DATA PROTECTION POLICY

Dormers Wells Primary

Believe Aspire Flourish

Diversity, Opportunity, Resilience, Moral values, Excellence, Respect, Self-Belief

Last reviewed, ratified and adopted by Full Governing Body	October 2025
Next review due by	October 2026

This policy will be reviewed every year.

New (in line with The Key)

From **19 June 2026**, schools **must** also give people a way of making data protection complaints. This is a new requirement introduced by the Data (Use and Access) Act 2025.

We've updated this policy to include a

- section on raising a complaint (section 6).

We've also made some additional changes; to

- clarify terminology; and related to SARs procedures and the sharing of data with third parties.

Contents

- **Introduction**
- **Legislation and guidance**
- **Section 1 – Definitions**

Section 2 - When can the school process personal data (Data Protection Principles)

- **Section 3 - Data subject's rights and requests**
- **Section 4 – Accountability**
- **Section 5 -Automated Processing and Automated Decision Making**
- **Section 6- Complaints**
- **Monitoring arrangements**
- **Links with other policies**
- **Appendix 1 – Subject Access Requests**

  Appendix 2 - Personal data breach procedure

  Appendix 3 - Subject Access Request Form

Introduction including Document Owner and Approval

Dormers Wells Primary School is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the School's policy review schedule.

A current version of this document is available to all members of staff. This can be found in the version history log.

The UK General Data Protection Regulation (UK GDPR) ensures a balance between an individual's rights to privacy and the lawful processing of personal data undertaken by organisations in the course of their business. It aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The school will protect and maintain a balance between data protection rights in accordance with the UK GDPR. This policy sets out how we handle the personal data of our pupils, parents, suppliers, employees, workers and other third parties.

This policy does not form part of any individual's terms and conditions of employment with the school and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the School's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

Legislation and guidance

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)
- Data (Use and Access) Act 2025

It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and from the Department for Education (DfE) on Generative artificial intelligence in education

It also reflects the ICO's guidance for the use of surveillance cameras and personal information.

In addition, this policy complies with our funding agreement and articles of association.

SECTION 1 - DEFINITIONS

Personal data

Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category 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 examples a name, Identification number, email address, location or date of birth, Online identifier, such as a username) or an opinion about that person's actions or behaviour. It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.

Special Categories of Personal Data and Data Relating to Criminal Convictions and Offences

Previously termed "Sensitive Personal Data", Special Category Data is similar by definition and refers to data concerning an individual Data Subject's racial or ethnic origin, political or religious beliefs, trade union membership, Genetics, Biometrics, physical and mental health, sexuality or biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes).

Personal data relating to criminal offences and convictions is included here for the purposes of this policy.

Processing

Processing data involves any activity that involves the use of personal data. This includes but is not limited to: collecting, obtaining, recording

or holding data or carrying out any operation or set of operations on that data such as organising, amending, structuring, storing, adapting, altering, retrieving using, disseminating, erasing or destroying it. Processing can be automated or manual and also includes transmitting or transferring personal data to third parties.

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.

An example of automated processing includes profiling and automated decision making. Automatic decision making is when a decision is made which is based solely on automated processing (without human intervention) which produces legal effects or significantly affects an individual. Automated decision making is prohibited except in exceptional circumstances.

Data Subject

The identified or identifiable individual whose personal data is held or processed. ~~An individual about whom such information is stored is known as the Data Subject. It includes but is not limited to employees.~~

Data Controller

A person or organisation (i.e., DWLT) that determines the purposes and the means of processing personal data. The data controller is responsible for establishing practices and policies in line with the UK GDPR.

Our school processes personal data relating to parents and carers, pupils, staff, governors, visitors and others, and therefore is a data controller.

Data processor

A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller. A data processor acts only on the instructions of the controller and does not determine the purposes or means of the processing.

Personal data breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Data Protection Impact Assessment (DPIA)

DPIAs are a tool used to identify risks in data processing activities with a view to reducing them.

Criminal Records Information

This refers to personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.

