



# **Blatchington Mill School**

## **DATA PROTECTION POLICY**

Date Policy Created: 22 October 2018

Date of last amendment: March 2026

Date to be reviewed: March 2027



## **Contents**

<b>1. Aims</b>	<b>2</b>
<b>2. Legislation and guidance</b>	<b>3</b>
<b>3. Definitions</b>	<b>3</b>
<b>4. The data controller</b>	<b>4</b>
<b>5. Roles and responsibilities</b>	<b>5</b>
5.1 Governing board	5
5.1 Data Protection officer (DPO)	5
5.3 Headteacher	5
5.4 All staff	5
<b>6. Data protection principles</b>	<b>6</b>
<b>7. Collecting personal data</b>	<b>6</b>
7.1 Lawfulness, fairness and transparency	6
7.1.1 Lawful basis for processing data	6
7.1.2 Special category data	6
7.1.3 Criminal offence data	7
7.2 Limitation, minimisation and accuracy	7
<b>8. Sharing personal data</b>	<b>8</b>
<b>9. Subject access and other rights of individuals</b>	<b>8</b>
9.1 Subject access requests	8
9.2 Children and subject access requests	9
9.3 Responding to subject access requests	9
9.4 Other data protection rights of the individual	10
<b>10. Parental requests to see the educational record</b>	<b>10</b>
<b>11. Freedom of Information requests</b>	<b>10</b>
<b>12. Requesting information from us</b>	<b>11</b>
12.1 To request information on a person	11
12.2 To request other information	11
<b>13. Biometric recognition systems</b>	<b>11</b>
<b>14. CCTV</b>	<b>12</b>
<b>15. Photographs and videos</b>	<b>12</b>
<b>16. Artificial Intelligence (AI)</b>	<b>13</b>
<b>17. Data protection by design and default</b>	<b>13</b>
<b>18. Data security and storage of records</b>	<b>14</b>
<b>19. Disposal of records</b>	<b>15</b>
<b>20. Personal data breaches</b>	<b>15</b>
<b>21. Training</b>	<b>15</b>
<b>22. Monitoring arrangements</b>	<b>15</b>
<b>23. Complaints</b>	<b>15</b>
<b>24. Links with other policies</b>	<b>16</b>
<b>25. Contact us</b>	<b>16</b>

---



<b>Appendix A - Freedom of Information</b>	<b>17</b>
<b>A.1 Publication Scheme</b>	<b>17</b>
A.1.1 Classes of information	17
A.1.2 The method by which information published under this scheme will be made available	18
A.1.3 Charges which may be made for information published under this scheme	18
A.1.4 Written requests	19
<b>A.2 Publication scheme - Information available</b>	<b>19</b>
A.2.1 Schedule of charges	22
A.2.2 Written requests	23
A.2.3 Further information	23
<b>Appendix B - Personal data breach procedure</b>	<b>24</b>
B.1 Actions to minimise the impact of data breaches	25
B.2 Measures in place to reduce the likelihood of data breaches	26



## 1. Aims

Our school aims to ensure that all personal data collected about students, staff, parents and carers, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

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:

- 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](#)
- [Freedom of Information Act 2000](#)

It is based on guidance published by the Information Commissioner’s Office (ICO) on the [UK GDPR](#) and guidance from the Department for Education (DfE) on [Generative artificial intelligence in education](#).

It meets the requirements of the [Protection of Freedoms Act 2012](#) when referring to our use of biometric data.

It also reflects the [ICO’s guidance](#) 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
<b>Personal data</b>	<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>● Date of Birth</li><li>● Address</li><li>● Identification number</li><li>● Location data</li><li>● Online identifier, such as a username</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 students, their parents and carers, staff, governors, visitors and others, and therefore is a data controller.

The school is registered as a data controller with the ICO, as legally required. Our ICO's registration reference is: Z1292305.



