DATA PROTECTION POLICY (PCC Model)

Adopted by the Governing Body

Contents

1.0 Introduction & Scope
- **1.1** Legislative Background
- **1.2** Application

Data Protection Policy:

2.0 Governance
- **2.1** Information Governance Team
- **2.2** Policy Dissemination & Enforcement
- **2.3** Data Protection Training
- **2.4** Data Protection by Design
- **2.5** Compliance Monitoring
- **2.6** Breach Reporting
- **2.7** Complaints

3.0 Data Protection Principles

4.0 Data Collection & Use of Data
- **4.1** Data Sources
- **4.2** Lawfulness of Processing
- **4.3** Privacy Notices
- **4.4** Data Quality
- **4.5** Data Retention
- **4.6** Technical & Organisational Measures
- **4.7** Data Sharing
- **4.8** Data Transfers
- **4.9** Children's Data
- **4.10** Data Processors

5.0 Data Subject Rights
- **5.1** Right to be Informed
- **5.2** Right of Access (Subject Access Request)
- **5.3** Right to Rectification
- **5.4** Right to Restrict Processing
- **5.5** Right to Erasure
- **5.6** Right to Data Portability
- **5.7** Right to Object
- **5.8** Rights Related to Automated Decision-Making Including Profiling

6.0 Law Enforcement Requests & Disclosures

7.0 Data Protection Exemptions

Appendices:

Appendix A – Further Guidance on Conditions for Processing

Appendix B - Substantial Public Interest Conditions

Appendix C - Exemptions

Data Protection Policy

1.0 Introduction & Scope

Pembrokeshire County Council and our School is committed to conducting its business in accordance with all applicable Data Protection laws and regulations and in line with the highest standards of ethical conduct. To demonstrate our commitment, Pembrokeshire County Council has signed up to the Personal Information Promise with the Information Commissioners Office.

This policy stipulates the expected behaviours of Pembrokeshire County Council Employees, Councillors, Volunteers, Partners, Governors, Contractors and commissioned Service Providers in relation to the collection, use, retention, sharing, disclosure and destruction of any Personal Data belonging to a Pembrokeshire County Council Contact (i.e. the Data Subject).

Personal Data is defined as any information relating to an identified or identifiable living individual (Data Subject). An identifiable living individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual. Personal Data is subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may process Personal Data. An organisation that handles Personal Data and makes decisions about its use is known as a Data Controller. Our school, as a Data Controller, is responsible for ensuring compliance with the Data Protection requirements outlined in this policy. Non-compliance may expose our school to complaints, regulatory action, fines and/or reputational damage.

As a Public & Education Authority, Pembrokeshire County Council has a number of roles including (but not limited to) an Employer, Service Provider, exercising Statutory duties, Partner, and Commissioner. In order to undertake its business the Council manages vast amounts of Personal Data. This Policy outlines the legal framework by which Personal Data will be managed by Pembrokeshire County Council and its Schools.

1.1 Legislative Background

The General Data Protection Regulation (GDPR) was adopted on 14 April 2016 and came into force on 25 May 2018. The GDPR is a regulation in EU law on data protection and privacy for all individuals within the European Union and European Economic Area. The GDPR provided national derogations for Member States to make exemptions for certain purposes. In light of the requirement to determine national derogations along with Britain's planned exit from the European Union, the Data Protection Act 2018 came into force on 25 May 2018. The Data Protection Act 2018 enshrines the GDPR in British law and extends it to cover legal areas for which the EU does not have oversight. It will remain in force after the UK leaves the EU.

1.2 Application

This policy applies to all services, processes and functions undertaken by or on behalf of Pembrokeshire County Council and our school where personal data is processed.

This will include personal data that forms part of a filing system, which is defined as any structured set of personal data which is accessible according to specific criteria, whether held by automated means or manually and whether centralised, decentralised or dispersed on a functional or geographic basis. Manual (not automated) unstructured data (which does not form part of a file or formal record) is exempt from most of the act. All automated data (including emails, skype conversations, etc.) must comply with this policy.

Data Protection Policy

2.0 Governance

2.1 Information Governance Team

The Audit, Risk & Information Service is managed by the Governance, Assurance & Information Manager who is Pembrokeshire County Councils designated Data Protection Officer. To demonstrate our commitment to Data Protection and to enhance the effectiveness of our compliance efforts, Pembrokeshire County Council has established an Information Governance Team within the Audit, Risk & Information Service, which operates independently of other Council Services and support functions.

The role of the Data Protection Officer is to undertake either directly or via the Information Governance Team, the following tasks:

a) To inform and advise Pembrokeshire County Council and its employees who carry out Processing pursuant to Data Protection Regulations, National Law or Union based Data Protection Provisions;

b) Ensuring alignment of this policy with Data Protection Regulations, National Law or Union based Data Protection Provisions;

c) Providing guidance with regards to carrying out Data Protection Impact Assessments (DPIA's) and monitor performance;

d) Acting as a point of conduct for and cooperating with the Information Commissioners Office (ICO);

e) Determining the need for notifications to the Information Commissioners Office (ICO) as a result of Pembrokeshire County Council's current or intended Personal Data Processing activities;

f) Have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing;

g) The establishment and operation of a system providing prompt and appropriate responses to Data Subjects requests;

h) Informing Senior Management, Members, and Officers of any potential corporate, civil and criminal penalties which may be levied against Pembrokeshire County Council and/or its Employees or Members for violation of applicable Data Protection laws;

i) Ensuring establishment of procedures and standard contractual provisions for obtaining compliance with this Policy by any Third Party who:

- Provide Personal Data to Pembrokeshire County Council
- Receives Personal Data from Pembrokeshire County Council
- Has access to Personal Data collected or processed by Pembrokeshire County Council.

2.2 Policy Dissemination & Enforcement

The Corporate Management Team of Pembrokeshire County Council and SLT at our school must ensure that all Pembrokeshire County Council Employees, Members and Governors are responsible for the Processing of Personal Data are aware of and comply with the contents of this policy.

Our school must make sure that all Third Parties engaged, on either a contractual or voluntary basis, to process personal data on behalf of our school (i.e. Data Processors) are aware of and comply with the contents of this policy. Assurance and evidence of such compliance (including a site visit) must be obtained from all Third Parties, whether companies or individuals, prior to granting them access to Personal Data controlled by our school.