SECTION 2 - WHEN CAN THE SCHOOL PROCESS PERSONAL DATA

Data Protection Principles

The UK GDPR is based on data protection principles that our school must comply with. The School are responsible for and adhere to the principles relating to the processing of personal data as set out in the UK GDPR. The principles the School must adhere to are set out below.

The 6 principles say that personal data must be:

Principle 1: processed lawfully, fairly and in a transparent manner

The school only collect, process and share personal data fairly and lawfully and for specified purposes. The school must have a specified purpose for processing personal data and special category of data as set out in the UK GDPR.

Before the processing starts for the first time, we will review the purposes of the particular processing activity and select the most appropriate lawful basis for that processing. We will then regularly review those purposes whilst processing continues in order to satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e., that there is no other reasonable way to achieve that purpose).

Personal Data

The school may only process a data subject's personal data if one of the following fair processing conditions are met: -

- The data subject has given their consent;
- The processing is necessary for the performance of a contract with the data subject or for taking steps at their request to enter into a contract;
- To protect the data subject's vital interests;
- To meet our legal compliance obligations (other than a contractual obligation);
- To perform a task in the public interest or in order to carry out official functions as authorised by law;
- For the purposes of the School's legitimate interests where authorised in accordance with data protection legislation. This is provided that it would not prejudice the rights and freedoms or legitimate interests of the data subject.

Special Category Data

The school may only process special category data if they are entitled to process personal data (using one of the fair processing conditions above) AND one of the following conditions are met:

- The data subject has given their explicit consent;
- The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed on the school in the field of employment law, social security law or social protection law. This may include, but is not limited to, dealing with sickness absence, dealing with disability and making adjustments for the same, arranging private health care insurance and providing contractual sick pay;
- To protect the data subject's vital interests;
- To meet our legal compliance obligations (other than a contractual obligation); The processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
- Where the data has been made public by the data subject;
- To perform a task in the substantial public interest or in order to carry out official functions as authorised by law;
- Where it 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;
- Where it is necessary for reasons of public interest in the area of public health;
- The processing in necessary for archiving, statistical or research purposes.

The school identifies and documents the legal grounds being relied upon for each processing activity.

Consent

Where the School relies on consent as a fair condition for processing (as set out above), it will adhere to the requirements set out in the UK GDPR.

Consent must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they signify agreement to the processing of personal data relating to them. Explicit consent requires a very clear and specific statement to be relied upon (i.e., more than just mere action is required).

A data subject will have consented to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity will not amount to valid consent.

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured.

In cases of processing special category data and explicit consent, the school will normally seek another legal basis to process that data. However, if explicit consent is required, the data subject will be provided with full information in order to provide explicit consent.

The school will keep records of consents obtained in order to demonstrate compliance with consent requirements under the UK GDPR.

Principle 2: collected only for specified, explicit and legitimate purposes

Personal data will not be processed in any matter that is incompatible with the legitimate purposes.

The school will not use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the data subject of the new purpose (and they have consented where necessary).

Principle 3: adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed

The school will only process personal data when our obligations and duties require us to. We will not collect excessive data and ensure any personal data collected is adequate and relevant for the intended purposes.

When personal data is no longer needed for specified purposes, the school shall delete or anonymise the data.
•Please refer to the School's data Retention Policy.

Principle 4: accurate and, where necessary, kept up to date

The school will endeavour to correct or delete any inaccurate data being processed by checking the accuracy of the personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out of date personal data.

Data subjects also have an obligation to ensure that their data is accurate, complete, up to date and relevant. Data subjects have the right to request rectification to incomplete or inaccurate data held by the school.

Principle 5: Kept for no longer than is necessary for the purposes for which it is processed

Legitimate purposes for which the data is being processed may include satisfying legal, accounting or reporting requirements. The school will ensure that they adhere to legal timeframes for retaining data.

We will take reasonable steps to destroy or erase from our systems all personal data that we no longer require. We will also ensure that data subjects are informed of the period for which data is stored and how that period is determined in our privacy notices.

Please refer to the School's Retention Policy for further details about how the school retains and removes data.