## **5. 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.

### **5.1 Governing board**

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

### **5.1 Data Protection officer (DPO)**

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.

Our DPO is our Business Manager and is contactable via [DataProtection@BlatchingtonMill.org.uk](mailto:DataProtection@BlatchingtonMill.org.uk) or 01273 736244 (see 'Contact us' below).

### **5.3 Headteacher**

The headteacher 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 UK
  - 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



## 6. Data protection principles

The UK 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.

## 7. Collecting personal data

### 7.1 Lawfulness, fairness and transparency

#### 7.1.1 Lawful basis for processing data

We will only process personal data where we have one of six 'lawful bases' (legal reasons) to do so under data protection law, as set out in [Article 6 of the UK GDPR](#):

- 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 exercise its official functions
- The data needs to be **processed for the legitimate interests** of the school (where the processing is not for any tasks the school performs as a public authority) 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 student) has freely **given clear consent**

#### 7.1.2 Special category data

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law, as set out in [Article 9 of UK GDPR](#):

- The individual (or their parent/carer when appropriate in the case of a student) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**



- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise or defence of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

### **7.1.3 Criminal offence data**

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law, as set out in [Article 10 of UK GDPR](#). Conditions include:

- The individual (or their parent/carer when appropriate in the case of a student) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

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

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

## **7.2 Limitation, minimisation and accuracy**

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will either ensure that the reasons are compatible with the original purpose or we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.



In addition, 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 Information and Records Management Society's toolkit for schools.

## **8. Sharing personal data**

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a student or parent/carer that puts the safety of any member of our school community 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 students (e.g., IT companies). When doing this, we will:
  - Only appoint suppliers or contractors which 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, 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.

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 students or staff.

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

## **9. Subject access and other rights of individuals**

### **9.1 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. The subject access right includes:

- Confirmation that their personal data is being processed
- The purposes of the data processing
- Access to a copy of the data

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

- Name of individual
- Correspondence address and/or contact number and email address



- Specific details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO; ideally, using the email address [DataProtection@BlatchingtonMill.org.uk](mailto:DataProtection@BlatchingtonMill.org.uk).

## **9.2 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 aged 12 and above are generally 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 students at our school may not be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

## **9.3 Responding to subject access requests**

When responding to requests, we:

- May ask the individual to provide two forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within one month of receipt of the request (or receipt of additional information needed, where relevant)
- Will perform reasonable and proportionate searches of our systems
- Will provide the information free of charge
- May tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within one month, and explain why the extension is necessary

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 student 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 consider 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 using our formal complaint procedures and then directly to the ICO, or they can seek to enforce their subject access right through the courts.



#### **9.4 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 certain processing at any time
- 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 data breach (in certain circumstances)
- Make a complaint to us in the first instance and then 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. Please contact us (see 'Contact Us' section below). If staff receive such a request, they must immediately forward it to the DPO.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain using our formal complaint procedures and then directly to the ICO or they can seek to enforce their individual right through the courts.

### **10. 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 student) within 15 school days of receipt of a written request.

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it.

This right applies as long as the student concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the student or another individual, or if it would mean releasing exam marks before they are officially announced.

### **11. Freedom of Information requests**

You have a right to request information (other than personal information) under the Freedom of Information Act. The main principle behind freedom of information legislation is that people have a right to know about the activities of public authorities, unless there is a good reason for them not to. As a local authority school, we must give public access to certain recorded information that we hold.

If you require further information on this right, please see the [ICO's guidance and resources](#).

---



We will endeavour to respond to your request promptly and within the regulation deadline of 20 school days or 60 working days – whichever is sooner. This timeline starts from the first working day after your submission, unless further clarification on your request is required. In those cases, time starts from the first working day after clarification is received to us.