2.3 Data Protection Training

All Pembrokeshire County Council employees will be required to undertake Data Protection Training on induction and as part of ongoing workplace training and development. There is a requirement to undertake the e-Learning training on an annual basis (based on expectations of the ICO). It is the responsibility of school Managers to ensure that their staff have undertaken the training, understand their responsibilities and adhere to the Data Protection Policy, the IT Security Policy and supporting Procedural guidance.

Information Asset Owners/Head teachers will be provided with additional training on their responsibilities to ensure continued compliance with Data Protection requirements.

2.4 Data Protection by Design

To ensure that all Data Protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes, the Data Protection Officer should be advised and will need to approve the process before the change is implemented. The involvement of the Data Protection Officer must be sought at the outset.

As part of this process a Data Protection Impact Assessment (DPIA) must be conducted, the Information Governance Team will be able to assist with this. The subsequent findings of the DPIA must then be submitted to the Data Protection Officer for review and approval. The IT department will work closely with the Information Governance Team to assess the impact of any new technology uses on the security of Personal Data.

2.5 Compliance Monitoring

To confirm compliance with this policy and the requirements of the Data Protection Act 2018 and other Data Protection legislation, the Information Governance Team will undertake annual risk based compliance checks within our school. The annual programme of compliance checks will be informed by the risk rating on the Information Asset Register and will be approved by the Data Protection Officer. Each compliance check will, as a minimum, assess:

- Compliance with Policy in relation to the protection of Personal Data, including:
  - The assignment of responsibilities
  - Raising awareness
  - Training of Employees
- The effectiveness of Data Protection related operational practices, including:
  - Security
  - Data Subject rights
  - Personal Data transfers
  - Personal Data incident management
  - Personal Data complaints handling
- The level of understanding of Data Protection policies and Privacy Notices
- The accuracy of Personal Data being stored
- Monitoring arrangements of Data Processor activities
- The adequacy of procedures for redressing poor compliance and Personal data Breaches.

The Information Governance Team, in cooperation with our school, will devise an action plan for correcting any identified deficiencies within a defined and reasonable timeframe. This will be monitored through the MKI automated system. Major deficiencies identified and non-compliance with agreed timescales will be reported to the Head Teacher & Governing body.

2.6 Breach Reporting

A data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to, personal data. A data incident, is a breach of security that could have, but did not lead to one of the above.

All data breaches must be reported immediately to the Data Protection Officer via the Information Governance Team. To assist, an online form is available on HWB, alternatively please complete with as much information as possible and email it to dataprotection@pembrokeshire.gov.uk. The Data Protection Officer is responsible for assessing data breaches and making a decision on reporting to the Information Commissioners Office. Under the GDPR reportable data breaches must be reported to the Information Commissioners Office within 72 hours of the Council becoming aware that the breach has occurred. A risk assessment is undertaken by the Data Protection Officer to determine whether the breach is reportable, this will include undertaking preliminary investigations into the circumstances of the breach, therefore it is critical that the Data Protection Officer is notified immediately via the Information Governance Team. Failure to notify the ICO of a reportable breach within 72 hours of the Council becoming aware of it could result in a substantial fine, as well as a fine for the breach itself.

Please inform the Information Governance Team of any data incidents. This is really useful so that we can measure our risk and learn from such incidents and further strengthen our security arrangements.

2.7 Complaints

The Council is committed to providing the highest standards of integrity and security of personal data that it processes. However, if you are unhappy about the way that your personal data has been processed or the application of your rights under the Data Protection legislation, then please address your concerns to:

Data Protection Officer

Pembrokeshire County Council

County Hall

Haverfordwest

Pembrokeshire

SA61 1TP

Email: DataProtection@pembrokeshire.gov.uk

The Information Commissioner's Office has developed a letter template to assist you in raising your concerns.

We will endeavour to respond to your concerns within one calendar month of receipt.

If you remain unsatisfied with how we are managing your personal data or applying your rights under the Data Protection legislation then you may contact the Information Commissioners Office via this link: https://ico.org.uk/make-a-complaint/your-personal-information-concerns/, or write to:

The Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

3.0 Data Protection Principles

In accordance with the Data Protection Act 2018, our school has adopted the following principles to govern its collection, use, retention, transfer, disclosure and destruction of Personal Data;

Principle 1: Lawfulness, Fairness and Transparency

Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. This means that our school must tell the Data Subject what Processing will occur (transparency), the processing must match the description given to the Data Subject (fairness), and it must be for one of the purposes specified in 4.2 (lawfulness of processing).

Principle 2: Purpose Limitation

Personal Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means that our school must specify exactly what the Personal Data collected will be used for and limit the Processing of that Personal Data to only what is necessary to meet the specified purpose.

Principle 3: Data Minimisation

Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This means that our school must not collect or store Personal Data beyond what is strictly required.

Principle 4: Accuracy

Personal Data shall be accurate and kept up to date. This means that our school must have in place processes for identifying and addressing out-of-date, incorrect and redundant Personal Data.

Principle 5: Storage Limitation

Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is processed. This means that our school must, wherever possible, store Personal Data in a way that limits or prevents identification of the Data Subject.

Principle 6: Integrity & Confidentiality

Personal Data shall be processed in a manner that ensures appropriate security of Personal Data, including protection against unauthorised or unlawful Processing, and against accidental loss, destruction or damage. Our school must use appropriate technical and organisational measures to ensure the integrity and confidentiality of Personal Data is maintained at all times.

Principle 7: Accountability

The Data Controller shall be responsible for, and be able to demonstrate compliance. This means that our school must demonstrate that the six Data Protection Principles (outlined above) are met for all Personal Data for which it is responsible (this will include the use for Third Parties for processing purposes).

4.0 Data Collection & Use of Data

4.1 Data Sources

Personal Data should be collected only from the Data Subject unless one of the following apply:

- The nature of the business purpose necessitates collection of the Personal Data from other persons or bodies;
- The collection must be carried out under emergency circumstances in order to protect the vital interests of the Data Subject or to prevent serious loss or injury to another person.