Principle 6: Processed in a way that ensures it is appropriately secure, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage

In order to assure the protection of all data being processed, the school will develop, implement and maintain reasonable safeguard and security measures. This includes using measures such as:

- Encryption;
- Pseudonymisation (this is where the school replaces 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);
- Ensuring authorised access (i.e., that only people who have a need to know the personal data are authorised to access it);
- Adhering to confidentiality principles;
- Ensuring personal data is accurate and suitable for the process for which it is processed.

The school follow procedures and technologies to ensure security and will regularly evaluate and test the effectiveness of those safeguards to ensure security in processing personal data.

The school will only transfer personal data to third party service providers who agree to comply with the required policies and procedures and agree to put adequate measures in place.

This policy sets out how the school aims to comply with these principles.

Sharing Personal Data

The school will generally not share personal data with third parties unless certain safeguards and contractual arrangements have been put in place. These include, but are not limited to situations where:

- There is an issue with a pupil, or a parent or carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
  - if the third party has a need to know the information for the purposes of providing the contracted services;
  - Sharing the personal data complies with the privacy notice that has been provided to the data subject and, if required, the data subject's consent has been obtained;
  - The third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
  - The transfer complies with any applicable cross border transfer restrictions; and
  - Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors that can provide sufficient guarantees that they comply with UK data protection law
  - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

The intention to share data relating to individuals to an organisation outside of our School shall be clearly defined within written notifications and details and basis for sharing that data given.

Artificial Intelligence

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. Dormers Well Primary recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, Dormers Well Primary will treat this as a data breach and will follow the personal data breach procedure outlined in **Appendix 2.**

Transfer of Data outside of the UK (*the European Economic Area EEA)*

The UK GDPR restricts data transfers to countries outside of the UK in order to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined.

The school will not transfer data to another country outside of the UK without appropriate safeguards being in place and in compliance with the UK GDPR. All staff must comply with the school's guidelines on transferring data outside of the UK. For the avoidance of doubt, a transfer of data to another country can occur when you transmit, send, view or access that data in that particular country.

Transfer of Data Outside the UK

The school may transfer personal information outside the UK and/or to international organisations on the basis that the country, territory or organisation is designated as having an adequate level of protection or that the organisation receiving the information has provided adequate safeguards by way of binding corporate rules, standard data protection clauses or compliance with an approved code of conduct**.**

SECTION 3 - DATA SUBJECT'S RIGHTS AND REQUESTS

Personal data must be made available to data subjects as set out within this policy and data subjects must be allowed to exercise certain rights in relation to their personal data.

The rights data subjects have in relation to how the school handle their personal data are set out below:

(a) (Where consent is relied upon as a condition of processing) To withdraw consent to processing at any time;

(b) Receive certain information about the School's processing activities;

(c) Request access to their personal data that we hold (see "Subject Access Requests" at Appendix 1);

(d) Prevent our use of their personal data for marketing purposes;

(e) Ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;

(f) Restrict processing in specific circumstances;

(g) Challenge processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) Request a copy of an agreement under which personal data is transferred outside of the UK;

(i) Object to decisions based solely on automated processing;

(j) Prevent processing that is likely to cause damage or distress to the data subject or anyone else;

(k) Be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;

(l) Make a complaint to the supervisory authority; and

(m) In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format.

If any request is made to exercise the rights above, it is a requirement for the relevant staff member within the school to verify the identity of the individual making the request.

Direct Marketing

The school are subject to certain rules and privacy laws when marketing. For example, a data subject's prior consent will be required for electronic direct marketing (for example, by email, text or automated calls).

The school will explicitly offer individuals the opportunity to object to direct marketing and will do so in an intelligible format which is clear for the individual to understand. The school will promptly respond to any individual objection to direct marketing.

Employee Obligations

Employees may have access to the personal data of other members of staff, suppliers, parents or pupils of the school in the course of their employment or engagement. If so, the school expects those employees to help meet the school's data protection obligations to those individuals. Specifically, you must:

- Only access the personal data that you have authority to access, and only for authorised purposes;
- Only allow others to access personal data if they have appropriate authorisation;
- Keep personal data secure (for example by complying with rules on access to school premises, computer access, password protection and secure file storage and destruction).

- Not to remove personal data or devices containing personal data from the School premises unless appropriate security measures are in place (such as pseudonymisation, encryption, password protection) to secure the information;

- Not to store personal information on local drives.

