



**BURTON  
BOROUGH  
SCHOOL**

## **DATA PROTECTION POLICY**

<b>Policy Reviewer</b>	Sarah McElduff	<b>Date of Review</b>	May 2018
<b>Date Presented to Governors</b>		<b>Date of Next Review</b>	May 2020

**This page intentionally left blank**

## Contents

<b>1. Aims</b>	<b>3</b>
<b>2. Legislation and Guidance</b>	<b>3</b>
<b>3. Definitions</b>	<b>4</b>
<b>4. The Data Controller</b>	<b>5</b>
<b>5. Roles and Responsibilities</b>	<b>5</b>
<b>6. Data Protection Principles</b>	<b>6</b>
<b>7. Collecting Personal Data</b>	<b>6</b>
<b>8. Subject Access Requests and Other Rights of Individuals</b>	<b>6</b>
<b>9. Accuracy and Relevance</b>	<b>7</b>
<b>10. Data Protection by Design and Default</b>	<b>7</b>
<b>11. Data Security and Storage of Records</b>	<b>7</b>
<b>12. Disposal of Records</b>	<b>8</b>
<b>13. Personal Data Breaches</b>	<b>8</b>
<b>14. Training</b>	<b>8</b>
<b>15. Monitoring Arrangements</b>	<b>8</b>
<b>16. Links with Other Policies</b>	<b>9</b>
<b>Appendix 1: Personal Data Breach Procedure</b>	<b>10</b>

.....

### **1. Aims**

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the [General Data Protection Regulation \(GDPR\)](#) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the [Data Protection Bill](#).

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

### **2. Legislation and Guidance**

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the [GDPR](#) and the ICO's [code of practice for subject access requests](#).

It also reflects the ICO's [code of practice](#) for the use of surveillance cameras and personal information. In addition, this policy complies with regulation 5 of the [Education \(Pupil Information\) \(England\) Regulations 2005](#), which gives parents the right of access to their child's educational record.

### 3. Definitions

Term	Definition
<p><b>Personal data</b></p>	<p>Any information relating to an identified, or identifiable, living 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 or pseudonymous data</li> </ul> <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.</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> </ul>
<p><b>Processing</b></p>	<p>Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.</p> <p>Processing can be automated or manual.</p>
<p><b>Data subject</b></p>	<p>The identified or identifiable individual whose personal data is held or processed.</p>
<p><b>Data controller</b></p>	<p>A person or organisation that determines the purposes and the means of processing of personal data.</p>
<p><b>Data processor</b></p>	<p>A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.</p>
<p><b>Personal data breach</b></p>	<p>A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.</p>

## 4. 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.

## 5. Roles and Responsibilities

Access and use of personal information held by the Council, is only permitted by employees (temporary or permanent), Members, contractors, agents and anyone else processing information on our behalf, for the purpose of carrying out their official duties. Use or access for any other purpose is not allowed unless the law requires it. Deliberate unauthorised use and access to copying, destruction or alteration of or interference with any personal information is strictly forbidden.

### 5.1 Governing board

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

### 5.2 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.

Our DPO is Rob Montgomery, Audit & Governance Team Leader, Telford & Wrekin Council and is contactable via email: [robert.montgomery@telford.gov.uk](mailto:robert.montgomery@telford.gov.uk).

### 5.3 Principal

The principal (or their named delegated individual) acts as the representative of the data controller on a day-to-day basis.

### 5.4 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

Any deliberate breach of this policy could amount to a criminal offence under one or more pieces of legislation, for example the Computer Misuse Act 1990 and the GDPR. All breaches will be investigated and appropriate action taken.

## 6. Data Protection Principles

The GDPR is based on data protection principles that our school must comply with. 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. If any school employee receives such a request on any of the above matters, they should seek advice immediately.

## 7. Lawful Basis for Processing

We collect and use pupil information under GDPR article 6(1) (e) where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

For special categories of personal data, we will also meet the special category conditions for processing under GDPR article 9(2) (g) where processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

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 where the pupil is under 13 (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

## 8. Disclosing Personal Information

Personal information must not be given to anyone internally or externally, unless the person giving the information is fully satisfied that the enquirer or recipient is authorised in all respects and is legally entitled to the information.

If personal information is given to another organisation or person outside of the school, the disclosing person must identify the lawful basis for the disclosure and record their reasoning for using this basis. This record as a minimum should include;

- A description of the information given;
- The name of the person and organisation the information was given to;
- The date;
- The reason for the information being given; and
- The lawful basis.

If an information sharing agreement or protocol exists, this should be adhered to when providing personal information to others. The agreement/protocol will provide the legal basis for disclosure.

In response to any lawful request, only the minimum amount of personal information should be given. The person giving the information should make sure that the information is adequate for the purpose, relevant and not excessive.

When personal information is given either externally or internally, it must be communicated in a secure manner. For external communications use an encrypted file, special delivery or courier, etc. For internal communications either hand deliver or make sure you email the information to the correct recipient.

## 9. Accuracy and Relevance

It is the responsibility of those who receive personal information to make sure so far as is possible, that it is accurate and up to date. Personal information should be checked at regular intervals, to make sure that it is still accurate and up to date. If the information is found to be inaccurate, steps must be taken to put it right. Individuals who input or update information must also make sure that it is adequate, relevant, clear and professionally worded.

'Data subjects' have a right to access personal information held about them and have errors corrected. More information about a 'data subject's' rights can be found in Section 9 of this policy.

## 10. 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 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

## 11. 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 staff handbook / acceptable use 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)

## 12. Disposal of Records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate, where we cannot or do not need to rectify or update it or it is out of date it will also be disposed of securely. Records will be kept in line with legal requirements and guidance from the Information and Records Management Society.

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.

## 13. Personal Data Breaches

The school will make all reasonable endeavour 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

## 14. Training

All staff and governors are provided with mandatory data protection training as part of their induction process, which is renewed annually.

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

## 15. Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the full governing board.



## **16. Links with Other Policies**

This data protection policy is linked to our:

- Privacy Notice
- Freedom of information publication scheme
- Data collection forms
- Home / school agreement
- Media agreement
- Staff handbook / acceptable use policy
- Records management policy
- CCTV policy

## Appendix 1: Personal Data Breach Procedure

This procedure is based on [guidance on personal data breaches](#) produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO.
- 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
- The DPO will alert the principal and the chair of governors.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out 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.
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
  - Loss of control over their data
  - Discrimination
  - Identify theft or fraud
  - Financial loss
  - Unauthorised reversal of pseudonymisation (for example, key-coding)
  - Damage to reputation
  - Loss of confidentiality
  - Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school computer system in a secure manner.
- Where the ICO must be notified, the DPO will do this via the ['report a breach' page of the ICO website](#) within 72 hours. 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. 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.

- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  - 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 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 computer system in a secure manner.

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

### **A3.1 Actions to Minimise the Impact of Data Breaches**

We will take appropriate action to mitigate the impact of different types of data breach, 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.