If Personal Data is collected from someone other than the Data Subject, the Data Subject must be informed of the collection unless one of the following apply:

- The Data Subject has received the required information by other means;
- The information must remain confidential due to a professional secrecy obligation;
- UK law expressly provides for the collection, Processing or transfer of the Personal Data (National Derogations awaited).

Where it has been determined that notification to a Data Subject is required, notification should occur promptly, but in no case later than:

- One calendar month from the first collection or recording of the Personal Data;
- At the time of first communication is used for communication with the Data Subject;
- At the time of disclosure if disclosed to another recipient.

4.2 Lawfulness of Processing

In preparing for the introduction of the General Data Protection Regulation (GDPR) and Data Protection Act 2018, the lawful basis of Processing (See Conditions of Processing, Appendix A) has been identified and documented within our school. This information has been captured within the Information Asset Register which is retained on the MKI System. The Data Protection Officer must be consulted and approve any changes to the lawful basis of Processing.

There are circumstances in which Personal Data may be further processed for purposes that go beyond the original purpose for which the Personal Data was collected. When making a determination as to the compatibility of the new reason for Processing, guidance and approval must be obtained from the Information Governance Team before any such Processing may commence.

In order to Process Personal Data Lawfully, at least one of the following conditions must apply:

a) The Data Subject has given consent to the processing of his or her personal data for one or more specific purposes;
b) Processing is necessary for the performance of a contract to which the Data Subject is party to or in order to take steps at the request of the Data Subject prior to entering into a contract;
c) Processing is necessary for compliance with a legal obligation to which our school is subject;
d) Processing is necessary in order to protect the vital interests of the Data Subject or of another living individual;
e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in our school;
f) Processing is necessary for the purposes of the legitimate interests pursued by our school 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.

In order to Process Special Categories of Personal Data Lawfully, at least one of the following conditions must apply:

a) The Data Subject has given explicit consent to the processing of those Personal Data for one or more specified purposes;
b) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of our school or of the Data Subject in the field of employment and social security and social protection law in so far as it is authorised by National Law; *(see Appendix A 1 for further guidance)*
c) Processing is necessary to protect the vital interests of the Data Subject or of another living individual where the Data Subject is physically or legally incapable of giving consent;
d) Processing relates to Personal Data which are manifestly made public by the Data Subject;
e) Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
f) Processing is necessary for reasons of substantial public interest; *(See Appendix B for further details)*
g) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State Law or pursuant to contract with a health professional and subject to conditions and safeguards (i.e. processed by or under the responsibility of a professional subject to the obligation of professional secrecy or by another person also subject to an obligation of secrecy by national competent bodies, e.g. professional codes of conduct); *(See Appendix A for further guidance).*
h) Processing is necessary for reasons of public interest in the area of public health, such as protecting against cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Members State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; *(see Appendix A 3 for further guidance)*
i) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject; *(see Appendix A 4 for further guidance)*
j) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. *(see Appendix A 4 for further guidance)*

4.3 Privacy Notices

The GDPR is more specific about the information we are required to provide to people about what we do with their personal data. We must provide this information to individuals in a way that is easy to access, read and understand.

Providing clear and concise privacy notices covers some of the key transparency requirements under the Data Protection legislation. The checklist in Appendix C provides guidance on what we are required to include within a privacy notice depending on whether the personal data was collected from the individual it relates to or from another source.

Privacy Notices for our school is published on our website.

4.4 Data Quality

Our school will adopt all necessary measures to ensure that the Personal Data it collects and processes is complete and accurate in the first instance, and is updated to reflect the current situation of the Data Subject (as applicable). The measures adopted by our school to ensure data quality include:

- Correcting Personal Data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the data subject does not request rectification;
- Keeping Personal Data only for the period necessary to satisfy the permitted uses or applicable statutory retention period;
- The removal of Personal Data if in violation of any of the Data Protection principles or if the Personal Data is no longer required;
- Restriction, rather than deletion of Personal Data, insofar as:
  - A law prohibits erasure
  - Erasure would impair legitimate interests of the Data Subject
  - The Data Subject disputes that their Personal Data is correct and it cannot be clearly ascertained whether their information is correct or incorrect.

4.5 Data Retention

To ensure Fair Processing, Personal Data will not be retained by our school for longer than necessary in relation to the purposes for which it was originally collected. Or for which it was further processed.

The length of time for which our school need to retain Personal Data is set out in the Pembrokeshire County Council Records Retention Schedule. This is based on the National Archives Guidance for Local Authorities, which defines the statutory timescales for categories of Personal Data processing across the Authority by service/function. In the absence of a Statutory Timescale, record retention is minimised in order to protect the rights of the Data Subject.

4.6 Technical & Organisational Measures

Our school will adopt physical, technical, and organisational measures to ensure the security of Personal Data. This includes the prevention of loss or damage, unauthorised alteration, access or processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment.

Further details on the minimum set of security measures adopted by our school are detailed within the following policies:

IT Security and e-Mail/Internet Policy

Records Management Policy

Confidential Waste Policy

A summary of the Personal Data related security measures is provided below:

- Prevent unauthorised persons from gaining access to data processing systems in which Personal Data are processed;
- Prevent persons entitled to use a data processing system from accessing Personal Data beyond their needs and authorisations;
- Ensure that Personal Data in the course of electronic transmission during transport cannot be read, copied, modified on or removed from a data processing system;
- Ensure that in the case where processing is carried out by a Data Processor, the data can be processed only in accordance with the instructions of the Data Controller;

- Ensure that Personal Data is protected against undesired destruction or loss;
- Ensure that Personal Data collected for different purposes can and is processed separately;
- Ensure that Personal Data is kept no longer than is necessary.

4.7 Data Sharing

There may be instances where requests to share information with third parties. This may be a one-off request or for systematic data sharing.

One-off Data Sharing

As a Data Controller we would not disclose personal data to any members of the public. Requests such as these would be dealt with under the Freedom of Information Act 2000, which provides an exemption for sharing of personal information.

However, there may be instances when it would be appropriate to share personal data with a third party, such as another professional, court, regulatory body, etc. The following points should be considered and documented to justify your rationale for decision-making:

- Do you think you should share the information?
- Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?
- Do you have concerns that an individual is at risk of serious harm?
- Do you need to consider an exemption in the DPA to share?
- Do you have the power to share?
- Do you have a legal obligation to share?