SECTION 4 - ACCOUNTABILITY

The school will ensure compliance with data protection principles by implementing appropriate technical and organisational measures. We are responsible for and demonstrate accountability with the UK GDPR principles.

The school have taken the following steps to ensure and document UK GDPR compliance:

Data Protection Officer (DPO)

Please find below details of the School's Data Protection Officer:

Data Protection Officer: Judicium Consulting Limited
Address: 72 Cannon Street, London, EC4N 6AE
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 0203 326 9174
Lead Contact: Craig Stilwell

The DPO is responsible for overseeing this data protection policy and developing data-related policies and guidelines.

Please contact the DPO with any questions about the operation of this Data Protection Policy or the UK GDPR or if you have any concerns that this policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:

(a) If you are unsure of the lawful basis being relied on by the school to process personal data;

(b) If you need to rely on consent as a fair reason for processing (please see below the section on consent for further detail);

(c) If you need to draft privacy notices or fair processing notices;

(d) If you are unsure about the retention periods for the personal data being processed (Refer to the **School's Data Retention Policy**);

(e) If you are unsure about what security measures need to be put in place to protect personal data (Refer to the procedure set out in **Appendix 2**];

(f) If there has been a personal data breach;

(g) If you are unsure on what basis to transfer personal data outside the EEA;

(h) If you need any assistance dealing with any rights invoked by a data subject;

(i) Whenever you are engaging in a significant new (or a change in) processing activity which is likely to require a data protection impact assessment or if you plan to use personal data for purposes other than what it was collected for;

(j) If you plan to undertake any activities involving automated processing or automated decision making;

(k) If you need help complying with applicable law when carrying out direct marketing activities;

(l) If you need help with any contracts or other areas in relation to sharing personal data with third parties.

Personal Data Breaches

The UK GDPR requires the school to notify any applicable personal data breach to the Information Commissioner's Office (ICO).

We have have put in place procedures to deal with any suspected personal data breach and will notify data subjects or any applicable regulator where we are legally required to do so. (**Refer to Data Breach Procedure-Appendix 2**)

If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person designated as the **key point of contact** for personal data breaches (who is Ellie Mosley, Deputy Headteacher) or your DPO.

Transparency and Privacy Notices

The school will provide detailed, specific information to data subjects. This information will be provided through the school's privacy notices which are concise, transparent, intelligible, easily accessible and in clear and plain language so that a data subject can easily understand them. The School's privacy notices are tailored to suit the data subject and set out information about how the School use their data.

Whenever we collect personal data directly from data subjects, including for human resources or employment purposes, we will provide the data subject with all the information required by the UK GDPR including the identity of the data protection officer, the school's contact details, how and why we will use, process, disclose, protect and retain personal data.

When personal data is collected indirectly (for example from a third party or publicly available source), we will provide the data subject with the above information as soon as possible after receiving the data. The school will also confirm whether that third party has collected and processed data in accordance with the UK GDPR.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as "children" under the UK GDPR.

Privacy By Design

The school adopt a privacy be design approach to data protection to ensure that we adhere to data compliance and to implement technical and organisational measures in an effective manner.

Privacy by design is an approach that promotes privacy and data protection compliance from the start. To help us achieve this, the school takes into account the nature and purposes of the processing, any cost of implementation and any risks to rights and freedoms of data subjects when implementing data processes.

Data Protection Impact Assessments (DPIAs)

In order to achieve a privacy by design approach, the school conduct DPIAs for any new technologies or programmes being used by the school which could affect the processing of personal data. In any event the school carries out DPIAs when required by the UK GDPR in the following circumstances:

- For the use of new technologies (programs, systems or processes) or changing technologies;
- For the use of automated processing;
- For large scale processing of special category data;
- For large scale, systematic monitoring of a publicly accessible area (through the use of CCTV).

Our DPIAs contain:

- A description of the processing, its purposes and any legitimate interests used;

- An assessment of the necessity and proportionality of the processing in relation to its purpose;
- An assessment of the risk to individuals; and
- The risk mitigation measures in place and demonstration of compliance.

