



*Achieving Excellence Together in a Caring Community*

# Data protection policy

Date of Approval: May 2022

Review Date: May 2023

---

## Contents

1. Introduction	2
2. Definitions	2
3. The data controller	6
4. Roles and responsibilities	6
5. Data protection principles	7
6. Collecting personal data	8
7. Sharing personal data	11
8. Subject access requests and other rights of individuals	12
9. Parental requests to see the educational record	137
10. CCTV	17
11. Photographs and videos	138
12. Data protection by design and default	18
13. Data security and storage of records	19
14. Disposal of records.	20
15. Personal data breaches.	20
16. Training	20
17. Direct Marketing	21
18. Monitoring arrangements	21
19. Links with other policies.	21
20. Record Keeping	21

## 1. Introduction

The 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.

## 2. Definitions

Term	Definition
<b>Personal data</b>	<p>Any information relating to an identified, or identifiable, individual.</p> <p>This may include the individual's:</p> <ul style="list-style-type: none"> <li>• Name (including initials)</li> <li>• Identification number</li> <li>• Location data</li> <li>• Online identifier, such as a username</li> <li>• Date of Birth</li> </ul> <p>Or an opinion about a person's actions or behaviour.</p> <p>This may also include special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.</p>

<p><b>Special categories of personal data</b></p>	<p>Personal data which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none"> <li>• Racial or ethnic origin</li> <li>• Political opinions</li> <li>• Religious or philosophical beliefs</li> <li>• Trade union membership</li> <li>• Genetics</li> <li>• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes</li> <li>• Health – physical or mental</li> <li>• Sex life or sexual orientation</li> <li>• Criminal offences and convictions</li> </ul>
<p><b>Processing</b></p>	<p>An activity that involves the use of personal data. This includes but it not limited to: obtaining, recording or holding data or carrying out any operation or set of operations on that data such as organisation, amending, retrieving using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties</p>
<p><b>Automated Processing</b></p>	<p>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.</p> <p>An example of automated processing includes profiling and automated decision making.</p> <p>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</p>

	is prohibited except in exceptional circumstances.
<b>Data subject</b>	The identified or identifiable individual whose personal data is held or processed.
<b>Data controller</b>	A person or organisation that determines the purposes and the means of processing of personal data.
<b>Data processor</b>	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
<b>Personal data breach</b>	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
<b>Data Protection Impact Assessment (DPIAs)</b>	DPIAs are a tool used to identify risks in data processing activities with a view to reducing them.

### 3. The Data Controller

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

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

### 4. Roles and responsibilities

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

#### 4.1 Governing board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

#### 4.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

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](mailto:dataservices@judicium.com)

Web: [www.judiciumeducation.co.uk](http://www.judiciumeducation.co.uk)

Telephone: 0203 326 9174

Lead Contact: Craig Stilwell

### **4.3 Headteacher**

The Headteacher acts as the representative of the data controller on a day-to-day basis.

### **4.4 All staff**

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  - If they have any concerns that this policy is not being followed
  - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
  - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
  - If there has been a data breach
  - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
  - If they need help with any contracts or sharing personal data with third parties

## **5. Data protection principles**

The UK GDPR is based on data protection principles that our school must adhere to.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

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

## 6. Collecting personal data

### 6.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest**, and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal 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);
- 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 is necessary for archiving, statistical or research purposes.

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

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

## **6.2 Purpose limitation**

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).

## **6.3 Data minimisation**

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 staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's Record management policy and Retention Disposal of Records Schedule.

## **6.4 Accuracy**

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.

## **6.5 Storage Limitation**

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.

## **6.6 Integrity and confidentiality**

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.

Full details on the School's security measures are set out in the School's Security Policy

## 7. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/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
- 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 which can provide sufficient guarantees that they comply with data protection law
  - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, 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, and information necessary to keep them safe while working with us

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

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

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.

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.

### 7.1 Transfer of Data Outside the European Economic Area (EEA)

The UK GDPR restricts data transfers to countries outside the EEA 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 EEA 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 EEA. 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

## **8. Subject access requests and other rights of individuals**

### **8.1 Subject access requests**

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 is not possible, the criteria used to determine this period
- 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

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, WhatsApp 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.

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.

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

All data subject access requests should be immediately directed to the School Bursar who should contact Judicium as DPO in order to assist with the request and what is required.

### **8.2 Children and subject access requests**

The school need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney. The School may also require proof of identity in certain circumstances.

When requests are made on behalf of children, it is important to note that even if a child is too young to understand the implications of subject access rights, it is still the right of the child,

rather than of anyone else such as a parent or guardian, to have access to the child's personal data. Before responding to a SAR for information held about a child, the School should consider whether the child is mature enough to understand their rights. If the school is confident that the child can understand their rights, then the School should usually respond directly to the child or seek their consent before releasing their information.

