>

Potters Green School

nurturing bright futures

UK GDPR
DATA PROTECTION POLICY

Review Programme:	**Annually**
Reviewed by School Business Manager:	**Mrs Karen Capell 20/09/23**
Date for next review:	**21st September 2024**
Signed – Headteacher	**Mrs Gillian Deery**

This Data Protection Policy was produced by the School's Data Protection Officer in September 2022 and is due for review in September 2023. Version 3.

1. PURPOSE

1.1 The UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 and subsequent domestic legislation replace the EU Data Protection Regulation 1995 and the Data Protection Act 1998 in an aid to update and manage a technologically advancing world. In order to provide adequate protection to these changes, the EU have increased the accountability of data controllers/processors and enhanced the rights of individuals.

The School has notified the Information Commissioner's Officer of its data processing and its registration number is Z4578272.

The objective of this policy is to establish a framework that ensures the School has in place structures and processes to manage the security of personal data collected, processed and stored by the School and requests to access information held by the School so as to:

a. ensure requests are dealt with in compliance with the requirements of the UK GDPR; and

b. ensure that the School employees are aware of their obligations in relation to security of personal data, recording processing activities and in providing access to information held by the School in accordance with the law.

1.2 A further objective of this policy is to provide a framework through which effective records management can be achieved.

1.3 The School's governing body retains overall responsibility for policy implementation, whereby individual staff members are required to abide by the procedures and systems put in place as a result of policy implementation and to support it. This policy will be communicated to all employees who will be expected to fulfil their responsibilities as detailed below.

1.4 This policy applies to all premises and activities within the control of the School and is supported by arrangements for implementation and monitoring.

1.5 The Data Protection Officer acts as a representative for the School with regard to its data controller responsibilities. The Data Protection Officer's details can be found on the School's Privacy Notice.

2. GENERAL PRINCIPLES OF THE UK GDPR

2.1 The School is a public authority and a Data Controller that is dependent upon its records collection and management systems for the discharge of its educational responsibilities. As a 'data controller' any suppliers that also process personal data on behalf of the school are called 'Data Processors'. Under the UK GDPR and domestic data protection legislation, Data Processors, alongside Data Controllers, can be held directly responsible should there be a data breach.

As a Data Controller, the School commits to ensure that:

2.1.1 Personal data is processed lawfully fairly and in a transparent manner;
2.1.2 Personal data is collected for a specified, explicit and legitimate purpose and not further processed;
2.1.3 Personal data is adequate, relevant and limited as it must not be excessive in relation to the reason it has been collected (or processed);
2.1.4 Personal data is updated regularly and every reasonable step is taken to ensure it is accurate;

2.1.5 Individuals can exercise their rights to their personal data
2.1.6 Personal data is kept in accordance with sound record retention and archiving procedures;
2.1.7 Personal data is protected against accidental, unlawful destruction, alteration, processing and disclosure;
2.1.8 Adequate technical and organisational security measures are applied when processing personal data.

3. INDIVIDUAL RIGHTS

The UK GDPR and domestic data protection legislation provides the following rights for individuals:

3.1 The right to be informed

3.2 The right to access

3.3 The right to rectification

3.4 The right to erasure

3.5 The right to restrict processing

3.6 The right to data portability

3.7 The right to object

3.8 Rights in relation to automated decision making and profiling

4. LAWFUL BASIS FOR PROCESSING

4.1 For personal data to be processed lawfully, it must be processed on the basis of one six lawful basis set out in the Data Protection Legislation. The School will normally process personal data under the following:

4.1.1 where the processing is necessary for the performance of a contract between us and the data subject, such as an employment contract;

4.1.2 where the processing is necessary to comply with a legal obligation that we are subject to, (e.g. the Education Acts);

4.1.3 where the law otherwise allows us to process the personal data or we are carrying out a task in the public interest or a task vested in us as a public authority;

4.1.4 where it is appropriate for the vital interests (life and death situation) of that individual;

4.1.5 where the processing is for our legitimate interests when we are not acting in our capacity as a public authority; and

4.1.6 where appropriate, with the consent of the data subject to the processing of their personal data.