Requests must be made in written format, but can be in either paper or electronic. If you would like to make a request, please contact us (see 'Contact us' below). You are not obliged to provide us with anything more than your name, contact details and the information you are requesting. However, if you are specific about what you are requesting, and provide us with a telephone number or email address, it may help us to process your request more efficiently and respond quicker. The information you supply will only be used for the purposes of identifying the information you are requesting and for responding to your request.

Please see Appendix A for the Blatchington Mill School Freedom of Information Publication Scheme

## **12. Requesting information from us**

To make any request for information, please see the 'Contact us' section below for contact details.

### **12.1 To request information on a person**

When deciding whether to submit a 'subject access request' (SAR) or a request to view the Educational Record, it is worth considering what information you wish to obtain.

- If you submit a SAR for you or your child's personal data, it is likely to disclose information contained in the educational record (if regarding a student) as well as any other personal data we may hold. If you are requesting on behalf of a child, we may require their consent.
- If you submit a request to view or receive a copy of your or your child's educational record, we will only disclose the information contained in the educational record and we are not obliged to disclose any further personal data that we may hold. If the request is for your child, we do not need their consent.

### **12.2 To request other information**

If you are requesting information that does not include personal information, then you will need to submit, in writing, a request under the Freedom of Information Act. Please email [DataProtection@BlatchingtonMill.org.uk](mailto:DataProtection@BlatchingtonMill.org.uk) to submit a Freedom of Information request or see the 'Contact us' section below for other contact detail information.

## **13. Biometric recognition systems**

*Note that in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18.*

Where we use students' biometric data as part of an automated biometric recognition system (e.g., students use fingerprints to access their catering account), we will comply with the requirements of the [Protection of Freedoms Act 2012](#).



Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will obtain written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and students have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those students. For example, students can be looked up on the till system by giving their name, if they wish.

Parents/carers and students can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a student refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the student's family.

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

## **14. CCTV**

We use CCTV (closed-circuit television) in various locations around the school site to ensure safety and security. We will adhere to the [ICO's guidance](#) for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear CCTV is used around the school. Cameras are located:

- Outside, on school grounds, including car parks and building access points
- Inside school, including corridors and open spaces
- At site access gates

Any enquiries about the CCTV system should be directed to the DPO (please see 'Contact us' section below).

## **15. Photographs and videos**

There are certain circumstances where we will obtain written consent from parents/carers for photographs and videos to be taken of students. For example, as part of our school activities, we may take photographs and record images of individuals within our school and use them for communication, marketing and promotional materials.

Before taking these types of photographs or videos, we ask students for their consent, giving them the opportunity to object before a photograph is taken.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carers and student.

Uses where we request consent 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. Please note that it may not be possible to completely remove images published historically on the internet.

When using photographs and videos in this way, we only disclose a child's first name.

See our Online Safeguarding policy for more information on our use of photographs and videos.

There are some circumstances where consent is not required for us to take students' photographs. We will clearly explain how the photograph will be used. An example of where we do not require consent is identification photos for our management information system.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. In order to support the need for informed consent we ask families attending events such as performances and sports fixtures, not to take photographs as they may include images of students for whom we do not have consent.

## **16. Artificial Intelligence (AI)**

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, students and parents/carers may be familiar with generative chatbots such as ChatGPT and Google's Gemini. Blatchington Mill School recognises that AI has many uses to help students 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, Blatchington Mill School will treat this as a data breach, and will follow the personal data breach procedure outlined in Appendix B.

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

We 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)
  - Taking children's needs into account when deciding how to use their personal information
-



- 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
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply.
- 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, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure

## **18. 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 staff room 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 out and in from the school office or seek specific authorisation from a member of the senior leadership team (SLT) (e.g., when taking contact details and emergency information on a school trip)
- Passwords that meet a rigorous level of security are used to access school computers, laptops and other electronic devices. Staff and students are reminded that they should not reuse passwords from other sites and 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 that may contain sensitive data
- Staff, students or governors are deterred from storing personal information on their personal devices; in exceptional cases when this is necessary, they are expected to follow the same security procedures as for school-owned equipment (see our Online Safeguarding 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)



## **19. 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.

## **20. 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 B.

When appropriate, we will report the data breach to the ICO within 72 hours of becoming aware of it.