It shall be assessed if the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, it should be taken into account, among other things:

- the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

Generally, a person aged 12 years or over is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown. In relation to a child 12 years of age or older, then provided that the School is confident that they understand their rights, and there is no reason to believe that the child does not have the capacity to make a request on their own behalf, the School will require the written authorisation of the child before responding to the requester, or provide the personal data directly to the child.

The School may also refuse to provide information to parents if there are consequences of allowing access to the child's information – for example if it is likely to cause detriment to the child.

### **8.3 Responding to subject access requests**

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- 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

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

## **8.4 School closure periods**

Requests received during school closure periods may not be able to be responded to within the one calendar month response period. This is because there will be no one on site to comply with the request. As a result, it is unlikely that your request will be able to be dealt with during this time. We may also 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. During school closure periods it is highly likely that the school will need to utilise some or all of the permitted 2 month's extension from receipt of the request, where a request is complex or numerous. 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.

## **8.5 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 individuals' 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.

## **8.6 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.

## **8.7 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 School's processing activities;
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a 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)

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.

## **9. Parental requests to see the educational record**

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

## **10. CCTV**

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's [code of practice](#) for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to Luke Norrie-Rolfe, Caretaker.

## **11. Photographs and videos**

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

See our child protection and safeguarding policy for more information on our use of photographs and videos.

## **12. Data protection by design and default**

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing data protection impact assessments (DPIAs) where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices

- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
  - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
  - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

### **13. Data security and storage of records**

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our e-safety policy and online safety policy)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

### **14. Disposal of records**

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

### **15. Personal data breaches**

The school will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

## **16. Training**

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

## **17. 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.**

## **18. Monitoring arrangements**

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary. Otherwise this policy will be reviewed **every 2 years** and shared with the full governing board.

## **19. Links with other policies**

This data protection policy is linked to our:

- Freedom of information publication scheme
- Online Safety Policy
- Child Protection and Safeguarding policy

## **20. 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.

# Appendix 1: Personal data breach procedure

## What Is A Personal Data Breach?

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

Examples of a data breach could include the following (but are not exhaustive): -

- Loss or theft of data or equipment on which data is stored, for example loss of a laptop or a paper file (this includes accidental loss);
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human error (for example sending an email or SMS to the wrong recipient);
- Unforeseen circumstances such as a fire or flood;
- Hacking, phishing and other “blagging” attacks where information is obtained by deceiving whoever holds it.

## When Does It Need To Be Reported?

The School must notify the ICO of a data breach where it is likely to result in a risk to the rights and freedoms of individuals. This means that the breach needs to be more than just losing personal data and if unaddressed the breach is likely to have a significant detrimental effect on individuals.

Examples of where the breach may have a significant effect includes: -

- potential or actual discrimination;
- potential or actual financial loss;
- potential or actual loss of confidentiality;
- risk to physical safety or reputation;
- exposure to identity theft (for example through the release of non-public identifiers such as passport details);
- the exposure of the private aspect of a person’s life becoming known by others.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, then the individuals must also be notified directly.

## Reporting A Data Breach

If you know or suspect a personal data breach has occurred or may occur which meets the criteria above, you should: -

- Complete a data breach report form (which can be obtained from Tracy Mullins);
- Email the completed form to Cathy Bell.

Where appropriate, you should liaise with your line manager about completion of the data report form. Breach reporting is encouraged throughout the School and staff and governors are expected to seek advice if they are unsure as to whether the breach should be reported and/or could result in a risk to the rights and freedom of individuals. They can seek advice from their line manager, Cathy Bell or the DPO.

Once reported, you should not take any further action in relation to the breach. In particular, you must not notify any affected individuals or regulators or investigate further. Cathy Bell will acknowledge receipt of the data breach report form and take appropriate steps to deal with the report in collaboration with the DPO.

## **Managing and Recording The Breach**

On being notified of a suspected personal data breach, Cathy Bell will notify the DPO. Collectively they will take immediate steps to establish whether a personal data breach has in fact occurred. If so they will take steps to:

- Where possible, contain the data breach;
- As far as possible, recover, rectify or delete the data that has been lost, damaged or disclosed;
- Assess and record the breach in the School's data breach register;
- Notify the ICO;
- Notify data subjects affected by the breach;
- Notify other appropriate parties to the breach;
- Take steps to prevent future breaches.

## **Notifying the ICO**

Cathy Bell will notify the ICO when a personal data breach has occurred which is likely to result in a risk to the rights and freedoms of individuals.

This will be done without undue delay and, where possible, within 72 hours of becoming aware of the breach. The 72 hour's deadline is applicable regardless of school holidays (I.e. it is not 72 working hours). If the School are unsure of whether to report a breach, the assumption will be to report it.

Where the notification is not made within 72 hours of becoming aware of the breach, written reasons will be recorded as to why there was a delay in referring the matter to the ICO.

## **Notifying Data Subjects**

Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, Cathy Bell will notify the affected individuals without undue delay including the name and contact details of the DPO and ICO, the likely consequences of the data breach and the measures the School have (or intended) to take to address the breach.

