map referred to above will assist here. Records 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 (DPO)
- 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 personal 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.

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, why, how and to whom personal data has been shared
- log the disposal and destruction of the personal data
- enable the school to target training at the most at-risk data
- record any breaches that impact on the personal data.

Data Protection Fee

Schools are required to pay the relevant annual fee to the Information Commissioner's Office (ICO) by law. This means the school is breaking the law if, as a data controller, it processes personal data and has either not paid a fee, or not paid the correct fee.

Responsibilities

Every maintained school is required to appoint an independent Data Protection Officer (DPO) as a core function of 'the business'

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 DPIA
- 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 law.

The school may also wish to appoint a Data Manager or Information Governance Lead. Schools 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 information risk policy and risk assessment
- oversee the System Controllers.

The school may also wish to appoint staff members to be responsible for the various types of data being held (e.g. learner information / staff information / assessment data etc.). These staff members 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 has the responsibility for handling protected or sensitive data (including learner data) in a safe and secure manner.

Governors are required to comply fully with this policy where they have access to personal data as part of their role as a Governor (either in the school or elsewhere if on school business).

Training & awareness

All staff must receive data handling awareness / data protection training and will be made aware of their responsibilities. This should be undertaken regularly. You can do this through:

- Induction training for new staff
- Annual data protection training for all staff
- Staff meetings / briefings / INSET
- Day to day support and guidance.

Freedom of Information Act

All schools must have a Freedom of Information (FOI) Policy which sets out how it will deal with FOI requests. FOI aims to increase "openness by design" in public sector organisations as part of a healthy democratic process. FOI requests are submitted by an individual and the school are required to consider whether the requested information should be released into the public domain. Any requests for personal data should be dealt with under data protection law. The FOI Section 40(1) and (2) exemption covers personal data.

Good advice would encourage the school to:

- delegate to the Headteacher day-to-day responsibility for FOI policy and the provision of advice, guidance, publicity and interpretation of the school's policy

- consider designating an individual with responsibility for FOI, to provide a single point of reference, and coordinate FOI (including related policies and procedures). The school should 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 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 publication scheme should be reviewed annually.

The ICO produce guidance on the model publication scheme for schools. This is designed to support schools in completing the Guide to Information for Schools.

Parental permission for use of cloud hosted services

Schools that use cloud hosting services are advised to identify the relevant lawful basis to set up an account for learners.

Use of Biometric Information

Biometric information is special category data. The Protection of Freedoms Act 2012 included measures that affect schools that use biometric recognition systems, such as fingerprint identification and facial scanning:

- For all pupils in schools 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 law.
- They must provide alternative means for accessing services where a parent or pupil has refused consent.

New advice to schools makes it clear that they are not able to use pupils' biometric data without parental consent. Schools may wish to incorporate the parental permission procedures into revised consent processes. (see Appendix Parent/carer Acceptable Use Agreement)

Privacy and Electronic Communications

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