If you decide to share you need to:

- Only share what is necessary
- Distinguish fact from opinion
- Share the information securely
- Ensure that you are giving information to the right person
- Consider whether it is appropriate/safe to inform the data subject that you have shared their information.

Record your decision:

- What information was shared and for what purpose
- Who it was shared with
- When it was shared
- Your justification for sharing
- Whether the information was shared with or without consent.

Requests for information should be discussed with your Information Asset Owner – this will be your Head Teacher.

Systematic Data Sharing

Our school will have reasons why we may wish to share personal data regularly with a third party. In these cases, we must have a data sharing agreement/information sharing protocol in place. As well as considering the key points above, the data sharing agreement/ information sharing protocol should cover the following issues:

- What information needs to be shared
- The organisations that will be involved
- What you need to tell data subject about the data sharing and how you will communicate that information (privacy notice)
- Measures to ensure adequate security is in place to protect the data
- What arrangement need to be in place to provide data subjects with access to their personal data if they request it
- Agreed common retention periods for the data
- Processes to ensure secure disposal/deletion takes place.

Pembrokeshire County Council has signed up to the Wales Accord on the Sharing of Personal Information (WASPI). This provides a good practice in data sharing and enables public services to meet their data protection responsibilities as they move to collaborative working. The Information Governance Team will be able to assist with the development of data sharing agreements/information sharing protocols and must be consulted at the outset.

4.8 Data Transfers

The GDPR imposes a general prohibition on the transfer of personal data outside the EU, unless:

- The transfer is based on an adequacy decision;
- The transfer is subject to appropriate safeguards;
- The transfer is governed by Binding Corporate Rules; or
- The transfer is in accordance with specific exceptions.

In all cases, you should refer to the Data Protection Officer before transferring data outside of the EU. Accessing personal data remotely when outside of the EU would be included in this definition.

4.9 Children's Data

Children need particular protection when you are collecting and processing their personal data because they may be less aware of the risks involved. As a school that process children's personal data we should consider the need to protect them and design systems and processes with this in mind (Data Privacy Impact Assessment).

If consent is being relied on as the lawful basis for processing then consideration needs to be given to the following:

- The competence of the child (whether they have the capacity to understand the implications of the collection and processing of their personal data). If a child isn't deemed to be competent then consent is not 'informed' and therefore not valid;
- The imbalance of power in your relationship with the child, to ensure that if you accept their consent if is freely given;

- Are you providing on online service to children? If you are relying on consent then you must seek parental consent for children under the age of 13, unless the online service is a preventative or counselling service.

Transparency is key. You can raise children's (and their parents') awareness of data protection risks, consequences, safeguards and rights by:

- Telling them what you are doing with their personal data;
- Being open about the risks and safeguards involved; and
- Letting them know what to do if they are unhappy.

We must have age-appropriate privacy notices for children. They must be clearly written so that they are able to understand what will happen to their personal data, and what rights they have.

4.10 Data Processors

A Data Processor is responsible for processing personal data on behalf of a data controller. An example would be use of the Royal Mail to deliver post, Cloud provision or third parties contracted to undertake confidential waste disposal. The GDPR applies to both Data Controllers and Data Processors. Data Processors have specific legal obligations placed on them, for example, they are required to maintain records of personal data processing activities. Data Processors now have a legal liability if they are responsible for a data breach.

The GDPR places certain obligations on Data Controllers to have a contract in place with Data Processors and certain clauses must be included. The Data Controller must also be able to evidence that they have undertaken due diligence checks prior to entering into a contract and must undertake and evidence regular contract monitoring to gain appropriate assurance that the Data Processor is GDPR compliant.

5.0 Data Subject Rights

5.1 Right to be Informed

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR. Section 4.1 on Data Sources, Section 4.3 on Privacy Notices and Appendix C provides further information on compliance with this right.

5.2 Right of Access (Subject Access Request)

If an individual makes a request relating to any of the rights listed, our school will consider each request in accordance with all applicable Data Protection laws and regulations.

No administration fee will be charged to the data subject for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature.

Data Subjects are entitled to obtain, based upon a request made to the Access to Records Team via our school and upon successful verification of their identity, the following information about their own Personal Data;

Confirmation as to whether or not personal data concerning him or her is being processed. Where that is the case, access to the personal information as defined below:

- The purposes of the collection, processing, use and storage of their personal data;
- The source(s) of the personal data, if it was not obtained from the Data Subject;
- The categories of personal data stored for the Data Subject;

- The recipients or categories of recipients to whom the personal data has been or may be transmitted, along with the location of those recipients;
- The envisaged period of storage for the personal data or the rationale for determining the storage period;
- The use of any automated decision-making, including profiling;
- The right of the Data Subject to:
    - Object to processing of their Personal Data
    - Lodge a complaint with the Information Commissioner's Office
    - Request rectification or erasure of their personal data
    - Request restriction of processing of their personal data.

It should be noted that situations may arise where providing the information requested by a Data Subject would disclose Personal Data about another individual which will need to be redacted.

The Access to Records Team are trained in handling requests and identifying third party data and are equipped with the redaction software to assist with this process, which is why it is essential that all requests are processed by the Access to Records Team.

5.3 Right to Rectification

Individuals have the right to have inaccurate personal data rectified, or completed if it is incomplete. An individual can make a request for rectification verbally or in writing. Requests must be recorded on the Data subjects record and processed within one calendar month. Retaining records of the date the request was received, who received it and how (e.g. email, letter, telephone call) and when actioned, will fulfil the accountability requirement.

In certain circumstances a request for rectification can be refused. For example, there may be a record maintained of an error: while it would be appropriate to correct an error it would also be appropriate to keep a record that the error had been corrected. If an individual requested that the record of the error be removed this could be refused as the record that the error occurred is in itself accurate. In certain circumstances, an individual may dispute the accuracy of a professional opinion, however, this is an opinion and in itself is subjective. As long as the record clearly records that it is an opinion and whose opinion it is, this would constitute an accurate record.

5.4 Right to Restrict Processing

This is not an absolute right and only applies in certain circumstances, e.g. the accuracy of the data is being contested, the data has been unlawfully processed, the individual has objected to processing and the legitimate grounds for processing are being considered.

