Data Protection & GDPR Policy

Phoenix Community Primary School

Author: Chris Johnson (Headteacher)

Ratified by the Governing Body: January 2022
Due for Review: January 2023

Table of Contents

GDPR and Data Protection Policy

GDPR and Data Protection Policy

General Data Protection Regulation (GDPR) and The Data Protection Act 2018 (DPA) is the law that protects personal privacy and upholds individual's rights. It applies to anyone who handles or has access to people's personal data.

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the legislation. It will apply to personal information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

Policy Objectives

The school as the Data Controller will comply with its obligations under the GDPR and DPA and other relevant legislation. Phoenix Community Primary School is committed to being concise, clear and transparent about how it obtains, uses, processes personal information and will ensure data subjects are aware of their rights under the legislation.

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

The Information Commissioner as the Regulator can impose fines of up to 20 million Euros (approximately £17 million) or in the case of an undertaking, up to 4% of the organisation's total global turnover of the preceding fiscal year, whichever is higher, for serious breaches of the GDPR, therefore it is imperative that Phoenix Community Primary School and all staff comply with the legislation.

Freedom of Information (FOI)

As a result of being a public body Phoenix Community Primary School is required to publish certain information once they receive a request from the public. The School is committed to transparency in its dealings with the public and fully embraces the aims of the Freedom of Information Act 2000 ("FOI Act"), with consideration to the data protection principles set forth under GDPR as well as DPA. Phoenix Community Primary School will make every effort to meet its obligations under the respective legislation and will regularly review procedures to ensure that it is doing so.

However, the School has right to refuse the entire request under FOI Act in cases of when (i) too much cost or staff time is needed to deal with the request; (ii) the request is vexatious; (iii) the request repeats a previous request from the same person. Moreover, Phoenix Community Primary School can refuse the request if there is an 'absolute' exemption, for example if the requested information is accessible by other means, or it is a court record or related to security matters.

The School can rely on a 'qualified' exemption if it can show with the facts (e.g., disclosing of the information would jeopardise the safety of national security, influence law enforcement activities, or the information must be protected legally) and if disclosing the requested information overrides the public interest. The School can refuse the request based on a commercial interest exemption, if the requested information constitutes a trade secret; and/or would, or would be likely to, biases the commercial interests of Phoenix Community Primary School or any person.

Scope of the Policy

Personal data is any information that relates to an identified or identifiable living individual who can be identified directly or indirectly from the information[1]. The information includes factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a living individual. This includes any expression of opinion about an individual and intentions towards an individual. Under the GDPR personal information also includes an identifier such as a name, an identification number, location data or an online identifier.

What Personal Information does the School Process?

The School collects a large amount of personal data every year including: pupil records, staff records, names and addresses of those requesting prospectuses, examination marks, references, fee collection as well as the many different types of research data used by the School. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies. This can include date on pupil assessments, incidents of discrimination including racial incidents and pupil specific information such as eligibility for Free School Meals. Categories of data we collect are parent data, pupil data, employee data & teacher data.

How does The School collect the personal information?

As a school we collect the data from individuals via registration forms, CTF files from other schools, safeguarding records from other schools (electronic and paper) as well as paper and electronic forms from other agencies such as social services. We also collect personal information in person or on the telephone from parents and other professionals, these are noted and recorded on school systems.

The Data Protection Principles

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

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

Transfer Limitation

In addition, personal data shall not be transferred to a country outside the UK unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the

[1] GDPR Article 4 Definitions

processing of personal data as determined by the ICO or where the organisation receiving the data has provided adequate safeguards[2].

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

The School shares personal information with third parties such as catering suppliers, parent communication portal (ParentMail), curriculum tools (Purple Mash, Seesaw, Accelerated Reader, My On Reading, Spelling Shed & Doodle Maths), safeguarding management software (My Concern), management information system for pupil and staff data (SIMS), recruitment (Kent Teach), school photographer, SEN specialists (educational psychologists), social services including social workers and Early Help, admissions and statutory returns.

The purposes of school processing personal information are for a range of contractual, statutory or public interest purposes, including the following:

- To deliver and administer pupils' education, record the details of learning, support accurate assessment and analysis of learning
- To administer the financial aspects efficiently, according to school policies including for parent payments, payments to 3rd parties and staff pay and allowances
- To deliver IT facilities to stakeholders including staff, parents and pupils. Some of these IT services are specific to an educational context (e.g. Seesaw and PurpleMash).
- To deliver facilities and services (e.g. sport, meals, trips).
- To enable participation at events (e.g. external competitions & visits).
- To communicate effectively by post, email and phone, including the distribution of relevant newsletters and circulars.
- To operate security (including CCTV), governance, disciplinary (including misconduct), complaint, audit and quality assurance processes and arrangements. Note that information collected for a different purpose may be re-used for disciplinary purposes, including to identify, where this is proportionate and necessary (e.g. IT logs showing network/computer access and use, or CCTV images/photos).
- To support training, medical, safety, welfare and religious requirements.
- To compile statistics and conduct surveys and research for internal, statutory reporting, or public or legitimate interest purposes.
- To fulfil and monitor our responsibilities under equalities, immigration and public safety legislation.
- To enable us to contact others in the event of an emergency (we will assume that you have checked with the individuals before you supply their contact details to us).

