



# GDPR UK & Data Protection Policy

Review Responsibility: Data Protection Co-ordinator

Frequency of Review: 1 year

Date Approved: Mar 26

Approved By: Board of Trustees

Next Review Due By: Mar 27

# Contents

<b>1. Aims</b>	<b>3</b>
<b>2. Legislation &amp; Guidance</b>	<b>3</b>
<b>3. Definitions</b>	<b>3</b>
<b>4. The Data Controller</b>	<b>4</b>
<b>5. Roles &amp; Responsibilities</b>	<b>4</b>
5.1 Governing Board	4
5.2 Data Protection Officer (DPO)	4
5.3 Headteacher	4
5.4 All Staff	4
<b>6. Data Protection Principles</b>	<b>5</b>
<b>7. Collecting Personal Data</b>	<b>5</b>
7.1 Lawfulness, Fairness and Transparency	5
7.2 Limitation, Minimisation and Accuracy	6
<b>8. Sharing Personal Data</b>	<b>6</b>
<b>9. Subject Access Requests and Other Rights of individuals</b>	<b>6</b>
9.2 Children and Subject Access Requests	7
9.3 Responding to Subject Access Requests	7
9.4 Other Data Protection Rights of the Individual	8
<b>10. Parental Requests to see the Educational Record</b>	<b>8</b>
<b>11. Biometric Recognition Systems</b>	<b>8</b>
<b>12. CCTV</b>	<b>9</b>
<b>13. Photographs and Videos</b>	<b>9</b>
<b>14. Artificial Intelligence (AI)</b>	<b>9</b>
<b>15. Data Protection by Design and Default</b>	<b>10</b>
<b>16. Data Security and Storage of Records</b>	<b>10</b>
16.1 Physical Security	10
16.2 Device & Equipment Security	11
16.3 Access Controls & Authentication	11
16.4 Encryption & Removable Media	11
16.5 Personal Devices (BYOD)	11
16.6 Data Sharing & Third Parties	11
<b>17. Disposal of Records</b>	<b>11</b>
<b>18. Personal Data Breaches</b>	<b>12</b>
<b>19. Training</b>	<b>12</b>
<b>20. Monitoring Arrangements</b>	<b>12</b>
<b>21. Links with Other Policies</b>	<b>12</b>
<b>Appendix 1: Personal Data Breach Procedure</b>	<b>12</b>
Actions to Minimise the Impact of Data Breaches	14
<b>Appendix 2 - Subject Access Request Form</b>	<b>15</b>

# 1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, 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 & 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 [European Union \(Withdrawal\) Act 2018](#)
- [Data Protection Act 2018 \(DPA 2018\)](#)

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.

# 3. Definitions

TERM	DEFINITION
<b>Personal data</b>	Any information relating to an identified, or identifiable, living individual. This may include the individual’s: <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></ul> It may also include factors specific to the individual’s physical, physiological, genetic, mental, economic, cultural or social identity.
<b>Special categories of personal data</b>	Personal data which is more sensitive and so needs more protection, including information about an individual’s: <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>
<b>Processing</b>	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
<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 personal data.

TERM	DEFINITION
<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.

## 4. The Data Controller

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

The school is registered with the ICO, as legally required.

## 5. Roles & 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.

### 5.2 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. 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 the Service Level Agreement with Cantium Solutions. Our DPO is Invicta Law and is contactable via [dpo@invicta.law](mailto:dpo@invicta.law) and our data protection co-ordinator is Kirsty Murphy [dpcoord@bordengrammar.kent.sch.uk](mailto:dpcoord@bordengrammar.kent.sch.uk)

### 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.

The UK GDPR also emphasises the importance of accountability in connection with the data protection principles, i.e. being able to demonstrate our compliance with the law.

## 7. Collecting Personal Data

### 7.1 Lawfulness, Fairness and Transparency

We will only process personal data where we have 1 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 or another person i.e. 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 or exercise its official authority**
- 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 pupil) has freely given clear **consent**

For special categories of personal data, we will also meet 1 of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) 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

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) 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 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 school's record retention schedule.

## 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 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 that can provide sufficient guarantees that they comply with UK data protection law
  - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
  - Only share data that the supplier or contractor needs to carry out their service

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

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

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

## 9. Subject Access Requests 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. This includes:

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

- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally

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

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

If staff receive a subject access request in any form they must immediately forward it to the data protection co-ordinator: [dpcoord@bordengrammar.kent.sch.uk](mailto:dpcoord@bordengrammar.kent.sch.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 pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis. Requests can be submitted using our Subject Access Request form, Appendix 2.

## 9.3 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 (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

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

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

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

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

## 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 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 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 data protection co-ordinator:

[dpcoord@bordengrammar.kent.sch.uk](mailto:dpcoord@bordengrammar.kent.sch.uk). If staff receive such a request, they must immediately forward it to the data protection co-ordinator.

## 10. Parental Requests to see the Educational Record

As an academy, there is no automatic parental right of access to the educational record of your child, however, this may be obtained by making a Subject Access Request (SAR) on your child's behalf. However, as per section 9.2 of this policy, we may require evidence of your child's authorisation to proceed with this.

## 11. Biometric Recognition Systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash, 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 get written consent from at least 1 parent or carer before we take any biometric data from their child and first process it. For children aged 13 and over, we would also require their own consent.

Parents/carers and pupils 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 pupils. For example, pupils can pay for school dinners using their name and form. The photograph we hold on the system will be used to check their identity to prevent unauthorised use of canteen accounts.

Parents/carers and pupils can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil 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 pupil's parent(s)/carer(s).

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.

## 12. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will follow the [ICO's guidance](#) for the use of CCTV, and comply with data protection principles.