Record Keeping

The school are required to keep full and accurate records of our data processing activities. These records include:

- The name and contact details of the School;
- The name and contact details of the Data Protection Officer;
- Descriptions of the types of personal data used;
- Description of the data subjects;
- Details of the School's processing activities and purposes;
- Details of any third-party recipients of the personal data;
- Where personal data is stored;
- Retention periods; and
- Security measures in place.

Training

The school will ensure all relevant personnel have undergone adequate training to enable them to comply with data privacy laws.

Audit

The school and/or the DPO regularly test our data systems and processes in order to assess compliance. These are done through data audits which take place annually/regularly in order to review use of personal data.

Complaints

We take complaints about how we collect and use personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concerns about our data processing, please raise this with us in the first instance. You can make a complaint to us at any time by contacting Ellie Mosley, Deputy Headteacher.

Upon receiving a complaint, we will:

- Acknowledge receipt of the complaint within 30 days of receiving it
- Without undue delay, take appropriate steps to respond to the complaint, including:
  - Making appropriate enquiries based on the circumstances of the complaint
  - Keeping the complainant informed on the progress of the investigation
- Without undue delay, inform the complainant of the outcome of the investigation

Monitoring

The School DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and approved by the full governing board.

Links to other policies

- Freedom of information publication scheme
- online safety policy,
- acceptable use of ICT,
- CCTV policy,
- child protection and safeguarding policy
- data retention policy

These policies are also designed to protect personal data and can be found on Staff Shared drive

Appendix 1 – Subject Access Requests

1.1 Subject access requests (SARs)

Under Data Protection Law, Data Subjects have a general right to find out whether the school hold or process personal data about them, to access that data, and to be given supplementary information. This is known as the right of access, or the right to make a data subject access request (SAR). The purpose of the right is to enable the individual to be aware of, and verify, the lawfulness of the processing of personal data that the school are undertaking.

This appendix provides guidance for staff members on how data subject access requests should be handled and for all individuals on how to make a SAR.

Failure to comply with the right of access under UK GDPR puts both staff and the School at potentially significant risk and so the School takes compliance with this policy very seriously.

A Data Subject has the right to be informed by the school of the following:

(a) Confirmation that their data is being processed;
(b) Access to their personal data;
(c) The purpose for which the information is being processed;

(d) The categories of personal data concerned

(e) The recipients/class of recipients to whom that information is or may be disclosed (Who the data has been, or will be, shared with)

(f) How long the data will be stored for or, if this isn't possible, the criteria used to determine this period

(g) Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
(h) The right to lodge a complaint with the ICO or another supervisory authority
(i) Details of the School's sources of information obtained (if not the individual);
(j) Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
(k) The safeguards provided if the data is being transferred internationally
(l) In relation to any Personal Data processed for the purposes of evaluating matters in relation to the Data Subject that has constituted or is likely to constitute the sole basis for any decision significantly affecting him or her, to be informed of the logic of the Data Controller's decision making. Such data may include, but is not limited to, performance at work, creditworthiness, reliability and conduct; and

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:

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

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

1.2 Children and subject access requests

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.

How to recognise a subject access request

A data subject access request is a request from an individual (or from someone acting with the authority of an individual, e.g., a solicitor or a parent making a request in relation to information relating to their child):

- for confirmation as to whether the school process personal data about him or her and, if so
- for access to that personal data
- and/or certain other supplementary information

A valid SAR can be both in writing (by letter, email, DOJO text) or verbally (e.g., during a telephone conversation). The request may refer to the UK GDPR and/or to 'data protection' and/or to 'personal data' but does not need to do so in order to be a valid request. For example, a letter which states 'please provide me with a copy of information that the school hold about me' will be a data subject access request and should be treated as such.

A data subject is generally only entitled to access their own personal data, and not information relating to other people.

How to make a data subject access request

Whilst there is no requirement to do so, we encourage any individuals who wish to make such a request to make the request in writing, detailing exactly the personal data being requested. This allows the school to easily recognise that you wish to make a data subject access request and the nature of your request. If the request is unclear/ vague we may be required to clarify the scope of the request which may in turn delay the start of the time period for dealing with the request.