[2] These may be provided by a legally binding agreement between public authorities or bodies, standard data protection clauses provided by the ICO or certification under an approved mechanism.

Lawful Basis for processing personal information

Before any processing activity starts for the first time, and then regularly afterwards, the purpose(s) for the processing activity and the most appropriate lawful basis (or bases) for that processing must be selected and explained with practical examples and reasons relevant to each processing activity (Please see next section):

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the school
- Processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract
- Processing is necessary for compliance with a legal obligation to which the data controller is subject
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person
- Processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party[3]
- The data subject has given consent to the processing of his or her data for one or more specific purposes. Agreement must be indicated clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, the consent must be kept separate from those other matters

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

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

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

What are the Purposes to process Personal Information?

Below are some common purposes for each of the six lawful bases to process personal information:

1. **Consent**: school may use consent to provide various marketing purposes such as for school photographers. Please note that this 'consent' is different to the consent school may use for other operational purposes (e.g. parental consent for a learner to attend a school visit).
2. **Contract**: The contract basis is appropriate when there will be a contract between the school and the Data Subject. It may be appropriate where contracts are formed between the school and parents for certain purposes (e.g. an after-school club or trip).

[3] The GDPR states that legitimate interests do not apply to processing carried out by public authorities in the performance of their tasks, Article 6 However, the ICO indicates that where there are other legitimate purposes outside the scope of the tasks as a public authority, legitimate interests may be considered where appropriate (particularly relevant for public authorities with commercial interests).

3. **Legal obligation**: there are a range of legal obligations that schools are required to comply with, set out in law or statutory guidance. Where this is the case, it may be appropriate to use the 'necessary for legal obligation' lawful basis for the required Processing.
4. **Vital interests**: this lawful basis is concerned with the protection of life where the Data Subject is unable to provide consent, it is conceivable that school might rely upon it for the provision of emergency medical care (e.g. where a learner has had a serious accident, and Personal Data [such as medical records] needs to be provided to ambulance staff).
5. **Public interests**: the Education Act 1996 requires that schools operate and that children in England and Wales aged five to 16 receive full-time education. Schools are therefore undertaking a public task (defined in the GDPR (Article 6e) as "a task carried out in the public interest or in the exercise of official authority vested in the school"). Providing that it is necessary for this 'public task' purpose – much processing in school would be supported by the 'public interests' lawful basis.
6. **Legitimate interests**: where school undertake activities that are not fundamental education activities, such as letting out school facilities, arranging or facilitating after-school or extra-curricular activities, or sporting events not part of taught sports in the school, it could be that the school would have a legitimate interest in undertaking Processing of Personal Data.

Sensitive Personal Information

Processing of sensitive personal information (known as 'special categories of personal data') is prohibited[4] unless a lawful special condition for processing is identified.

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

Sensitive personal information will only be processed if:

- There is a lawful basis for doing so as identified on previous page
- One of the special conditions for processing sensitive personal information applies:

  a. the individual ('data subject') has given explicit consent (which has been clearly explained in a Privacy Notice)
  b. the processing is necessary for the purposes of exercising the employment law rights or obligations of the school or the data subject
  c. the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent
  d. the processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim
  e. the processing relates to personal data which are manifestly made public by the data subject
  f. the processing is necessary for the establishment, exercise, or defence of legal claims
  g. the processing is necessary for reasons of substantial public interest
  h. the processing is necessary for purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, the provision of social care and the management of social care systems or services
  i. the processing is necessary for reasons of public interest in the area of public health.

The school's privacy notice(s) set out the types of sensitive personal information that it processes, what it is used for, the lawful basis for the processing and the special condition that applies.

Sensitive personal information will not be processed until an assessment has been made of the proposed processing as to whether it complies with the criteria above and the individual has been informed (by way of

[4] GDPR, Article 9

a privacy notice or consent) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

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

In terms of keeping children safe from online harm the School is required to comply with the requirements of 'codes of practice' laid out by the regulator. The School is responsible to provide clear information to children and their parents regarding harmful content that the children may reach via school computers and it must put in place risk management (potential issues children might face eg online malicious behaviours, catfishing, grooming, extremism must be written down) and implement online safety precautions for children. The school should provide training for children about the risks they can face online, these should include educating children on how to communicate with teachers and their parents and share any concerns they have without feeling embarrassed or intimidated.