When processing is restricted it can be stored, but not used. Information Asset Owners will be responsible for ensuring that there are appropriate safeguards within their systems to enable the restriction of processing.

5.5 Right to Erasure

This is also known as 'the right to be forgotten'. Individuals can make the request for erasure verbally or in writing and must be responded to within one calendar month. The right to erasure only applies in certain circumstances:

- The personal data is no longer necessary for the purpose which it was originally collected or processed for;
- The legal basis for processing is 'consent';

- The legal basis for processing is 'legitimate interests', the individual objects to the processing and there is no overriding legitimate interest to continue this processing;
- The processing is for direct marketing purposes and the individual objects to that processing;
- The personal data has been processed unlawfully;
- Compliance with a legal obligation;
- The personal data has been processed to offer information society services to a child.

There is an emphasis on the right to have personal data erased if the request relates to data collected from children. This reflects the enhanced protection of children's information, especially in online environments, under the GDPR.

If the personal data has been disclosed to others, each recipient must be contacted and informed of the erasure, unless this proves impossible or involves disproportionate effort. If asked to do so, you must inform the individual's about these recipients.

5.6 Right to Data Portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes within our school. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability. This right will mainly apply to utility service providers, banking and mobile phone providers and is unlikely to apply to service provided by our school. The right only applies to information provided to the school.

5.7 Right to Object

The GDPR gives individuals the right to object to processing of their personal data in certain circumstances. Individuals have the absolute right to stop their data being used for direct marketing.

An individual can object where one of the following lawful bases are being relied on:

- 'public task' (for the performance of a task carried out in the public interest);
- 'public task' (for the exercise of official authority vested in the Council/School); or
- 'legitimate interests'.

An individual must provide a specific reason why they are objecting to the processing of their data. In these circumstances, this is not an absolute right, and processing can continue if:

- The Council/School can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- The processing is for the establishment, exercise or defence of legal claims.

Individuals must be informed of their right to object. If an objection is received it must be responded to within one calendar month. The rationale for the decision must be clearly recorded and communicated to the individual. If the objection is refused the individual must be notified of their right to make a complaint to the ICO.

5.8 Rights Related to Automated Decision-Making Including Profiling

The GDPR has provisions on:

- Automated individual decision-making (making a decision solely by automated means without any human involvement); and
- Profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision making process.

The GDPR has additional rules to protect individuals solely automated decision-making is being undertaken that has a legal or similarly significant effects on them. This type of decision-making can only be undertaken where the decision is:

- Necessary for the entry into or performance of a contract; or
- Authorised by Union or UK law; or
- Based on an individual's explicit consent.

6.0 Law Enforcement Requests & Disclosures

In certain circumstances, it is permitted that personal data be shared without the knowledge or consent of the data subject. This is the case where the disclosure of the personal data is necessary for any of the following purposes:

- The prevention or detection of crime;
- The apprehension or prosecution of offenders;
- The assessment or collection of a tax or duty;
- By the order of a court or by any rule of law.

If our school processes personal data for one of these purposes, then it may apply an exception to the processing rules outlined in this policy (Appendix C) but only to the extent that not doing so would be likely to prejudice the case in question.

If any School employee receives a request from a court or any regulatory or law enforcement authority for information relating to a School contact, the Information Governance Team must be notified and will be able to provide guidance and assistance.

7.0 Data Protection Exemptions

The Data Protection Act 2018 defines exemptions to the application of certain requirements under the GDPR. Appendix C provides a breakdown of the exemptions to the GDPR and are cross-referred to the requirements (Articles) of the GDPR. The application of the exemptions in certain circumstances is quite complex and will require reference to specific guidance within the Data Protection Act 2018, which is why the table cross-refers to the relevant section of the Act. Advice should be sought from the Data Protection Officer via the Information Governance team.

In order to meet the Accountability requirement, the rationale for applying an exemption must be documented and retained. If the ICO receives a complaint they will ask for this information when assessing the complaint.

Appendix A – Further Guidance on Conditions for Processing

1. **Employment, Social Security and Social Protection**

   This condition is met if:

   a) The processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment, social security or social protection, and

b) When the processing is carried out, the controller has an appropriate policy document in place.

2. Health and Social Care Purposes

This condition is met if the processing is necessary for one of the following purposes:

a) Preventative or occupational medicine

b) The assessment of the working capacity of an employee

c) Medical diagnosis

d) The provision of health care or treatment

e) The provision of social care, or

f) The management of health care systems or service or social care systems or services.

Personal data may be processed for these purposes when processed by or under the responsibility of a professional subject to the obligation of professional secrecy established by national competent bodies.

3. Public Health

The condition is met if the processing:

a) Is necessary for reasons of public interest in the area of public health, and

b) Is carried out –

i. By or under the responsibility of a health professional, or

ii. By another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.

4. Research, etc.

This condition is met if the processing:

a) Is necessary for archiving purposes, scientific or historical research purposes or statistical purposes

b) Is subject to appropriate technical and organisational safeguards including, e.g. data minimisation, pseudonymisation. Where the purpose can be met without the identification of the data subject, those purposes should be fulfilled in that manner.

c) Such processing does not satisfy requirements if the processing is likely to cause substantial damage or distress to a data subject or if the processing is carried out for the purposes of measures or decisions with respect to a particular individual.

Appendix B - Substantial Public Interest Conditions

1. **Statutory and Government Purposes**

This condition is met if the processing is necessary for:

a) The exercise of a function conferred on a person by an enactment or rule of law;

b) The exercise of a function of the Crown, a Minister of the Crown or a government department**.**

And is for reasons of substantial public interest.

Administration of Justice and Parliamentary Purposes

This condition is met if the processing is necessary for:

a) The administration of justice, or

b) The exercise of a function of either House of Parliament,

2. **Equality of Opportunity or Treatment**

This condition is met if the processing:

a) Is of a specified category of personal data, and

b) Is necessary for the purposes of identifying or keeping under review the existence or absence of equality of opportunity or treatment between groups of people specified in relation to that category with a view to enabling such equality to be promoted or maintained;

Specified means:

Category of Personal Data	**Groups of people (in relation to a category of personal data)**
Personal data revealing racial or ethnic origin	People of different racial or ethnic origins
Personal data revealing religious or philosophical beliefs	People holding different religious or philosophical beliefs
Data concerning health	People with different states of physical or mental health
Personal data concerning an individual's sexual orientation	People of different sexual orientation

Processing does not meet the condition if it is carried out for the purposes of measures or decisions with respect to a particular data subject.