## **21. 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.

## **22. Monitoring arrangements**

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and shared with the full governing board.

## **23. Complaints**

We take any complaints about our collection and use of 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 let the data protection team know in the first instance. If you wish to make a formal complaint, you should follow the procedures outlined in our complaints policy.

If your complaint is not resolved to your satisfaction within a reasonable timeframe, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/make-a-complaint/>
- Call 0303 123 1113



- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

## 24. Links with other policies

This data protection policy is linked to our:

- [Child Protection and Safeguarding Policy](#)
- [Online Safeguarding Policy](#)
- [Privacy Notices for staff, students, staff, visitors and volunteers](#)
- [Complaints Policy & Procedure](#)

## 25. Contact us

If you have any questions or concerns, or would like more information about anything mentioned in this data protection policy, please contact our **data protection officer**:

Data Protection Officer & Business Manager  
[DataProtection@BlatchingtonMill.org.uk](mailto:DataProtection@BlatchingtonMill.org.uk)  
01273 736244  
Blatchington Mill School  
Nevill Avenue  
BN3 7BW



## Appendix A - Freedom of Information

### A.1 Publication Scheme

This publication scheme is based on, but has been adapted from, the model scheme published by the [Information Commissioner's Office](#).

This publication scheme commits Blatchington Mill School to make information, required by law, available to the public as part of its normal business activities. The information covered is included in the classes of information mentioned below, where this information is held by Blatchington Mill. Additional assistance is provided to the definition of these classes in sector specific guidance manuals issued by the Information Commissioner.

The scheme commits Blatchington Mill School:

- To proactively publish or otherwise make available as a matter of routine, information, including environmental information, which is held by the school and falls within the classifications below.
- To specify the information which is held by the school and falls within the classifications below.
- To proactively publish or otherwise make available as a matter of routine, information in line with the statements contained within this scheme.
- To produce and publish the methods by which the specific information is made routinely available so that it can be easily identified and accessed by members of the public.
- To review and update on a regular basis the information the school makes available under this scheme.
- To produce a schedule of any fees charged for access to information which is made proactively available.
- To make this publication scheme available to the public.
- To publish any dataset held by Blatchington Mill School that has been requested, and any updated versions it holds, unless the school is satisfied that it is not appropriate to do so; to publish the dataset, where reasonably practicable, in an electronic form that is capable of re-use; and, if any information in the dataset is a relevant copyright work and the school is the only owner, to make the information available for re-use under the terms of the Re-use of Public Sector Information Regulations 2015, if they apply, and otherwise under the terms of the Freedom of Information Act section 19.

The term 'dataset' is defined in section 11(5) of the Freedom of Information Act. The term 'relevant copyright work' is defined in section 19(8) of that Act.

#### A.1.1 Classes of information

- **Who we are and what we do.**  
Organisational information, locations and contacts, constitutional and legal governance.
- **What we spend and how we spend it.**  
Financial information relating to projected and actual income and expenditure, tendering, procurement and contracts.
- **What our priorities are and how we are doing.**  
Strategy and performance information, plans, assessments, inspections and reviews.
- **How we make decisions.**



Policy proposals and decisions. Decision making processes, internal criteria and procedures, consultations.

- **Our policies and procedures.**

Current written protocols for delivering our functions and responsibilities.

- **Lists and registers.**

Information held in registers required by law and other lists and registers relating to the functions of the school.

- **The services we offer.**

Advice and guidance, booklets and leaflets, transactions and media releases. A description of the services offered.

The classes of information will not generally include:

- Information the disclosure of which is prevented by law, or exempt under the Freedom of Information Act, or is otherwise properly considered to be protected from disclosure.
- Information in draft form.
- Information that is no longer readily available as it is contained in files that have been placed in archive storage, or is difficult to access for similar reasons.