4.2 When special category personal data is being processed then an additional safeguard must apply to that processing. The School will normally only process special category personal data under the following conditions:

4.2.1 where the processing is necessary for employment law purposes, for example in relation to sickness absence;

4.2.2 where the processing is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment and/or safeguarding individuals at risk and provided the appropriate policy document is in place;

4.2.3 where the processing is necessary for health or social care purposes, for example in relation to pupils with medical conditions or disabilities;

4.2.4 where appropriate, with the explicit consent of the individual.

4.3 We will inform data subjects of the above matters by way of appropriate privacy notice which shall be provided to them when we collect the data or as soon as possible thereafter.

4.4 If any employee, contractor or supplier is in doubt as to whether they can use any personal data for any purpose then they must contact the DPO before doing so.

4.5 Consent

4.5.1 In order to collect and process data that does not fall into another lawful basis, the School will seek to gain freely given, informed and unambiguous consent provided with affirmative action, in order to collect information from:

a. a child with competency unless consent specifically relates to processing information on a direct online service (in which case this will be a child over the age of 13 with sufficient competency); or

b. a parent/guardian of that child who holds parental responsibility.

4.5.2 The School recognises its responsibility to ensure that any collection of data for children without competency is consented to by the parent(s) or carers who hold parental responsibility.

4.5.3 The School recognises that if it accepts consent from a holder of parental responsibility over a child, in order to process their personal information it will need to gain the personal consent of the child once the child has either;

a. gained a developed sense of understanding and competence; or

b. reached the age of maturity in terms of online services (13 years).

4.5.4 The School recognises that this age of competence will vary from child to child.

5. OBLIGATIONS OF THE SCHOOL

5.1 It is committed to creating, storing and managing its records securely, efficiently accurately and effectively. The School recognises that this is necessary to support its core functions, to comply with legal requirements and for its operational and information needs and to contribute to the effective management of the institution. It also recognises that efficient, accurate, secure and effective record management is helpful to the wider support of staff and students and contributes to the safeguarding of their health, safety and welfare.

5.2 To underpin the collection of information, processing and management of records, the School will endeavour to ensure:

a. the regulation of efficient creation, storage, maintenance and destruction of records including pseudonymisation;

b. that information will only be shared if the appropriate parents, carers or pupils have been notified of this via a privacy notice prior to the collection of the personal data or with their unequivocal consent where applicable;

c. the sharing of individuals' data will be in relation to a legal obligation, a data sharing agreement or a contractual arrangement;

d. the efficient and effective maintenance of the School academic, management and administrative systems;

e. the upkeep of annual staff training in regard to data protection;

f. the secure retention, retrieval and destruction of records, in compliance with statutory and School requirements;

g. regular audits are conducted to ensure the compliance of the UK GDPR via the Data Protection Officer;

h. the creation and maintenance of accurate and complete records in order to maximise efficiency, adopting the 'privacy by design' approach;

i. that a record is kept of the information being processed;

j. the delivery of services to staff, students and stakeholders in a consistent and equitable manner using computerised systems, where appropriate;

j. a continuity of service in the event of a disaster;

k. appropriate safeguards are in place in the event of transferring personal data outside of the UK and EEA.

6. ORGANISATIONAL SCOPE

6.1 This policy applies to the School and to any commercial organisations or service providers (including agencies or consultancy companies) contracted to carry out work for the School.

7. POLICY STATEMENT

7.1 In order to support its compliance, the School will adhere to the principles and codes of practice enshrined in the UK GDPR and domestic data protection legislation.

7.2 The School will increase openness, promote transparency and demonstrate accountability by supporting the proactive sharing of information with its parents/ carers, pupils, employees and those who come into contact with the School.

7.3 The UK GDPR and domestic data protection legislation gives individuals the right to know what information is held about them, how it is processed and subject to certain exemptions, receive a copy of that information. It also provides a framework to ensure that personal data is handled appropriately.

8. RIGHTS OF THE INDIVIDUAL

Introduction

8.1 Data subjects have certain rights in respect of their personal data. When we process data subjects' personal data, we shall respect those rights. These procedures provide a framework for responding to requests to exercise those rights. It is our policy to ensure that requests by data subjects covered by these procedures to exercise their rights in respect of their personal data are handled in accordance with applicable law.

8.2 For the purposes of these procedures, "personal data" means any information relating to an identified or identifiable data subject. An identifiable data subject is anyone who can be identified, directly or indirectly, by reference to an identifier, such as a name, identification number or online identifier. "Processing" means any operation or set of operations that is performed on personal data, such as collection, use, storage, dissemination and destruction.