What to do when you receive a data subject access request

All data subject access requests should be immediately directed to Yatish Parmar, Trust Wide Lead, who should contact Judicium as DPO in order to assist with the request and what is required. There are limited timescales within which the School must respond to a request and any delay could result in failing to meet those timescales, which could lead to enforcement action by the Information Commissioner's Office (ICO) and/or legal action by the affected individual.

1.3 Responding to subject access requests

When receiving a SAR the School shall acknowledge the request as soon as possible and inform the requester about the statutory deadline (of one calendar month) to respond to the request.

When responding to requests, we: May ask the individual to provide 1/2 forms of identification proof of ID (if needed);

- May contact the individual (e.g. via phone) to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge

- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary (these timeframes continue to apply when the school is closed during holidays)

- further clarification about the requested information;
- if it is not clear where the information shall be sent, the school must clarify what address/email address to use when sending the requested information; and/or
- consent (if requesting third party data).

The school should work with their DPO in order to create the acknowledgment.

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

Verifying the identity of a requester or requesting clarification of the request

Before responding to a SAR, the School will take reasonable steps to verify the identity of the person making the request. In the case of current employees, this will usually be straightforward. The school is entitled to request additional information from a requester in order to verify whether the requester is in fact who they say they are. Where the School has reasonable doubts as to the identity of the individual making the request, evidence of identity may be established by production of a passport, driving license, a recent utility bill with current address, birth/marriage certificate, credit card or a mortgage statement.

If an individual is requesting a large amount of data the school may ask the requester for more information for the purpose of clarifying the request, but the requester shall never be asked why the request has been made. The school shall let the requestor know as soon as possible where more information is needed before responding to the request.

When it is necessary to verify the identity of the person making the request, the one calendar month period for responding begins when sufficient confirmation of identity is provided.

When it is necessary to request more information for the purpose of clarifying the request, the one calendar month period for responding pauses when further information is requested and does not restart until sufficient clarification is provided.

In both cases, the period of responding begins when the additional information has been received. If the School do not receive this information, they will be unable to comply with the request.

Fee for responding to a SAR

The school will usually deal with a SAR free of charge. Where a request is considered to be manifestly unfounded or excessive a fee to cover administrative costs may be requested. If a request is considered to be manifestly unfounded or unreasonable the School will inform the requester why this is considered to be the case and that the School will charge a fee for complying with the request.

A fee may also be requested in relation to repeat requests for copies of the same information. In these circumstances a reasonable fee will be charged taking into account the administrative costs of providing the information.

If a fee is requested, the period of responding begins when the fee has been received.

Time Period for Responding to a SAR

The school has one calendar month to respond to a SAR. This will run from the day that the request was received or from the day when any additional identification or other information requested is received, or payment of any required fee has been received.

The circumstances where the School is in any reasonable doubt as to the identity of the requester, this period will not commence unless and until sufficient information has been provided by the requester as to their identity and in the case of a third-party requester, the written authorisation of the data subject has been received.

The period for response may be extended by a further two calendar months in relation to complex requests. What constitutes a complex request will depend on the particular nature of the request. The DPO must always be consulted in determining whether a request is sufficiently complex as to extend the response period.

Where a request is considered to be sufficiently complex as to require an extension of the period for response, the school will need to notify the requester within one calendar month of receiving the request, together with reasons as to why this extension is considered necessary.

School closure periods

Requests received during or just before school closure periods may not be able to be responded to within the one calendar month response period. This is because the School will be closed/no one will be on site to comply with the request/our mail gets forwarded/ we do not review emails during this period. As a result, it is unlikely that your request will be able to be dealt with during this time. We may not be able to acknowledge your request during this time (i.e., until a time when we receive the request), however, if we can acknowledge the request, we may still not be able to deal with it until the school re-opens. The school will endeavour to comply with requests as soon as possible and will keep in communication with you as far as possible. If your request is urgent, please provide your request during term times and not during/close to closure periods.