### **A.1.2 The method by which information published under this scheme will be made available**

The school will indicate clearly to the public what information is covered by this scheme and how it can be obtained.

Where it is within the capability of Blatchington Mill School, information will be provided on our website. Where it is impracticable to make information available on our website or when an individual does not wish to access the information by the website, we will indicate how information can be obtained by other means and provide it by those means.

In exceptional circumstances some information may be available only by viewing in person. Where this manner is specified, contact details will be provided. An appointment to view the information will be arranged within a reasonable timescale.

Information will be provided in the language in which it is held or in such other language that is legally required. Where the school is legally required to translate any information, it will do so.

Obligations under disability and discrimination legislation and any other legislation to provide information in other forms and formats will be adhered to when providing information in accordance with this scheme.

### **A.1.3 Charges which may be made for information published under this scheme**

The purpose of this scheme is to make the maximum amount of information readily available at minimum inconvenience and cost to the public. Charges made for routinely published material will be justified and transparent and kept to a minimum.

Material which is published and accessed on a website will be provided free of charge. Charges may be made for information subject to a charging regime specified by Parliament. Charges may be made for actual disbursements incurred such as:



- photocopying
- postage and packaging and / or
- the costs directly incurred as a result of viewing information

Charges may also be made for information provided under this scheme where they are legally authorised, they are in all the circumstances, including the general principles of the right of access to information held by public authorities, justified and are in accordance with a published schedule or schedules of fees which is readily available to the public.

Charges may also be made for making datasets (or parts of datasets) that are relevant copyright works available for re-use. These charges will be in accordance with the terms of the Re-use of Public Sector Information Regulations 2015, where they apply, or with regulations made under section 11B of the Freedom of Information Act, or our other statutory powers.

If a charge is to be made, confirmation of the payment due will be given before the information is provided. Payment may be requested prior to provision of the information.

[Version 1.2](#)

#### **A.1.4 Written requests**

Information held by Blatchington Mill School that is not published under this scheme can be requested in writing, when its provision will be considered in accordance with the provisions of the Freedom of Information Act.

### **A.2 Publication scheme - Information available**

Guide to information available from Blatchington Mill School under the publication scheme, as per [guidance](#) provided by the ICO. See A.2.3 for contact details to request a copy of any of the below documents.

<b>Information to be published</b>	<b>How you can obtain the information</b>
	Hard copy upon request or available on the website
<b>Class one: Who we are and what we do</b> Organisational information, structures, locations and contacts	
Instrument of government	<a href="#">Our Vision/Governors</a>
School prospectus and curriculum	<a href="#">For Families/Information for Prospective Families</a>
Governing board - including: Names, contact details and the basis on which they have been appointed	<a href="#">Our Vision/Governors</a>
Information about and duties of the governors	<a href="#">Our Vision/Governors</a>
Gender pay gap reporting	<a href="#">Brighton &amp; Hove City Council website</a>
School session times Term dates	<a href="#">Key Information/School Day Times</a> <a href="#">Key Information/Term Dates</a>
<b>Location and contact information</b> Name and contact details of school	<a href="#">Key Information/Contact Us</a>