8.3 To ensure that where relevant and / or where appropriate a Privacy Notice will, where necessary, be displayed at the head of forms, requiring the disclosure of personal data from an individual. The School's standard privacy notice can be found on its website**.** This notice will inform the individual completing the form why their information is being collected, with whom it will be shared and why, what will be done with it, where it will be stored,for how long and their rights under data protection legislation.

8.4 These procedures only apply to data subjects whose personal data we process.

9. Responding to requests to access personal data

9.1 Data subjects have the right to request access to their personal data processed by us. Such requests are called subject access requests (SARs). When a data subject makes an SAR we shall take the following steps on the SAR spreadsheet:

9.1.1 log the date on which the request was received (to ensure that the relevant timeframe of one calendar month for responding to the request is met);

9.1.2 confirm the identity of the data subject who is the subject of the personal data. For example, we may request additional information from the data subject to confirm their identity (this may stop the statutory time limit of one calendar month until identification is provided);

9.1.3 search databases, systems, applications and other places where the personal data which are the subject of the request may be held;

9.1.4 confirm to the data subject whether or not personal data of the data subject making the SAR are being processed; and

9.1.5 record all key dates i.e. acknowledgement sent and date of final disclosure.

9.2 If personal data of the data subject are being processed, we shall provide the data subject with the following information in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in writing or by other (including electronic) means:

9.2.1 the purposes of the processing;

9.2.2 the categories of personal data concerned (for example, contact details, bank account information and details of sales activity);

9.2.3 the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients overseas (for example, US-based service providers);

9.2.4 where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

9.2.5 the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data or to object to such processing;

9.2.6 the right to lodge a complaint with the Information Commissioner's Office (ICO);

9.2.7 where the personal data are not collected from the data subject, any available information as to their source;

9.2.8 the existence of automated decision-making and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject; and

9.2.9 where personal data are transferred outside the UK and EEA, details of the appropriate safeguards to protect the personal data.

9.3 We shall also, unless there is an exemption (see paragraph 16 below), provide the data subject with a copy of the personal data processed by us in a commonly used electronic form (unless the data subject either did not make the request by electronic means or has specifically requested not to be provided with the copy in electronic form) within one month of receipt of the request. If the request is complex, or there are a number of requests, we may extend the period for responding by a further two months. If we extend the period for responding we shall inform the data subject within one month of receipt of the request and explain the reason(s) for the delay.

Where a request for the education record is received from a parent, we will consider the request in line with The Education (Pupil Information) Regulations 2005.

9.4 Before providing the personal data to the data subject making the SAR, we shall review the personal data requested to see if they contain the personal data of other data subjects. If they do, we may redact the personal data of those other data subjects prior to providing the data subject with their personal data, unless those other data subjects have consented to the disclosure of their personal data or it is reasonable to disclose.

9.5 If the SAR is manifestly unfounded or excessive, for example, because of its repetitive character, we may charge a reasonable fee, taking into account the administrative costs of providing the personal data, or refuse to act on the request.

9.6 If we are not going to respond to the SAR we shall inform the data subject of the reason(s) for not taking action and of the possibility of lodging a complaint with the ICO.

9.7 Where a non-work (i.e. private) email account is used to conduct work-related communications and/or official School business and the School reasonably suspects that information concerning the School's official business is held on that private account, The School shall require that individual to search their private email account. A record of the action taken will be recorded by the School. School personnel should note that they may be guilty of a criminal offence if they altar, deface, block, erase, destroy or conceal any record held by or on behalf of School, with the intention of preventing the disclosure of all, or any part, of the information that the applicant would be entitled to under the UK GDPR and domestic data protection legislation. The discovery or suspicion of any such offence must be reported immediately to management and the named Data Protection Officer and may be referred to the police. This policy applies to all recorded information held by the School in any format, including text message, messages sent over instant messaging networks, Facebook messages and other forms of electronic communications where they relate to the business of the School, whether sent using official or private accounts.

9.8 Personal Data will, under normal circumstances, only be disclosed to a third party after written consent from the individual concerned has been obtained or the disclosure falls under an alternative legal basis, alongside a privacy notice being brought to the individual's attention.

