Data Protection, GDPR, Freedom of Information & Protection of Biometric Information of Pupils Policy

1. Introduction

The General Data Protection Regulation (GDPR) together with the new Data Protection Act (DPA) 2018 came into force from 25 May 2018, replacing the Data Protection Act 1998. This is the law that protects personal privacy and upholds individual's rights. It applies to anyone who handles or has access to people's personal data. The GDPR imposes new requirements (relating to the appointment of a data protection officer (DPO) and notification of personal data breaches) and provides new rights for individuals. This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the Data Protection Act. It will apply to information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

Note: Since the United Kingdom (UK) left the European Union (EU) the UK no longer is subject to the EU GDPR. With effect from 31 January 2020 a new UK-GDPR has been in place alongside the Data Protection Act 2018. The UK-GDPR is very similar to the EU-GDPR.

The Federation of St Martin's & Seabrook CEP Schools is a "public authority" and "data controller" within the meaning of the Freedom of Information Act 2000 and Data Protection Act 2018, respectively. Accordingly, subject to the obligations and requirements of the law the Federation will, in the course of its day-to-day activities, determine the purposes for which and the manner in which any personal data are, or are to be, processed; and will also provide certain information in response to a request in writing to do so on the basis of a general right of access, particularly in relation to a right of access to personal data.

The Acts referred to above contain much detail and are complex pieces of legislation. It follows that this policy does not seek to replicate or to provide an exhaustive interpretation of their provisions nor to prescribe each and every case where certain information will or will not be given. Instead the intention is to set out a broad understanding of the spirit and intention of the law in this area and how, generally speaking, the Federation will seek to comply with it. In the event of any conflict or inconsistency then the provisions of the Acts themselves shall prevail.

2. Policy Objectives

The Federation, as the Data Controller, will comply with its obligations under the UK - GDPR and DPA. The Federation is committed to being concise, clear and transparent about how it obtains and uses personal information and will ensure data subjects are aware of their rights under the legislation.

All staff must have a general understanding of the law and understand how it may affect their decisions in order to make an informed judgement about how information is gathered, used and ultimately deleted. All staff must read, understand and comply with this policy.

The Information Commissioner as the Regulator can impose fines of up to £17.5million for serious breaches of the UK - GDPR, therefore it is imperative that the Federation and all staff comply with the legislation.

3. Scope of the Policy

Personal data is any information that relates to an identified or identifiable living individual who can be identified directly or indirectly from the information. The information includes factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a living individual. This includes any expression of opinion about an individual and intentions towards an individual. Under the

GDPR personal information also includes an identifier such as a name, an identification number, location data or an online identifier.

The Federation collects a large amount of personal data every year including: pupil records, staff records, names and addresses of those requesting prospectuses, examination marks, references as well as many different types of research data used by the Federation. The personal data held by the Federation in relation to its pupils is mainly used to support teaching and learning; to monitor and to report on progress; to provide appropriate pastoral care; and to assess how well the Federation is performing in its role and also to help other bodies to evaluate the effectiveness of the National Curriculum. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of the Local Authority (LA), government agencies and other bodies.

4. The Principles

The principles set out in the GDPR must be adhered to when processing personal data:

1. Personal data must be processed lawfully, fairly and in a transparent manner (**lawfulness, fairness and transparency**).
2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (**purpose limitation**).
3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed (**data minimisation**).
4. Personal data shall be accurate and where necessary kept up to date and every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay (**accuracy**).
5. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data is processed (**storage limitation**).
6. Appropriate technical and organisational measures shall be taken to safeguard the rights and freedoms of the data subject and to ensure that personal information is processed in a manner that ensures appropriate security of the personal data and protects against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data (**integrity and confidentiality**).

5. Transfer Limitation

An agreement has been reached between the UK and the EU that personal data may continue to flow unrestricted between the UK and countries within the EEA (European Economic Area) at least until June 2025. However, personal data shall not be transferred to a country outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data or where the organisation receiving the data has provided adequate safeguards.

This means that individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer. It may also be possible to transfer data where the data subject has provided explicit consent or for other limited reasons. Staff should contact the Data Protection Officer (DPO) if they require further assistance with a proposed transfer of personal data outside of the EEA.