Head teacher's name and contact details Who's who in the school	<a href="#">Our Vision/Headteacher's Welcome</a> An appropriately redacted version is available by request
<b>Class 2 - What we spend and how we spend it</b> Financial information about projected and actual income and expenditure, procurement, contracts and financial audit	
Annual budget and financial statements	<a href="#">DfE benchmarking website</a>
Expenditures	An appropriately redacted version is available by request
Capital funding	An appropriately redacted version is available by request
Financial audit reports	An appropriately redacted version is available by request
Procurement and contracts	An appropriately redacted version is available by request
Staff allowances and expenses	An appropriately redacted version is available by request
Staff pay and grading structures	An appropriately redacted version is available by request
Governors' allowances	An appropriately redacted version is available by request
Premiums or other forms of financial support available	<a href="#">Our Vision/Educational Disadvantage</a>
Trade Union facility time reporting	An appropriately redacted version is available by request
<b>Class 3 - What our priorities are and how we are doing</b> Strategies and plans, performance indicators, audits, inspections and reviews	
Performance data supplied to the government	<a href="#">Key Information/Exam Results</a>
Latest reports from Ofsted	<a href="#">Key Information/Ofsted</a>
Performance management information	An appropriately redacted version is available by request
Future plans	<a href="#">Our Vision/School Development Plan</a>
Exam and assessment results	<a href="#">For Students/Exams</a>
Performance tables	<a href="#">DfE Website</a>
Data Protection impact assessments	An appropriately redacted version is available by request
Other impact assessments	An appropriately redacted version is available by request
<b>Class 4 - How we make decisions</b> Decision-making processes and records of decisions	
Admissions policy and admission decisions (not individual)	<a href="#">For Families/Information for Prospective Families/Admissions</a>
Agendas and minutes of meetings of the governing body and its committees (unless an exemption applies to the information or parts of it)	<a href="#">Our Vision/Governors</a>



<p><b>Class 5 - Our policies and procedures</b> Current written protocols, policies and procedures for delivering our services and responsibilities</p>	
<p><b>School policies and other documents</b> (this list is not exhaustive) Accessibility plan Anti-bullying policy School Behaviour - behaviour principles written statement Special education needs and disability Home-school agreement document Premises management documents  Relationships and sex education</p>	<p><a href="#">Our Policies/Policies</a> <a href="#">Our Policies/Policies</a> <a href="#">Our Policies/Policies</a> <a href="#">Our Policies/Policies</a> <a href="#">Our Policies/Policies</a> <a href="#">Our Policies/Policies</a> An appropriately redacted version is available by request <a href="#">Our Policies/Policies</a></p>
<p><b>Records management, personal data and access to information policies</b> Information security policies Data privacy notices Data protection policy - including:     Records retention     Destruction and archive policies     Data sharing     CCTV usage     Protection of biometric information of children in schools     Freedom of information     Publication scheme</p>	<p><a href="#">Our Policies/Policies</a> <a href="#">Our Policies/Privacy Policies</a> <a href="#">Our Policies/Policies</a></p>
<p><b>Equality and Diversity</b> Equality information and objectives Equality policy</p>	<p><a href="#">Our Vision/Equalities</a> <a href="#">Our Policies/Policies</a></p>
<p><b>Safeguarding and child protection</b> Child protection policy and procedures</p>	<p><a href="#">Our Policies/Policies</a></p>
<p><b>Pay policy</b> Teachers' pay</p>	<p>An appropriately redacted version is available by request</p>
<p><b>Health and safety</b> Health and Safety policy - including:     First aid in school</p>	<p><a href="#">Our Policies/Policies</a></p>
<p><b>Policies and procedures for human resources and the recruitment of staff</b> Teacher appraisal procedures Central record of recruitment and vetting checks Capability of staff Staff discipline, conduct and grievance (procedures for addressing) Early career teachers (ECTs) Statement of procedures for dealing with allegations of abuse against staff</p>	<p>Appropriately redacted versions of these may be available by request</p>
<p><b>Careers programme information</b> Careers guidance: details of careers programme</p>	<p><a href="#">Our Vision/Careers</a></p>