Automated Decision Making

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

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

Data Protection Impact Assessments (DPIA)

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

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

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

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

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

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

Documentation and records

Written records of processing activities must be kept and recorded including:

- the name(s) and details of individuals or roles that carry out the processing

- the purposes of the processing
- a description of the categories of individuals and categories of personal data
- categories of recipients of personal data
- details of transfers to third countries, including documentation of the transfer mechanism safeguards in place
- retention schedules
- a description of technical and organisational security measures.

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

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

Records of processing of sensitive information are kept on:

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

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

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

Privacy Notice

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

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

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

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

Phoenix Community Primary School will issue a minimum of two privacy notices, one for pupil information, and one for workforce information, and these will be reviewed in line with any statutory or contractual changes. Follow this link where you will find the model privacy notice: https://www.phoenix-primary.kent.sch.uk/parents/privacy-notice-pupil-info
Follow this link to the GDPR page on KELSI where you will find the model privacy notice(s) for schools to use: http://www.kelsi.org.uk/school-management/data-and-reporting/access-to-information/the-general-data-protection-regulation-gdpr

Purpose Limitation

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

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

Data minimisation

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

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

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

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

Individual Rights

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

- To be informed about how, why and on what basis that information is processed *(see the relevant privacy notice)*
- To obtain confirmation that personal information is being processed and to obtain access to it and certain other information, by making a subject access request *(see Appendix 1 - Procedure for Access to Personal Information)*
- To have data corrected if it is inaccurate or incomplete
- To have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing ('the right to be forgotten')
- To restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased) or where the school no longer need the personal information, but you require the data to establish, exercise or defend a legal claim
- To restrict the processing of personal information temporarily where you do not think it is accurate (and the school are verifying whether it is accurate), or where you have objected to the processing (and the school are considering whether the school's legitimate grounds override your interests)
- In limited circumstances to receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format
- To withdraw consent to processing at any time (if applicable)
- To request a copy of an agreement under which personal data is transferred outside of the EEA.
- To object to decisions based solely on automated processing, including profiling
- To be notified of a data breach which is likely to result in high risk to their rights and obligations
- To make a complaint to the ICO or a Court.

How can Individuals perform their rights?

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- The source of the data, if not the individual

- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

If staff receive a subject access request in any form they must immediately forward it to the DPO.

Individual Responsibilities

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

If you have access to personal information, you must:

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

Information Security

The school will use appropriate technical and organisational measures to keep personal information secure, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. School uses online secure server providers for secure storage of personal date (One Drive, Microsoft hosted services – KLZ and Google Drive) and no personal data to be stored on the physical hard drives of individual machines. Individual machines and cloud server access is by individual passwords with permissions granted to each folder according to role.

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

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

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

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

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

Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it.

Integrity means that personal data is accurate and suitable for the purpose for which it is processed.

Availability means that authorised users can access the personal data when they need it for authorised purposes.

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

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

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

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

Storage and retention of personal information

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

Personal data should not be retained for any longer than necessary. The length of time data should be retained will depend upon the circumstances, including the reasons why personal data was obtained.
Staff should adhere to the KCC Information Management Toolkit for Schools on KELSI with reference to the Record Retention Schedule, available at the following link:
http://www.kelsi.org.uk/__data/assets/word_doc/0012/60213/InformationManagementToolkitforSchoolsv4-2.docx

Personal information that is no longer required will be deleted in accordance with the School's Record Retention Schedule.

How long does the school keep the personal information and how is it stored?

Phoenix Community Primary School keeps personal information, stored in secure locked storage or electronically with secure passwords, according to the data retention schedule which is based on the KCC Information Management Toolkit for Schools on KELSI.

Data breaches

A data breach may take many different forms:

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

The school must report a data breach to the Information Commissioner's Office (ICO) without undue delay and where possible within 72 hours, if the breach is likely to result in a risk to the rights and freedoms of individuals. The school must also notify the affected individuals if the breach is likely to result in a high risk to their rights and freedoms.

Staff should ensure they inform their line manager/DPO/Head teacher immediately that a data breach is discovered and make all reasonable efforts to recover the information, following the school's agreed breach reporting process.

Training

The school will ensure that staff are adequately trained regarding their data protection responsibilities.

Consequences of a failure to comply

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

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

If you have any questions or concerns about this policy, you should contact your line manager or the school's DPO.

Review of Policy

This policy will be updated as necessary to reflect best practice or amendments made to the GDPR or DPA and other relevant legislation.

The Supervisory Authority in the UK

Please follow this link to the ICO's website (https://ico.org.uk/) which provides detailed guidance on a range of topics including individuals' rights, data breaches, dealing with subject access requests, how to handle requests from third parties for personal data etc.

Glossary

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

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

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

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

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

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

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

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

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

General Data Protection Regulation (GDPR): General Data Protection Regulation (*(EU) 2016/679*). Personal data is subject to the legal safeguards specified in the GDPR.

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

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

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

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

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

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

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

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