6. Lawful Basis for Processing Personal Information

Before any processing activity starts for the first time, and then regularly afterwards, the purpose(s) for the processing activity and the most appropriate lawful basis (or bases) for that processing must be selected:

- 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 Federation.

- Processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract.

- Processing is necessary for compliance with a legal obligation to which the data controller is subject.

- Processing is necessary in order to protect the vital interests of the data subject or of another natural person.

- Processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party.

- The data subject has given consent to the processing of his or her data for one or more specific purposes. Agreement must be indicated clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, the consent must be kept separate from those other matters.

- Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be reviewed if personal data is intended to be processed for a different and incompatible purpose which was not disclosed when the data subject first gave consent.

The decision as to which lawful basis applies must be documented, to demonstrate compliance with the data protection principles and include information about both the purposes of the processing and the lawful basis for it in the Federation's relevant privacy notice(s).

When determining whether legitimate interests are the most appropriate basis for lawful processing (only where appropriate outside the Federation's public tasks) a legitimate interests assessment must be carried out and recorded. Where a significant privacy impact is identified, a data protection impact assessment (DPIA) may also need to be conducted.

7. Sensitive Personal Information

Processing of sensitive personal information (known as 'special categories of personal data') is prohibited unless a lawful special condition for processing is identified.

Sensitive personal information is data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life or orientation or is genetic or biometric data which uniquely identifies a natural person.

Sensitive personal information will only be processed if:

- There is a lawful basis for doing so as identified above.
- One of the special conditions for processing sensitive personal information applies:
    (a) The individual ('data subject') has given explicit consent (which has been clearly explained in a Privacy Notice).
    (b) The processing is necessary for the purposes of exercising the employment law rights or obligations of the Federation or the data subject.
    (c) The processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent.
    (d) The processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim.

(e) The processing relates to personal data which are manifestly made public by the data subject.
(f) The processing is necessary for the establishment, exercise or defence of legal claims.
(g) The processing is necessary for reasons of substantial public interest.
(h) The processing is necessary for purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, the provision of social care and the management of social care systems or services.
(i) The processing is necessary for reasons of public interest in the area of public health.

The Federation's privacy notice(s) set out the types of sensitive personal information that it processes, what it is used for, the lawful basis for the processing and the special condition that applies. Sensitive personal information will not be processed until an assessment has been made of the proposed processing as to whether it complies with the criteria above and the individual has been informed (by way of a privacy notice or consent) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

Unless the Federation can rely on another legal basis of processing, explicit consent is usually required for processing sensitive personal data. Evidence of consent will need to be captured and recorded so that the Federation can demonstrate compliance with the UK - GDPR.

8. Automated Decision Making

Where the Federation carries out automated decision making (including profiling) it must meet all the principles and have a lawful basis for the processing. Explicit consent will usually be required for automated decision making (unless it is authorised by law or it is necessary for the performance of or entering into a contract).

Additional safeguards and restrictions apply in the case of solely automated decision-making, including profiling. The Federation must as soon as reasonably possible notify the data subject in writing that a decision has been taken based on solely automated processing and that the data subject may request the Federation to reconsider or take a new decision. If such a request is received staff must contact the DPO as the Federation must reply within 21 days.

9. Data Protection Impact Assessments (DPIA)

All data controllers are required to implement 'Privacy by Design' when processing personal data.

This means the Federation's processes must embed privacy considerations and incorporate appropriate technical and organisational measures (like pseudonymisation) in an effective manner to ensure compliance with data privacy principles.

Where processing is likely to result in high risk to an individual's data protection rights (for example where a new technology is being implemented) a DPIA must be carried out to assess:

- Whether the processing is necessary and proportionate in relation to its purpose.
- The risks to individuals.
- What measures can be put in place to address those risks and protect personal information.

Staff should adhere to the Data Protection Toolkit for Schools from the DfE with reference to the DPIA template.

When carrying out a DPIA, staff should seek the advice of the DPO for support and guidance and once complete, refer the finalised document to the DPO for sign off.

10. Documentation and Records
Written records of processing activities must be kept and recorded including:

- The name(s) and details of individuals or roles that carry out the processing.
- The purposes of the processing.
- A description of the categories of individuals and categories of personal data.
- Categories of recipients of personal data.
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place.
- Retention schedules.
- A description of technical and organisational security measures.