9.9 However, the requirement to obtain consent may be overridden in the event that the data falls within: a) an information sharing protocol or contract; b) one or more of the exemptions under the UK GDPR and domestic data protection legislation; or c) a court order or Parliamentary statute.

9.10 In exceptional circumstances, staff will take reasonable action to inform the responsible authorities or employers of relevant Personal Data where there is a risk from others, a risk to an individual or where School receives lawful authority to disclose personal information or where there is an emergency situation based on the lawful basis of vital interests.

10. Responding to requests to rectify personal data

10.1 Data subjects have the right to have their inaccurate personal data rectified. Rectification can include having incomplete personal data completed, for example, by a data subject providing a supplementary statement regarding the data. Where such a request is made, we shall, unless there is an exemption (see paragraph 16 below), rectify the personal data without undue delay.

10.2 We shall also communicate the rectification of the personal data to each recipient to whom the personal data have been disclosed (for example, our third party service

providers who process the data on our behalf), unless this is impossible or involves disproportionate effort. We shall also inform the data subject about those recipients if the data subject requests it.

10.3 Staff will regularly liaise with pupils and parents to ensure an adequate process of updating information.

10.4 However, staff will also allow parents/pupils to update their details through the normal means of contact with the School.

11. Responding to requests for the erasure of personal data

11.1 Data subjects have the right, in certain circumstances, to request that we erase their personal data. Where such a request is made, we shall, unless there is an exemption (see paragraph 16 below), erase the personal data without undue delay if:

11.1.1 the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

11.1.2 the data subject withdraws their consent to the processing of their personal data and consent was the basis on which the personal data were processed and there is no other legal basis for the processing;

11.1.3 the data subject objects to the processing of their personal data on the basis of our performance of a task carried out in the public interest or in the exercise of official authority vested in us, or on the basis of our legitimate interests which override the data subject's interests or fundamental rights and freedoms, unless we either can show compelling legitimate grounds for the processing which override those interests, rights and freedoms, or we are processing the data for the establishment, exercise or defence of legal claims;

11.1.4 the data subject objects to the processing of their personal data for direct marketing purposes;

11.1.5 the personal data have been unlawfully processed;

11.1.6 the personal data have to be erased for compliance with a legal obligation to which we are subject; or

11.1.7 the personal data have been collected in relation to the offer of e-commerce or other online services.

11.1.8 When a data subject makes a request for erasure in the circumstances set out above, we shall, unless there is an exemption (see paragraph 16 below), take the following steps:

11.1.9 log the date on which the request was received (to ensure that the relevant timeframe of one month for responding to the request is met);

11.1.10 confirm the identity of the data subject who is the subject of the personal data. We may request additional information from the data subject to do this;

11.1.11 search databases, systems, applications and other places where the personal data which are the subject of the request may be held and erase such data within one month of receipt of the request. If the request is complex, or there are a number of requests, we may extend the period for responding by a further two months. If we extend the period for responding we shall inform the data subject within one month of receipt of the request and explain the reason(s) for the delay;

11.1.12 where we have made the personal data public, we must, taking reasonable steps, including technical measures, inform those who are processing the personal data that the data subject has requested the erasure by them of any links to, or copies or replications of, those personal data; and

11.1.13 communicate the erasure of the personal data to each recipient to whom the personal data have been disclosed unless this is impossible or involves disproportionate effort. We shall also inform the data subject about those recipients if the data subject requests it.

11.2 If the request is manifestly unfounded or excessive, for example, because of its repetitive character, we may charge a reasonable fee, taking into account the administrative costs of erasure, or refuse to act on the request.

11.3 If we are not going to respond to the request we shall inform the data subject of the reasons for not taking action and of the possibility of lodging a complaint with the ICO.

11.4 In addition to the exemptions in paragraph 16 below, we can also refuse to erase the personal data to the extent processing is necessary:

11.4.1 for exercising the right of freedom of expression and information;

11.4.2 for compliance with a legal obligation which requires processing by law and to which we are subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in us;

11.4.3 for reasons of public interest in the area of public health;

11.4.4 for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

11.4.5 for the establishment, exercise or defence of legal claims.