When determining whether it is necessary to notify individuals directly of the breach, Cathy Bell will co-operate with and seek guidance from the DPO, the ICO and any other relevant authorities (such as the police).

If it would involve disproportionate effort to notify the data subjects directly (for example, by not having contact details of the affected individual) then the School will consider alternative means to make those affected aware (for example by making a statement on the School website).

### **Notifying Other Authorities**

The School will need to consider whether other parties need to be notified of the breach. For example: -

- Insurers;
- Parents;
- Third parties (for example when they are also affected by the breach);
- Local authority;
- The police (for example if the breach involved theft of equipment or data).

This list is non-exhaustive.

### **Assessing The Breach**

Once initial reporting procedures have been carried out, the School will carry out all necessary investigations into the breach.

The School will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data. We will identify ways to recover correct or delete data (for example notifying our insurers or the police if the breach involves stolen hardware or data).

Having dealt with containing the breach, the School will consider the risks associated with the breach. These factors will help determine whether further steps need to be taken (for example notifying the ICO and/or data subjects as set out above). These factors include: -

- What type of data is involved and how sensitive it is;
- The volume of data affected;
- Who is affected by the breach (i.e. the categories and number of people involved);
- The likely consequences of the breach on affected data subjects following containment and whether further issues are likely to materialise;
- Are there any protections in place to secure the data (for example, encryption, password protection, pseudonymisation);
- What has happened to the data;
- What could the data tell a third party about the data subject;
- What are the likely consequences of the personal data breach on the school; and
- Any other wider consequences which may be applicable.

### **Preventing Future Breaches**

Once the data breach has been dealt with, the School will consider its security processes with the aim of preventing further breaches. In order to do this, we will: -

- Establish what security measures were in place when the breach occurred;
- Assess whether technical or organisational measures can be implemented to prevent the breach happening again;
- Consider whether there is adequate staff and governor awareness of security issues and look to fill any gaps through training or tailored advice;
- Consider whether it is necessary to conduct a privacy or data protection impact assessment;
- Consider whether further audits or data protection steps need to be taken;
- To update the data breach register;
- To debrief governors/management following the investigation.

### **Reporting Data Protection Concerns**

Prevention is always better than dealing with data protection as an after-thought. Data security concerns may arise at any time and we would encourage you to report any concerns (even if they don't meet the criteria of a data breach) that you may have to Cathy Bell or the DPO. This can help capture risks as they emerge, protect the School from data breaches and keep our processes up to date and effective.

### **Monitoring**

We will monitor the effectiveness of this and all of our policies and procedures and conduct a full review and update as appropriate.

Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to the School.

At Dorchester Primary School we aim to use the best value principles to ensure the budget is spent wisely to meet the needs of the school, pupils and staff.

- Termly comparisons are made using the DfE bench marking data to analyse expenditure against other schools in similar families.
- On line reports are used to analyse and generate challenging questions in order to target improvement.
- Self evaluation and a rigorous monitoring policy ensure areas of improvement are identified and priorities for the use of the school resources are determined in the School Improvement Plan.
- Curriculum action plans are evaluated annually and proposals are made to ensure that each child is making progress and high standards are maintained.
- National and local priorities are considered carefully and resources allocated appropriately to meet future demands.

- The projection of pupil numbers and income is completed annually for a three-year cycle and continuously monitored.
- Opportunities for generating income are considered carefully. A balance between the time, effort and the income to be gained is analysed, before embarking on a new project.
- Curriculum development plans, staffing plans and premises plans are drawn up annually and costed. These are used to allocate sufficient funds to appropriate areas for development.
- Up to three scenarios are offered to the Governors' Resources Committee for consideration before taking a major change or course of action.
- Staff, governors, parents, and sometimes pupils are consulted on proposals which will make a significant change.
- The Senior Leadership Team and staff regularly discuss proposals to meet the needs of the children and aims of the school.
- The allocation of funds is carefully monitored by the Bursar, Headteacher and Governors.
- All services purchased are evaluated annually by the Headteacher and recommendations are put forward to the Governors.
- At least three quotes are obtained from competitive providers before agreeing or extending a contract.
- Levels of staffing are monitored carefully to ensure good value for money in order to raise standards and meet the children's needs. The roles and responsibilities of all staff are reviewed annually against job descriptions to ensure an efficient service is maintained.
- A training budget for all staff is a high priority to meet the needs of the school and individuals as well as new national initiatives. Costs are identified in the Staff Development Plan.
- All curricular areas are allocated some funds for the co-ordinator to purchase resources to meet their School Improvement Plan action plan.
- The school has a clear monitoring and evaluation policy which includes the monitoring of the financial status and use of resources on a regular basis.

- The cost effectiveness of the budget and allocated funds is evaluated by analysing standards, the progress of the children and the impact on the children's learning by the Senior Leadership Team, Staff and Governors.
- The school is continually striving to improve the efficiency and effective use of all resources.