Information to be provided in response to a request

The individual is entitled to receive access to the personal data we process about him or her and the following information:

- the purpose for which we process the data;
- the recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular where those recipients are in third countries or international organisations;
- where possible, the period for which it is envisaged the personal data will be stored, or, if not possible, the criteria used to determine that period;

1.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Receive certain information about the data controller's processing activities
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing that has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)

- Be notified of a personal data breach (in certain circumstances)
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)
- where the personal data has not been collected from the individual, any information available regarding the source of the data;

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

The information should be provided in a way that is concise, transparent, easy to understand and easy to access using clear and plain language, with any technical terms, abbreviations or codes explained. The response shall be given in writing if the SAR was made in writing in a commonly used electronic format.

The information that the school are required to supply in response to a SAR must be supplied by reference to the data in question at the time the request was received. However, as the school have one month in which to respond the school is allowed to take into account any amendment or deletion made to the personal data between the time the request is received and the time the personal data is supplied if such amendment or deletion would have been made regardless of the receipt of the SAR.

The school is therefore, allowed to carry out regular housekeeping activities even if this means deleting or amending personal data after the receipt of a SAR. The school is not allowed to amend or delete data to avoid supplying the data.

How to locate information

The personal data the school need to provide in response to a data subject access request may be located in several of the electronic and manual filing systems. This is why it is important to identify at the outset the type of information requested so that the search can be focused.

Depending on the type of information requested, the School may need to search all or some of the following:

- electronic systems, e.g., databases, networked and non-networked computers, servers, customer records, human resources system, email data, back up data, CCTV;
- manual filing systems in which personal data is accessible according to specific criteria, e.g., chronologically ordered sets of manual records containing personal data;
- data systems held externally by our data processors;
- occupational health records;
- pensions data;
- share scheme information;

- insurance benefit information.

The School should search these systems using the individual's name, employee number or other personal identifier as a search determinant.

Protection of third parties -exemptions to the right of subject access

There are circumstances where information can be withheld pursuant to a SAR. These specific exemptions and requests should be considered on a case-by-case basis.

The school will consider whether it is possible to redact information so that this does not identify those third parties. If their data cannot be redacted (for example, after redaction it is still obvious who the data relates to) then the school do not have to disclose personal data to the extent that doing so would involve disclosing information relating to another individual (including information identifying the other individual as the source of information) who can be identified from the information unless:

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information without the individual's consent, all of the relevant circumstances will be taken into account, including:

- the type of information that they would disclose;
- any duty of confidentiality they owe to the other individual;
- any steps taken to seek consent from the other individual;
- whether the other individual is capable of giving consent; and
- any express refusal of consent by the other individual.

It needs to be decided whether it is appropriate to disclose the information in each case. This decision will involve balancing the data subject's right of access against the other individual's rights. If the other person consents to the school disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, the school must decide whether to disclose the information anyway. If there are any concerns in this regard, then the DPO should be consulted.

Other exemptions to the right of subject access

In certain circumstances the school may be exempt from providing some or all of the personal data requested. These exemptions are described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.

Crime detection and prevention: The School do not have to disclose any personal data being processed for the purposes of preventing or detecting crime; apprehending or prosecuting offenders; or assessing or collecting any tax or duty.

Confidential references: The School do not have to disclose any confidential references given to third parties for the purpose of actual or prospective:

- education, training or employment of the individual;
- appointment of the individual to any office; or
- provision by the individual of any service

This exemption does not apply to confidential references that the school receive from third parties. However, in this situation, granting access to the reference may disclose the personal data of another individual (i.e., the person giving the reference), which means that the school must consider the rules regarding disclosure of third-party data set out above before disclosing the reference.

Legal professional privilege: The School do not have to disclose any personal data which are subject to legal professional privilege.

Management forecasting: The School do not have to disclose any personal data processed for the purposes of management forecasting or management planning to assist us in the conduct of any business or any other activity.

Negotiations: The School do not have to disclose any personal data consisting of records of intentions in relation to any negotiations with the individual where doing so would be likely to prejudice those negotiations.

Refusing to Respond to a Request

The school can refuse to comply with a request if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

If a request is found to be manifestly unfounded or excessive the school can:

- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request.

In either case the school need to justify the decision and inform the requestor about the decision.

The reasonable fee should be based on the administrative costs of complying with the request. If deciding to charge a fee the school should contact the individual promptly and inform them. The school do not need to comply with the request until the fee has been received.