12. Responding to requests to restrict the processing of personal data

12.1 Data subjects have the right, unless there is an exemption (see paragraph 16 below), to restrict the processing of their personal data if:

12.1.1 the data subject contests the accuracy of the personal data, for a period to allow us to verify the accuracy of the personal data;

12.1.2 the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

12.1.3 we no longer need the personal data for the purposes we collected them, but they are required by the data subject for the establishment, exercise or defence of legal claims; and

12.1.4 the data subject has objected to the processing, pending verification of whether we have legitimate grounds to override the data subject's objection.

12.2 Where processing has been restricted, we shall only process the personal data (excluding storing them):

12.2.1 with the data subject's consent;

12.2.2 for the establishment, exercise or defence of legal claims;

12.2.3 for the protection of the rights of another person; or

12.2.4 for reasons of public interest.

12.3 Prior to lifting the restriction, we shall inform the data subject of the lifting of the restriction.

12.4 We shall communicate the restriction of processing of the personal data to each recipient to whom the personal data have been disclosed, unless this is impossible or involves disproportionate effort. We shall also inform the data subject about those recipients if the data subject requests it.

13. Responding to requests for the portability of personal data

13.1 Data subjects have the right, in certain circumstances, to receive their personal data that they have provided to us in a structured, commonly used and machine-readable format that they can then transmit to another company. Where such a request is made, we shall, unless there is an exemption (see paragraph 16 below), provide the personal data without undue delay if:

13.1.1 the legal basis for the processing of the personal data is consent or pursuant to a contract; and

13.1.2 our processing of those data is automated.

13.2 When a data subject makes a request for portability in the circumstances set out above, we shall take the following steps:

13.2.1 log the date on which the request was received (to ensure that the relevant timeframe of one month for responding to the request is met);

13.2.2 confirm the identity of the data subject who is the subject of the personal data. We may request additional information from the data subject to confirm their identity; and

13.2.3 search databases, systems, applications and other places where the personal data which are the subject of the request may be held and provide the data subject with such data (or, at the data subject's request, transmit the personal data directly to another company, where technically feasible) within one month of receipt of the request. If the request is complex, or there are a number of requests, we may extend the period for responding by a further two months. If we extend the period for responding we shall inform the data subject within one month of receipt of the request and explain the reason(s) for the delay.

13.3 If the request is manifestly unfounded or excessive, for example, because of its repetitive character, we may charge a reasonable fee, taking into account the administrative costs of providing or transmitting the personal data, or refuse to act on the request.

13.4 If we are not going to respond to the request we shall inform the data subject of the reasons for not taking action, the possibility of lodging a complaint with the ICO and their right to a judicial remedy.

14. Responding to objections to the processing of personal data

14.1 Data subjects have the right to object to the processing of their personal data where such processing is on the basis of our performance of a task carried out in the public interest or in the exercise of official authority vested in us, or on the basis of our legitimate interests which override the data subject's interests or fundamental rights and freedoms, unless we either:

14.1.1 can show compelling legitimate grounds for the processing which override those interests, rights and freedoms; or

14.1.2 are processing the personal data for the establishment, exercise or defence of legal claims.

14.2 Data subjects also have the right to object to the processing of their personal data for scientific or historical research purposes, or statistical purposes, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

14.3 Where personal data are processed for direct marketing purposes, data subjects have the right to object at any time to the processing of their personal data for such marketing. If a data subject makes such a request, we shall stop processing the personal data for such purposes.

15. Responding to requests not to be subject to automated decision-making

15.1 Data subjects have the right, in certain circumstances, not to be subject to a decision based solely on the automated processing of their personal data, if such decision produces legal effects concerning them or similarly significantly affects them. Where such a request is made, we shall, unless there is an exemption (see paragraph 16 below), no longer make such a decision unless it:

15.1.1 is necessary for entering into, or the performance of, a contract between us and the data subject;

15.1.2 is authorised by applicable law which lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests; or

15.1.3 is based on the data subject's explicit consent.

15.2 If the decision falls within paragraph 15.1.1 or paragraph 15.1.3, we shall implement suitable measures to safeguard the data subject's rights, freedoms and legitimate interests, including the right to obtain human intervention, to express their point of view and to contest the decision.

16. Exemptions

16.1 Before responding to any request we shall check whether there are any exemptions or restrictions that apply to the personal data that are the subject of the request. Exemptions may apply where it is necessary and proportionate not to comply with the requests described above.