Processing does not meet the condition if it is likely to cause substantial damage or substantial distress to an individual.

Processing does not meet the condition if:

a) The data subject (or one of the data subjects) has given notice in writing to the School not to process their personal data and the requirement has not been withdrawn;

b) The notice gave the School a reasonable period in which to stop processing such data; and

c) The period has ended.

3. Racial and Ethnic Diversity at Senior Level of Organisations

This condition is met if the processing:

a) Is of personal data revealing racial or ethnic origin,
b) Is carried out as part of a process of identifying suitable individuals to hold senior positions in a particular organisation, a type of organisation or organisations generally;
c) Is necessary for the purposes of promoting or maintaining diversity in the racial and ethnic origins of individuals who hold senior positions in the organisation or organisations, and
d) Can reasonably be carried out without the consent of the data subject (unless it is likely to cause substantial damage or substantial distress to the data subject). Processing can reasonably be carried out if the School cannot reasonably expected to obtain consent and the School is not aware of the data subject withholding consent.

4. Preventing or Detecting Unlawful Acts

This condition is met if the processing:

a) Is necessary for the purposes of the prevention or detection of an unlawful act;
b) Must be carried out without the consent of the data subject so as not to prejudice those purposes; and
c) Is necessary for the reasons of substantial public interest.

5. Protecting the Public form Dishonesty

This condition is met if the processing:

a) Is necessary for the exercise of a protective function,
b) Must be carried out without the consent of the data subject so as not to prejudice the exercise of that function, and
c) Is necessary for reasons of substantial public interest.

"Protective Function" means a function which is intended to protect members of the public against:

a) Dishonestly, malpractice or other seriously improper conduct,
b) Unfitness or incompetence,
c) Mismanagement in the administration of a body or association, or
d) Failures in services provided by a body or association.

6. Regulatory Requirements Relating to Unlawful Acts and Dishonesty

This condition is met if:

a) The processing is necessary for the purposes of complying with, or assisting other persons to comply with, a regulatory requirement which involves a person taking steps to establish whether another person has:

   i. Committed an unlawful act, or

   ii. Been involved in dishonesty, malpractice or other seriously improper conduct.

b) In the circumstances, the School cannot reasonably be expected to obtain consent of the data subject to the processing, and

c) The processing is necessary for reasons of substantial public interest.

7. Journalism etc. in Connection with Unlawful Acts and Dishonesty

This condition is met if:

a) The processing consists of the disclosure of personal data for the special purposes,
b) It is carried out in connection with a matter described below,
c) It is necessary for reasons of substantial public interest,
d) It is carried out with a view to the publication of the personal data by any person, and
e) The School reasonably believes the publication of the personal data would be in the public interest.

The matters referred to in 7b are any of the following (whether alleged or established):

a) The commission of an unlawful act by a person;
b) Dishonesty, malpractice or other seriously improper conduct of a person;
c) Unfitness or incompetence of a person;
d) Mismanagement in the administration of a body or association;
e) A failure in services provided by a body or association

8. Preventing Fraud

This condition is met if the processing:

a) Is necessary for the purposes of preventing fraud or a particular kind of fraud, and
b) Consists of:
   i. The disclosure of personal data by a person as a member of an anti-fraud organisation,
   ii. The disclosure of personal data in accordance with arrangements made by an anti-fraud organisation.

9. Suspicion of Terrorist Financing or Money Laundering

This condition is met if the processing is necessary for the purposes of making a disclosure in good faith under either of the following:

a) Section 21CA of the Terrorism Act 2000;
b) Section 339ZB of the Proceeds of Crime Act 2002 (disclosures within regulated sector in relation to suspicion of money laundering).

10. Support for individuals with a particular disability or medical condition

This condition is met if the processing:

a) Is carried out by a not-for-profit body which provides support to individuals with a particular disability or medical condition,
b) Involves personal data that falls within these sub-paragraphs:
   i. Personal data revealing racial or ethnic origin;
   ii. Genetic data or biometric data;
   iii. Data concerning health
   iv. Personal data concerning an individual's sex life or sexual orientation.

And relates to an individual who is a member of the not-for-profit body and:

   i. Has the disability or condition, has had the disability or condition or has a significant risk of developing that disability or condition, or
   ii. Is a relative or carer of an individual who falls within the category above?

c) Is necessary for the purposes of:
   i. Raising awareness of the disability or medical condition, or

ii. Providing support to individuals or enabling individuals to provide support to each other,

d) Can reasonably be carried out without the consent of the data subject, and

e) Is necessary for reasons of substantial public interest.

11. Counselling, etc.

This condition is met if the processing:

a) Is necessary for the provision of confidential counselling, advice or support or of another similar service provided confidentially,

b) Is carried out without the consent of the data subject (consent cannot be given by the data subject, consent cannot reasonably be obtained, obtaining consent would prejudice the provision of the service).

12. Safeguarding of Children and Individuals at Risk

The condition is met if:

a) The processing is necessary for the purposes of:

i. Protecting an individual from neglect or physical, mental or emotional harm, or

ii. Protecting the physical, mental or emotional well-being of an individual,

b) The individual is:

i. Aged under 18, or

ii. Aged 18 or over and at risk,

c) The processing is carried out without the consent of the data subject for one of the following reasons:

i. In the circumstances, consent to the processing cannot be given by the data subject;

ii. In the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing;

iii. Obtaining consent would prejudice the provision of the protection.

d) The processing is necessary for reasons of substantial public interest.

For the purposes of b) ii., an individual aged 18 or over is “at risk” if the controller has reasonable cause to suspect that the individual:

a) Has needs for care and support,

b) Is experiencing, or at risk of, neglect or physical, mental or emotional harm, and

c) As a result of those needs is unable to protect himself or herself against the neglect or harm or the risk of it.