As part of the Federation's record of processing activities the DPO will document, or link to documentation on:

- information required for privacy notices
- records of consent
- controller-processor contracts
- the location of personal information
- DPIAs
  and
- records of data breaches.

Records of processing of sensitive information are kept on:

- the relevant purposes for which the processing takes place, including why it is necessary for that purpose
- the lawful basis for our processing
  and
- whether the personal information is retained or erased in accordance with the Retention Schedule and, if not, the reasons for not following the policy.

The Federation should conduct regular reviews of the personal information it processes and update its documentation accordingly. This may include:

- Carrying out information audits to find out what personal information is held.
- Talking to staff about their processing activities.
- Reviewing policies, procedures, contracts and agreements to address retention, security and data sharing.

11. Privacy Notice
The Federation will issue privacy notices as required, informing data subjects (or their parents, depending on age of the pupil, if about pupil information) about the personal information that it collects and holds relating to individual data subjects, how individuals can expect their personal information to be used and for what purposes.

When information is collected directly from data subjects, including for HR or employment purposes, the data subject shall be given all the information required by the UK-GDPR including the identity of the DPO, how and why the Federation will use, process, disclose, protect and retain that personal data through a privacy notice (which must be presented when the data subject first provides the data).

When information is collected indirectly (for example from a third party or publicly available source) the data subject must be provided with all the information required by the UK-GDPR as soon as possible after collecting or receiving the data. The Federation must also check that the data were collected by the third party in accordance with the UK-GDPR and on a basis which is consistent with the proposed processing of the personal data.

The Federation will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

The Federation will issue a minimum of two privacy notices, one for pupil information, and one for workforce information, and these will be reviewed in line with any statutory or contractual changes.

12. Purpose Limitation

Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

Personal data must not be used for new, different or incompatible purposes from that disclosed when it was first obtained unless the data subject has been informed of the new purposes and they have consented where necessary.

13. Data Minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

Staff may only process data when their role requires it. Staff must not process personal data for any reason unrelated to their role.

The Federation maintains a Retention Schedule to ensure personal data are deleted after a reasonable time for the purpose for which it was being held, unless a law requires such data to be kept for a minimum time. Staff must take all reasonable steps to destroy or delete all personal data that are held in its systems when they are no longer required in accordance with the Schedule. This includes requiring third parties to delete such data where applicable.

Staff must ensure that data subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

14. Individual Rights

Staff as well as any other 'data subjects' have the following rights in relation to their personal information:

- To be informed about how, why and on what basis that information is processed *(see the relevant privacy notice).*
- To obtain confirmation that personal information is being processed and to obtain access to it and certain other information, by making a subject access request.
- To have data corrected if they are inaccurate or incomplete.
- To have data erased if they are no longer necessary for the purpose for which they were originally collected/processed, or if there are no overriding legitimate grounds for the processing ('the right to be forgotten').
- To restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased) or where the

Federation no longer needs the personal information, but the data are required to establish, exercise or defend a legal claim.
- To restrict the processing of personal information temporarily where you do not think it is accurate (and the Federation is verifying whether it is accurate), or where you have objected to the processing (and the Federation is considering whether the Federation's legitimate grounds override your interests).
- In limited circumstances to receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format.
- To withdraw consent to processing at any time (if applicable).
- To request a copy of an agreement under which personal data are transferred outside of the EEA.
- To object to decisions based solely on automated processing, including profiling.
- To be notified of a data breach which is likely to result in high risk to their rights and obligations.
- To make a complaint to the Information Commissioner's Office (ICO) or a Court.

15. Individual Responsibilities

During their employment, staff may have access to the personal information of other members of staff, suppliers, clients or the public. The Federation expects staff to help meet its data protection obligations to those individuals.

If you have access to personal information, you must:

- Only access the personal information that you have authority to access and only for authorised purposes.
- Only allow other staff to access personal information if they have appropriate authorisation.
- Only allow individuals who are not Federation staff to access personal information if you have specific authority to do so.
- Keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction in accordance with the Federation's policies).
- Not remove personal information, or devices containing personal information (or which can be used to access it) from the Federation's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device.
- Not store personal information on local drives or on personal devices that are used for work purposes.

16. Information Security

The Federation will use appropriate technical and organisational measures to keep personal information secure, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

All staff are responsible for keeping information secure in accordance with the legislation and must follow the Federation's acceptable usage policy.