Record Keeping

A record of all subject access requests shall be kept by the Deputy Head, Ellie Mosley. The record shall include the date the SAR was received, the name of the requester, what data the School sent to the requester and the date of the response.

Appendix 2 Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

- On finding or causing a breach or potential breach, the staff member, governor or data processor must immediately notify the data protection officer (DPO) by using a dedicated email address.
- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- Staff and governors will co-operate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation
- If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the headteacher and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types at the end of this procedure)
- The DPO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences
- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool
- The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school's computer system.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the school's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

- Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:

  - A description, in clear and plain language, of the nature of the personal data breach
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

- The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

  - Facts and cause
  - Effects
  - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on the school's computer system.

- The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

- The DPO and headteacher will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches

Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Relevant actions the school will take for different types of risky or sensitive personal data processed by the school. For example:

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error

- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error

- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the [ICT department/external IT support provider] to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence)

- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted
- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its 3 local safeguarding partners

Appendix 3 – Subject Access Request Form

The Data Protection Act 2018 provides you, the data subject, with a right to receive a copy of the data/information we hold about you or to authorise someone to act on your behalf. Please complete this form if you wish to make a request for your data. Your request will normally be processed within one calendar month upon receipt of a fully completed form and proof of identity.

Proof of Identity

We require proof of your identity before we can disclose personal data. Proof of your identity should include a copy of a document such as your birth certificate, passport, driving licence, official letter addressed to you at your address e.g., bank statement, recent utilities bill or council tax bill. The document should include your name, date of birth and current address. If you have changed your name, please supply relevant documents evidencing the change.

Section 1

Please fill in the details of the data subject (i.e., the person whose data you are requesting). If you are not the data subject and you are applying on behalf of someone else, please fill in the details of the data subject below and not your own.

Title	
Surname/Family Name	
First Name(s)/ Forename	
Date of Birth	
Address	
Post Code	
Phone Number	
Email address	

I am enclosing the following copies as proof of identity (please tick the relevant box):

- ☐ Birth certificate
- ☐ Driving licence
- ☐ Passport
- ☐ An official letter to my address

Personal Information

If you only want to know what information is held in specific records, please indicate in the box below. Please tell us if you know in which capacity the information is being held, together with any names or dates you may have. If you do not know exact dates, please give the year(s) that you think may be relevant.

Details:

Employment records:

If you are, or have been employed by the School and are seeking personal information in relation to your employment please provide details of your staff number, unit, team, dates of employment etc.

Details:

Section 2

Please complete this section of the form with your details if you are acting on behalf of someone else (i.e., the data subject).

If you are **NOT** the data subject, but an agent appointed on their behalf, you will need to provide evidence of your identity as well as that of the data subject and proof of your right to act on their behalf.

Title	
Surname/ Family Name	
First Name(s)/Forenames	
Date of Birth	
Address	
Post Code	
Phone Number	

I am enclosing the following copies as proof of identity (please tick the relevant box):

- ☐ Birth certificate
- ☐ Driving licence
- ☐ Passport
- ☐ An official letter to my address

What is your relationship to the data subject? (e.g., parent, carer, legal representative)

I am enclosing the following copy as proof of legal authorisation to act on behalf of the data subject:

- ☐ Letter of authority
- ☐ Lasting or Enduring Power of Attorney
- ☐ Evidence of parental responsibility
- ☐ Other (give details):

Section 3

Please describe as detailed as possible what data you request access to (e.g., time period, categories of data, information relating to a specific case, paper records, electronic records).

I wish to:

- ☐ Receive the information by post*
- ☐ Receive the information by email
- ☐ Collect the information in person
- ☐ View a copy of the information only
- ☐ Go through the information with a member of staff

*Please be aware that if you wish us to post the information to you, we will take every care to ensure that it is addressed correctly. However, we cannot be held liable if the information is lost in the post or incorrectly delivered or opened by someone else in your household. Loss or incorrect delivery may cause you embarrassment or harm if the information is 'sensitive'.

Please send your completed form and proof of identity by email to: admin@dwps.co.uk