13. Safeguarding of Economic Well-being of Certain Individuals

This condition is met if the processing:

a) Is necessary for the purposes of protecting the economic well-being of an individual at economic risk who is aged 18 or over,

b) Is of data concerning health,

c) Is carried out without the consent of the data subject
d) Is necessary for reasons of substantial public interest.

"Individuals at risk" means an individual who is less able to protect his or her economic well-being by reason of physical or mental injury, illness or disability.

14. Insurance

This condition is met if the processing:

a) Is necessary for an insurance purpose,

b) Is of personal data revealing racial or ethnic origin, religious or philosophical beliefs or trade union membership, genetic data or data concerning health, and

c) Is necessary for the reasons of substantial public interest, where:

i. The processing is not carried out for the purposes of measures or decisions with respect to the data subject, and

ii. The data subject does not have or is not expected to acquire: rights or obligations to a person who is an insured person under an insurance contract or other rights or obligations in connection with such a contract.

15. Occupational Pensions

This condition is met if the processing:

a) Is necessary for the purpose of making a determination in connection with eligibility for, or benefits payable under, an occupational pension scheme,

b) Is of data concerning health which relates to a data subject who is the parent, grandparent, great-grandparent or sibling of a member of the scheme,

c) Is not carried out for the purposes of measures or decisions with respect to the data subject, and

d) Can reasonably be carried out without the consent of the data subject.

16. Political Parties

This condition is met is the processing:

a) Is of personal data revealing political opinions,
b) Is carried out by a person or organisation included in the register maintained under section 23 of the Political Parties, Elections and Referendums Act 2000, and
c) Is necessary for the purposes of the person's or organisation's political activities

The condition is not met if it is likely to cause substantial damage or substantial distress to a person.

The condition is not met if:

a) An individual who is the data subject (or one of the data subjects) has given notice in writing to the School requiring the School not to process personal data in respect of which the individual is the data subject (and has not given notice in writing withdrawing that requirement),
b) The notice gave the controller a reasonable period in which to stop processing such data, and
c) That period has ended.

d) In this paragraph political activities include campaigning, fund-raising, political surveys and case-work.

17. Elected Representatives Responding to Requests

This condition is met if:

a) The processing is carried out:

i. By an elected representative or a person acting with the authority of such a representative,

ii. In connection with the discharge of the elected representative's functions, and

iii. In response to a request by an individual that the elected representative has taken action on behalf of, and

b) The processing is necessary for the purposes of, or in connection with, the action reasonably taken by the elected representative in response to that request.

Where the request to the Elected Representative is made by an individual other that the data subject, the condition is only met if the processing must be carried out without the consent of the data subject for one of the following reasons:

a) In the circumstances, consent to the processing cannot reasonably be given by the data subject;

b) In the circumstances, the elected representative cannot reasonably be expected to obtain the consent of the data subject to the processing;

c) Obtaining the consent of the data subject would prejudice the action taken by the elected representative;

d) The processing is necessary in the interests of another individual and the data subject has withheld consent unreasonable.

18. Disclosure to Elected Representatives

This condition is met if:

a) The processing consists of the disclosure of personal data:

i. To an elected representative or a person acting with the authority of such a representative, and

ii. In response to a communication to the School from that representative or person which was made in response to a request from an individual,

b) The personal date is relevant to the subject matter of the communication, and

c) The disclosure is necessary for the purpose of responding to that communication

Where the request to the elected representative came from an individual other than the data subject, the condition is met only if the disclosure must be made without the consent of the data subject for one of the following reasons:

a) In the circumstances, consent to the processing cannot be given by the data subject;

b) In the circumstances, the elected representative cannot reasonably be expected to obtain the consent of the data subject to the processing;

c) Obtaining the consent of the data subject would prejudice the action taken by the elected representative;

d) The processing is necessary in the interests of another individual and the data subject had withheld consent unreasonably.

Appendix C - Exemptions

The table below provides a summary of the exemptions in the Data Protection Act 2018 (reference to the relevant part of the Act) from the relevant articles of the GDPR.

For ease of reference, the relevant GDPR Articles are:

Article 5: the Principles

Article 13: Transparency information when collecting personal data directly

Article 14: Transparency information when not collecting personal data directly

Article 15: Subject access

Article 16: Right of rectification

Article 17: Right of erasure

Article 18: Right to rectification of processing

Article 19: Notification regarding rectification, erasure or restriction

Article 20: Right of data portability

Article 21: Right to object

Exemption	GDPR Article									
	5	13	14	15	16	17	18	19	20	21
Crime and Taxation: general (Schedule 2, Paragraph 2) Exemption for the purposes of the prevention or detection of crime, the apprehension or prosecution of offenders or the assessment or collection of tax or duty.	✓	✓	✓	✓	✓	✓	✓		✓	✓
Crime and Taxation: risk assessment system (Schedule 2, Paragraph 3) Exemption for personal data which consists of a classification applied to a data subject as part of a risk assessment system operated by government, local authority or another authority administering housing benefit for crime and taxation purposes.	✓	✓	✓	✓						
Immigration (Schedule 2, Paragraph 4) Exemption for the purposes of the maintenance of effective immigration control, or the investigation or detection of activities that would undermine the maintenance of effective immigration control.	✓	✓	✓	✓		✓	✓			
Information required to be disclosed by law etc or in connection with legal proceeding (Schedule 2, Paragraph 5) Exemption if: • The controller is obliged by enactment to make personal data available to the public; • Disclosure is required by an enactment, rule of law or court/tribunal order: or • Disclosure is necessary for the purposes of actual or prospective legal proceedings, or obtaining of legal advice or establishing, exercising or defending legal rights.	✓	✓	✓	✓	✓	✓	✓		✓	✓