Provider access statement	
<b>Complaints procedures, including for dealing with parental complaints</b> Complaints policy	<a href="#">Our Policies/Policies</a>
<b>Charging regimes and policies</b> Charging and Remissions	<a href="#">Our Policies/Policies</a>
<b>Class 6 - Lists and Registers</b>	<b>(hard copy or website; some information may only be available by inspection)</b>
Curriculum circulars and statutory instruments	Hard copy, or otherwise, upon request
CCTV - Notification of use of CCTV onsite	Notices at entrances, hard copy, or otherwise, upon request
Disclosure logs	An appropriately redacted version is available by request
Asset register and Information Asset register	An appropriately redacted version is available by request
Any information you are currently legally required to hold in publicly available registers Register of business interests of headteachers and governors Register of students' admissions to school Register of students' attendance	Internal platform. Appropriately redacted versions may be available by request.
<b>Class 7 - The services we offer</b>	<b>(hard copy or website; some information may only be available by inspection)</b>
Extra-curricular activities	<a href="#">For Students/Extra-Curricular</a>
Out of school clubs	<a href="#">For Students/Extra-Curricular</a>
School publications	<a href="#">For Families/Latest News</a>
Services for which we are entitled to recover a fee, together with those fees	<a href="#">Our Policies/Hire Facilities</a>
Leaflets, booklets and newsletters	<a href="#">For Families/Latest News</a> or otherwise, upon request

### A.2.1 Schedule of charges

This describes how the charges have been arrived at. Charges will be advised at the time of request and payment is required prior to provision of the information.

Single copies of information covered by this publication will be provided free if marked 'hard copy' and postal charges at the time will apply. Items marked 'web' are available free of charge and should be downloaded by any interested party.

Type of charge	Description	Bases of charge
Disbursement cost	Photocopying / printing (black and white) at 10p per sheet including small admin fee	Actual cost incurred by the school
	Postage 2nd class based of weight	Actual cost of Royal Mail service



### **A.2.2 Written requests**

Information held by us that is not published under this scheme can be requested in writing, when its provision will be considered in accordance with the provisions of the Freedom of Information Act.

### **A.2.3 Further information**

If you have any questions or concerns, or would like more information about anything mentioned in this guide to the specific information we hold, please contact our **data protection officer**:

Data Protection Officer & Business Manager

[DataProtection@BlatchingtonMill.org.uk](mailto:DataProtection@BlatchingtonMill.org.uk)

01273 736244

Blatchington Mill School

Nevill Avenue

BN3 7BW



## Appendix B - 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) (please see 'Contact us' section above).
- 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 cooperate with the investigation (including allowing access to information and responding to questions).
- If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the headteacher.
- 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 the Local Authority). (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.
- 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 (e.g., 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 a document shared between the DPO and the headteacher.
- 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.

### **B.1 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.

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 undo sending 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 Network Services Team 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 endeavour 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 local safeguarding partners.

Details of pupil premium interventions for named children being published on the school website

- The information would be removed immediately and a message posted acknowledging the mistake and requesting readers not to share any information or knowledge gained.

Non-anonymised student exam results or staff pay information being shared with governors

- The information would be anonymised and previous versions would be deleted with an acknowledgement to governors along with a request not to share any information or knowledge gained.

A school laptop containing non-encrypted sensitive personal data being stolen or hacked



- The Network Services Team would block the device.

The school's cashless payment provider being hacked and parents' financial details stolen

- We only use reputable companies who have processes for protection of such data.

Hardcopy reports sent to the wrong students or families

- Contact would be made with the recipient with a request to not open the information, the school would arrange to collect the documents.

## **B.2 Measures in place to reduce the likelihood of data breaches**

- Rigorous investigation will be carried out when entering into a data sharing agreement with an organisation.
- The management information systems used by the school have a layered/modular structure meaning that staff can view only what they have the authority to. Access is restricted.
- An open and honest culture is encouraged to ensure that breaches, whether actual or possible, are reported.
- Staff are thoroughly dissuaded from using personal equipment for storage or processing of student information.
- Hard copy records of student and staff personal details are kept in secure cabinets in locked rooms.
- A secure email system is available to all staff and those who are most likely to need to share student information have training and familiarisation with that system.