The Federation will develop, implement and maintain safeguards appropriate to its size, scope and business, its available resources, the amount of personal data that it owns or maintains on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). It will regularly evaluate and test the effectiveness of those safeguards to ensure security of processing.

Staff must guard against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. Staff must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure.

Staff must follow all procedures and technologies put in place to maintain the security of all personal data from the point of collection to the point of destruction. Staff may only transfer personal data to third-party service providers who agree in writing to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

Staff must maintain data security by protecting the **confidentiality, integrity and availability** of the personal data, defined as follows:

> **Confidentiality** means that only people who have a need to know and are authorised to use the personal data can access the data.
>
> **Integrity** means that personal data are accurate and suitable for the purpose for which it is processed.
>
> **Availability** means that authorised users can access the personal data when they need the data for authorised purposes.

Staff must comply with and not attempt to circumvent the administrative, physical and technical safeguards the Federation has implemented and maintains in accordance with the UK-GDPR and DPA.

Where the Federation uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. Contracts with external organisations must provide that:

- The organisation may only act on the written instructions of the Federation.
- Those processing data are subject to the duty of confidence.
- Appropriate measures are taken to ensure the security of processing.
- Sub-contractors are only engaged with the prior consent of the Federation and under a written contract.
- The organisation will assist the Federation in providing subject access and allowing individuals to exercise their rights in relation to data protection.
- The organisation will delete or return all personal information to the Federation as requested at the end of the contract.
- The organisation will submit to audits and inspections, provide the Federation with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the Federation immediately if it does something infringing data protection law.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval from the DPO.

17. Storage and Retention of Personal Information

Personal data will be kept securely in accordance with the Federation's data protection obligations.

Personal data should not be retained for any longer than necessary. The length of time data should be retained will depend upon the circumstances, including the reasons why personal data were obtained. Staff should adhere to the KCC Information Management Toolkit for Schools on KELSI with reference to the Record Retention Schedule.
Personal information that is no longer required will be deleted in accordance with the Federation's Record Retention Schedule.

18. Data breaches
A data breach may take many different forms:

- Loss or theft of data or equipment on which personal information is stored.
- Unauthorised access to or use of personal information either by a member of staff or third party.
- Loss of data resulting from an equipment or systems (including hardware or software) failure.
- Human error, such as accidental deletion or alteration of data.
- Unforeseen circumstances, such as a fire or flood.
- Deliberate attacks on IT systems, such as hacking, viruses or phishing scams.
- Blagging offences where information is obtained by deceiving the organisation which holds it.

The Federation must report a data breach to the Information Commissioner's Office (ICO) without undue delay and where possible within 72 hours, if the breach is likely to result in a risk to the rights and freedoms of individuals. The Federation must also notify the affected individuals if the breach is likely to result in a high risk to their rights and freedoms.
Staff should ensure they inform the Executive Headteacher immediately that a data breach is discovered and make all reasonable efforts to recover the information, following the Federation's agreed breach reporting process.

19. Training
The Federation will ensure that staff are adequately trained regarding their data protection responsibilities.

20. Consequences of a failure to comply
The Federation takes compliance with this policy very seriously. Failure to comply puts data subjects whose personal information is being processed at risk and carries the risk of significant civil and criminal sanctions for the individual and the Federation and may in some circumstances amount to a criminal offence by the individual.

Any failure to comply with any part of this policy may lead to disciplinary action under the Federation's procedures and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

If you have any questions or concerns about this policy, you should contact the Executive Headteacher.

21. Review of Policy
This policy will be updated as necessary to reflect best practice or amendments made to the UK-GDPR or DPA.

22. Freedom of Information
The Freedom of Information Act 2000 provides public access to information held by public authorities.

It does this in two ways:
(a) public authorities are obliged to publish certain information about their activities; and
(b) members of the public are entitled to request information from public authorities.

The main principle behind freedom of information legislation is that people have a right to know about the activities of public authorities, unless there is a good reason for them not to. This is sometimes described as a presumption or assumption in favour of disclosure. The Act is also sometimes described as purpose and applicant blind.

In accordance with the Freedom of Information Act, the Federation will adhere to its two main obligations:
(a) to publish certain information proactively as determined by the Local Authority, the Diocese and/or the DfE.
(b) To respond to requests for information in accordance with legal requirements.