16.2 Before applying an exemption or restriction, the School will confer with the School's Data Protection Officer.

16.3 In the event of a Subject Access Request, staff may be asked to provide all details, hard copy or electronic, concerning personal information of that individual to the Senior Leadership Team.

17. DATA RETENTION

17.1 The School have implemented a record retention schedule.

18. DATA PROTECTION IMPACT ASSESSMENTS

18.1 Information risk is considered and afforded a priority in decisions within School in the same way as financial and operational risk. The School agrees to conduct Data Protection Impact Assessments (DPIA) whenever a new process is implemented that presents a significant risk to pupil, parent, visitor or employee personal data and/or where a new digital system is implemented. The School recognises that as a Data Controller, the decision to carry out a DPIA lies with it. However, the implementation of a DPIA will be conducted with the guidance of the School's Data Protection Officer.

18.2 Data Impact Assessments will be recorded in a format recommended by the Information Commissioner's Office and stored in a safe and secure system where risk assessments are usually placed, accessible to authorised individuals only.

18.3 Information risk will be managed by a process of identifying, controlling, minimising and/or eliminating risks that may affect School's information or information systems.

19. DATA SECURITY

19.1 The School recognises its obligations to safely store documents that hold personally identifiable information.

19.1.1 **Non-Electronic Files**:

a. Storage of hard copies will be kept in locked cabinets, secure desk drawers and individual rooms will have access cards/key locks to allow authorised entry only.

b. In the event that hard copy documents containing personal information need to be physically transported, they will be stored in a secure wallet with an authorised individual.

19.1.2 **Electronic Files**:

a. Electronic Files will be stored on a database that is password protected and allows only authorised staff member access.

b. In the event that files containing personal information need to be sent, moved or shared, they will be encrypted and password protected to ensure they are available to authorised individuals only.

c. Where necessary, pseudonymisation of personal data will be implemented.

20. RESPONSIBILITY FOR ACCESS TO INFORMATION

20.1 Overall responsibility for disclosure of Personal Data lies with the Senior Leadership Team.

20.2 The Governing body will endeavour to ensure effective implementation of this policy and put in place mechanisms for its review in line with guidance from the School's named Data Protection Officer.

20.3 Each individual employee is responsible for actively supporting this policy. School personnel are responsible for promptly retrieving information where they are requested to do so for the purpose of responding to a subject access request.

20.4 School employees must seek advice in the event of uncertainty in relation to this policy.

20.5 Senior Leadership Team in conjunction with the named Data Protection Officer's guidance, are responsible for ensuring that School Personnel within their area of control are aware of this policy and are adequately trained in the handling of information and Subject Access Requests.

20.6 School Personnel must familiarise themselves with their obligations via the rolling programme of staff training, specifically, procedures and guidance available.

20.7 The Data Protection Officer has responsibility for the following tasks:

a) To oversee the development and review of this Data Protection Policy, Privacy Notice, Record Retention Schedule and relating documents;

b) The interpretation of this policy, for monitoring compliance with the policy and for providing advice and guidance on its implementation;

c) To develop procedures and guidance to enable staff to carry out their own effective record management, ensuring that procedures are published and communicated to Senior Leadership Team and trickled down;

d) To act as a competent person regarding data protection, by providing guidance for subject access requests and record management;

e) To ensure that Subject Access Requests are dealt with efficiently and effectively, meeting legislative requirements;

f) To provide advice and guidance to staff on security of information, access to information and records management;

g) To identify current and proposed legislation relevant to School and inform School management;

k) Be responsible for liaising with the Information Commissioner's Office on any matter relating to School's handling or resolution of a Subject Access Request, incident or breach of the UK GDPR or domestic data protection legislation.

21. BREACH OF ANY REQUIREMENT OF the UK GDPR AND DOMESTIC LEGISLATION

21.1 Any breach will be reported as soon as it is discovered to nominated members of the Senior Leadership Team.

21.2 The Data Protection Officer will be made aware of the breach as soon as possible and advise the school as to whether the breach should be reported to the Information Commissioner or if further investigation is required.

21.3 The breach will be treated in accordance with the School's Breach Procedure.

22. ICO CONTACT

22.1 If an individual believes that their data has not been handled appropriately, they can send a complaint to the School (the Data Controller) who will forward this on to the Data Protection Officer for guidance.