Exemption	GDPR Article									
	5	13	14	15	16	17	18	19	20	21
Functions designed to protect the public etc. (Schedule 2, Paragraph 7) Exemption for the purposes of certain bodies or persons discharging functions, including: • To protect the public in relation to financial loss, harm by persons authorised to carry on any professions or other activity; • To protect charities and community interest companies and their property from mishandling; • To protect the health and safety of persons at work or other persons in connection with the action of persons at work; • To protect the public from maladministration and failures by a public body and to regulate anti-competitive behaviour.	✓	✓	✓	✓	✓	✓	✓		✓	✓
Regulatory functions relating to legal services, the health service and children's services (Schedule 2, Paragraph 8) Exemption for the purpose of certain bodies or persons discharging functions relating to the Legal Services Board, considering legal complaints, complaints as to the maladministration of a health service redress scheme by anybody or other person, complaints relating to social and palliative care and complaints about social services.	✓	✓	✓	✓	✓	✓	✓		✓	✓
Regulatory function of certain other bodies (Schedule 2, Paragraph 9) Exemption for the purpose of certain bodies or persons discharging functions relating to the Financial Ombudsman, the investigator of complaints against the financial regulators, a consumer protection officer other than the Competition and Markets Authority, the monitoring officer of a relevant authority and the Public Services Ombudsman for Wales.	✓	✓	✓	✓	✓	✓	✓		✓	✓

Exemption	GDPR Article									
	5	13	14	15	16	17	18	19	20	21
Parliamentary Privilege (Schedule 2, Paragraph 11) Exemption if this is required for the purpose of avoiding an infringement of parliamentary privilege.	✓	✓	✓	✓	✓	✓	✓		✓	✓
Protection of the Rights of Others (Schedule 2, Paragraph 14) Exemption if a disclosure of information by a controller would involve disclosing information relating to another individual identifiable from the information.	✓			✓						
Legal Professional Privilege (Schedule 2, Paragraph 17) Exemption for information subject to legal professional privilege.	✓	✓	✓	✓						
Self-Incrimination (Schedule 2, Paragraph 20) Exemption from certain GDPR provisions where compliance would reveal evidence of the commission of an offence and would expose that person to proceedings for that offence.	✓	✓	✓	✓						
Confidential References (Schedule 2, Paragraph 22) Exemption if the personal data consists of a confidential reference for purposes including the education, training or employment of the data subject. This exemption also applies to the appointment of the data subject to any office, including that of a volunteer, or the provision of any service by the data subject.	✓	✓	✓	✓						
Exam Scripts and Exam Marks (Schedule 2, Paragraph 23) Exemption when personal data consisting of information recorded by candidates during an exam.	✓	✓	✓	✓						
Research and Statistics (Schedule 2, Paragraph 25) Exemption if personal data is processed for scientific or historical research purposes, or for statistical purposes.				✓	✓		✓	✓	✓	✓

Exemption	GDPR Article									
	5	13	14	15	16	17	18	19	20	21
Archiving in the Public Interest (Schedule 2, Paragraph 26) Exemption if personal data is processed for archiving purposes in the public interest.				✓	✓		✓	✓	✓	✓
Health Data Processed by a Court (Schedule 3, Paragraph 3) Exemption if health personal data is processed by a Court.	✓	✓	✓	✓	✓	✓	✓		✓	✓
Data Subject Expectations and Wishes with Respect to Health Data (Schedule 3 Paragraph 4) Exemption relating to a request for health data in certain situations where the data subject is under 18 years old and the requestor has parental responsibility or the data subject is incapable of managing their own affairs and responding to the request would not conform with the data subjects wishes.	✓	✓	✓	✓	✓	✓	✓		✓	✓
Serious Harm from Health Data Disclosure (Schedule 3, Paragraph 5) Exemption from Article 15 (1) and (3) when the serious harm test[1] is met or where a controller who is not a health professional obtains an opinion from someone who appears to be an appropriate health professional.				✓[1]						
Social Work Data Processed by a Court (Schedule 3, Paragraph 9) Exemption if personal data concerning social work is processed by the Court.	✓	✓	✓	✓	✓	✓	✓		✓	✓

[1] The Serious Harm Test involves consideration of whether the application of the Article 15 Right of Access under the GDPR to the data would be likely to cause serious harm to the physical or mental health of the data subject or another individual.

Exemption	GDPR Article									
	5	13	14	15	16	17	18	19	20	21
Data Subjects Expectations and Wishes with Respect to Social Work Data (Schedule 3, Paragraph 10) Exemption relating to a request for social work data in certain situations where the data subject is under 18 years old and the requestor has parental responsibility or the data subject is incapable of managing their own affairs and responding to the request would not conform with the data subject's wishes.	✓	✓	✓	✓	✓	✓	✓		✓	✓
Serious Harm from Social Work Data Disclosure (Schedule 3, Paragraph 11) Exemptions from Article 15 (1) and (3) of the GDPR when the serious harm test 1 is met.				✓[1]						
Education Data Processed by Court (Schedule 3, Paragraph 18) Exemption if educational personal data is processed by the Court.	✓	✓	✓	✓	✓	✓	✓		✓	✓
Serious Harm from Education Data Disclosure (Schedule 3, Paragraph 19) Exemption from Article 15 (1) and (3) when the serious harm test 1 is met.				✓[1]						

Exemption	GDPR Article									
	5	13	14	15	16	17	18	19	20	21
Child Abuse Data (Schedule 3, Paragraph 21) Exemption from Article 15 (1) and (3) when a request for child abuse data would not be in the best interests of the data subject under 18 years old and the requestor has parental responsibility or the data subject is incapable of managing their own affairs and the person making the request has been appointed by a court to manage those affairs.				✓						
Journalistic, Academic, Artistic and Literary Purposes (Schedule 2, Paragraph 24) Exemption from certain GDPR provisions if the personal daa is being processed for the special purposes with a view to publication by a person of journalistic, academic, artistic and literary material in the public interest. [2]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Other Exemption from certain GDPR provisions if personal data is processed for the following purposes, when disclosing information about: • Human fertilisation and embryology information (**Schedule 4, Paragraph 2**); • Adoption records and reports (**Schedule 4, Paragraph 3**); • Statements of special educational needs (**Schedule 4, Paragraph 4**); • Parental order records and reports (**Schedule 4, Paragraph 5**); • Information provided by the Principle Reporter for children's hearing (**Schedule 4, Paragraph 6**).	✓			✓						

[2] Also exempt from Articles 60-67.

There are additional exemptions available for the following specific circumstances:

- When assessing a person's suitability for judicial office or the office of Queen's Counsel;
- When assessing a person's suitability for offices such as the Poet Laureate;
- In connection with a corporate finance service involving price-sensitive information;
- Management forecasting or planning in relation to a business or other activity;
- Any negotiations with the data subject and where this would be likely to prejudice those negotiations.