23. Requests and fees
Any request for personal data or other information should be submitted to the Federation in writing for the attention of the Executive Headteacher and, depending on the nature of the request, will usually be responded to within 14 days and incur no charge. Requests of an exceptional nature however may take longer to deal with and may incur a charge.

24. Role of the Data Protection Officer (DPO)
The Federation uses Accordio to provide the services of the DPO across the Federation.

25. The Supervisory Authority in the UK and Other Sources of Information
Further information on data protection and freedom of information matters, including individuals' rights, data breaches, dealing with subject access requests, how to handle requests from third parties for personal data to be disclosed can be obtained from the Information Commissioner's Office at www.ico.gov.uk.

26. Use of Biometric Information

(a) What is biometric data?
Biometric data means personal information about an individual's physical or behavioural characteristics that can be used to identify that person; this can include their fingerprints, facial shape, retina and iris patterns, and hand measurements.

The Information Commissioner considers all biometric information to be personal data as defined by the Data Protection Act 1998; this means that it must be obtained, used and stored in accordance with that Act.

The Protection of Freedoms Act includes provisions which relate to the use of biometric data in schools when used as part of an automated biometric recognition system. These provisions are in addition to the requirements of the Data Protection Act 1998.

(b) What is an automated biometric recognition system?
An automated biometric recognition system uses technology which measures an individual's physical or behavioural characteristics by using equipment that operates 'automatically' (i.e. electronically). Information from the individual is automatically compared with biometric information stored in the system to see if there is a match in order to recognise or identify the individual.

Biometric recognition systems can use many kinds of physical or behavioural characteristics such as those listed in the above section of 'What is biometric data'.

(c) Federation's use of biometric information
Currently, the Federation does **not** capture, process or use biometric information.

Glossary

Automated Decision-Making (ADM): when a decision is made which is based solely on automated processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits automated decision-making (unless certain conditions are met) but not automated processing.

Automated Processing: any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. profiling is an example of automated processing.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, which signifies agreement to the processing of personal data relating to them.

Data Audit/Data Asset Register: The assessment of data and its quality, for a specific purpose. Other terms are data map or information asset log.

Data Breach: This means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data, e.g. sending a list of pupil names, attainment marks and dates of birth to the wrong school.

Data Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. It is responsible for establishing practices and policies in line with the UK-GDPR. The Federation is the Data Controller of all personal data relating to its pupils, parents and staff.

Data Item: A single piece of information about a data subject, e.g. ethnicity, attendance.

Data Item Group: A group of data items that are typically captured about the same activity or business process e.g. behaviour management, catering.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major systems or business change programs involving the processing of personal data.

Data Processor: A person or organisation that process data on behalf of and on the orders of a controller, e.g. catering supplier.

Data Protection Officer (DPO): the person required to be appointed in public authorities under the GDPR.

Data Retention: How long the information is held for a processing job that it is need for, e.g. how long parent's phone numbers are kept after their child leaves school in case there are any outstanding issues to be resolved.

Data Subject: a living, identified or identifiable individual about whom we hold personal data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their personal data.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement (not just action).

General Data Protection Regulation (GDPR): Personal data is subject to the legal safeguards specified in the UK-GDPR.

Personal data is any information relating to an identified or identifiable natural person (data subject) who can be identified, directly or indirectly by reference to an identifier such as a name, 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. Personal data includes sensitive personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the UK-GDPR.

Privacy Notices: separate notices setting out information that may be provided to Data Subjects when the Federation collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, workforce privacy policy) or they may be stand-alone privacy statements covering processing related to a specific purpose.

Processing means anything done with personal data, such as collection, recording, structuring, storage, adaptation or alteration, retrieval, use, disclosure, dissemination or otherwise making available, restriction, erasure or destruction.

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal data relating to criminal offences and convictions.

Subject Access Request (SAR): This is where a data subject requests access to the information held on them. Timescales for responding, as well as reasons why the request has to be complied with or may be refused, are set out in law.

System: A piece of software, compute package or manually managed asset that supports the administration of one or more areas of school life, e.g. Capita SIMS, ParentPay.

System Group: An umbrella term to describe the areas of school administration where systems that contain personal level data typically reside, e.g. Core SIMS, curriculum tools.