If individuals remain unsatisfied once they have received a response from the School, they can send a complaint directly to the ICO:

Information Commissioner's Office
Wycliffe House,
Water Ln,
Wilmslow
SK9 5AF

Telephone: 0303 123 1113, Monday-Friday 9am-5pm.

Appendix

Definitions

UK GDPR: The UK General Data Protection Regulation and all legislation operating within England enacted in relation to this legislation.

Personal Data: means any information relating to an identifiable natural person, whether they can be directly or indirectly identified by reference to name, identification number, online identifier, or to specific things such as physical, physiological, genetic, mental, economic, cultural or social identity factors. You will often see this in reference to the term Natural Person.

Special Category Data: As above but this is called Special Category personal data and needs to be looked after very carefully; it refers to very specific groups of personal data such as race or ethnic origin, political views, trade union membership, genetic and biometric data, health and sexual orientation. It should not be collected unless it is necessary.

ICO: The Information Commissions Office is the UKs Supervisory Authority, which is the organisation that oversees data protection in England, Wales and Northern Ireland and, to a limited extent, in Scotland. The Commissioner is the regulator appointed by the Crown to promote public access to official information and protect personal information.

Information and processing: any information, data or records, irrespective of format or medium, which are generated or processed. Examples include electronic communications, e-mails, video recordings, hardcopy (paper) files, images, graphics, maps, plans, technical drawings, programs, software and all other types of data. Processing is a collective term when you collect, use, share or store data. The UK GDPR focuses specifically, but not completely, on digital data such as used in computers, phones and tablets, and on websites.

Data Controller: is the person or organisation that an individual has allowed, or is obliged, to hold their personal details on the lawful basis of Public Interest. The Data Controller decides what, why, how, where and when personal data is processed. A School is most often the Data Controller.

Domestic Data Protection Legislation: The Data Protection Act 2018 and any other applicable domestic data protection legislation.

Data Processor: This is a person or organisation that the Data Controller has asked to ‘do something’ with the data they control. They must only ‘do’ what is allowed in the data sharing agreement. They are breaking the law if they use this data for any other purpose. In a number of cases, the Data Controller and the Data Processor is the same person or organisation. If a School collects and uses the data, without it being shared or processed with anyone else, then they are both Data Controller and Data Processor. Data Controllers need to have a Data Sharing Agreement in place with Processors to outline agreed processing and confidentiality obligations.

Subject Access Request (SAR): request made by, or on behalf of, a data subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data.

Privacy notice: This is your notice to the world about the way you handle information you have access to. Every School must have one already and it’s important that all staff know what it says and means. It should also be in clear language so it can be easily understood by parents and children, where relevant.

Lawful basis for processing: Also referred to as legal basis for processing. No organisation can process data unless there is a legal reason for doing so. There are six main categories for lawful processing; consent, contract, legitimate interests, vital interests, public task, legal obligation. The majority of the School's ability to collect and process personal data will rely on the lawful basis of 'Public Task' or 'Legal Obligation'. It may on occasion rely on consent, although this can easily be withdrawn.

Encrypted Data: This is when the data is scrambled and only a key (such as a password) can align the data to make it identifiable. Personal data that leaves a safe and secure environment must be encrypted.

Data Breach: This is a breach of security, a breach of availability or data that is not correct when it should be; where accidentally or unlawfully personal data has been destroyed or misused. This might lead to physical or mental harm to an individual.

Data Protection Impact Assessment (DPIA): Is a tool used to identify and reduce the privacy risks. It is particularly used when implementing new systems. A DPIA is a risk assessment for a particular processing activity. The school conducts DPIAs for new systems and when processing special category data or processing on a large scale.

Privacy by Design: This means you consider data protection and privacy from every angle. It is beneficial to internalise this method prior to implementing a procedure/process.

Data Erasure/Right to be forgotten: An individual can ask the Data Controller to remove and stop processing their personal data. If the Data Controller can justify it needs to process this data, then the request can be refused.

Data Protection Officer (DPO): An expert on data protection who works independently to oversee that data protection policies and issues are correctly managed. See 1.5 for details.

Pseudonymisation: This is a process that is used a lot in education where data is analysed and presented in reports or for examples, but the links to identify individuals are removed.