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. Please see our CCTV Policy for further information.

Any enquiries about the CCTV system should be directed to [school@bordengrammar.kent.sch.uk](mailto:school@bordengrammar.kent.sch.uk)

## 13. 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, as well as consent from pupils aged 13 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials. Where we need parental/pupil consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and the pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

Where the school takes photographs and videos, 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 School Image Use Policy.

## 14. Artificial Intelligence (AI)

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

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

If personal and/or sensitive data is entered into an unauthorised generative AI tool, we will treat this as a data breach, and will follow the personal data breach procedure outlined in appendix 1. Please see our AI policy for further information.

## 15. 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
- 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, type of 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

## 16. 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.

### 16.1 Physical Security

- Paper-based records containing personal or special category data are stored securely under lock and key when not in active use.
- Confidential documents must not be left unattended on desks, in classrooms, staffrooms, or in any location where unauthorised access may occur.
- Access to areas where personal data is stored is restricted to authorised staff only.

### 16.2 Device & Equipment Security

- Portable electronic devices, including laptops, Chromebooks, and tablets that store or process personal data, are stored securely when not in use.
- All school-issued devices are configured in accordance with the school's security standards and managed by the IT team.

### 16.3 Access Controls & Authentication

- Access to school systems and devices is protected by strong passwords with a minimum length of 10 characters, including letters and numbers.
- Staff and pupils are required not to reuse school passwords for personal or external accounts.
- User access is role-based and limited to what is necessary to perform job responsibilities.

### 16.4 Encryption & Removable Media

- Full-disk encryption is applied to all portable staff devices wherever technically feasible. Chromebooks are encrypted by default, and all Windows laptops are protected using BitLocker encryption.

- Removable media is encrypted as a standard requirement. Use of removable media is kept to a minimum and is permitted only on approved devices for staff with a clearly defined and justified business need.
- Non-encrypted removable media is permitted only within the Design Technology, Art, and Examinations departments for specific purposes such as photography and media playback, where encryption is not technically possible.

### **16.5 Personal Devices (BYOD)**

- Staff, pupils, and governors who store or process personal data on personal devices are required to comply with the same security standards applied to school-owned equipment.
- This includes adherence to the Online Safety Policy, Computer Network Pupil Code of Conduct, and Acceptable Use Policy.
- Failure to comply may result in restricted access to school systems.

### **16.6 Data Sharing & Third Parties**

- Where personal data is shared with third parties, the school undertakes appropriate due diligence to ensure that the recipient provides sufficient guarantees regarding data security and compliance with UK GDPR (see Section 8).
- Data Processing Agreements (DPAs) or equivalent contractual safeguards are in place where required.

## **17. 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.

The school follows The Record Retention Schedule for Schools on the KELSI website:

<https://www.kelsi.org.uk/school-management/data-and-reporting/access-to-information/records-management>

## **18. Personal Data Breaches**

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the 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 after becoming aware of it.

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
- An email about someone being sent to an unintended recipient, and/or to someone who has no right/authority to access this personal data

## **19. 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. Data protection training will be reviewed at least every two years.

## **20. Monitoring Arrangements**

The DPO is responsible for monitoring and reviewing this policy.  
This policy will be reviewed annually and approved by the Trust Board.

## **21. Links with Other Policies**

This data protection policy is linked to our:

- Safeguarding & Child Protection Policy
- Privacy Notices
- Online Safety Policy
- Computer Network Pupil's Code of Conduct
- Acceptable Use Policy
- School Image Use Policy
- Staff Code of Conduct Policy
- CCTV Policy
- AI Policy

## Appendix 1: Personal Data Breach Procedure

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

- On finding or causing a breach or potential breach, the staff member, governor or data processor must immediately notify the data protection officer (DPO) by emailing [dpo@invicta.law](mailto:dpo@invicta.law) and the data protection co-ordinator, Kirsty Murphy, by emailing [dpocoord@bordengrammar.kent.sch.uk](mailto:dpocoord@bordengrammar.kent.sch.uk)
- The incident will be investigated and it will be determined whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
  - Lost
  - Stolen
  - Destroyed
  - Altered
  - Disclosed or made available where it should not have been
  - Made available to unauthorised people
- Staff and governors will co-operate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation
- If a breach has occurred or it is considered to be likely that is the case, the data protection co-ordinator will alert the headteacher or in their absence, the deputy headteacher
- The DPO will advise on how to make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types at the end of this procedure)
- The DPO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences
- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's [self-assessment tool](#)
- The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on GDPRIS platform which the school is registered with
- 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, either the DPO or another appropriate member of staff, 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 school's DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

- The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - Facts and cause
  - Effects
  - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on the GDPRiS platform.

- The DPO and headteacher or deputy headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible
- The DPO and headteacher will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches

### **Actions to Minimise the Impact of Data Breaches**

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

#### **Sensitive information being disclosed via email (including safeguarding records)**

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the data protection co-ordinator as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the data protection co-ordinator will ask the ICT department 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 data protection co-ordinator, with advice from 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 data protection co-ordinator will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request
- The data protection co-ordinator 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 data protection co-ordinator will inform the designated safeguarding lead and discuss whether the school should inform any or all of its local safeguarding partners

Other types of breach that you might want to consider could include:

- Details of pupil premium interventions for named children being published on the school website
- Non-anonymised pupil exam results or staff pay information being shared with governors
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- The school's cashless payment provider being hacked and parents' financial details stolen
- Hardcopy reports sent to the wrong pupils or families

## Appendix 2 - Subject Access Request Form



### SUBJECT ACCESS REQUEST (SAR)

Please complete the following form and return it to the school office or email it to:  
[dpcoord@bordengrammar.kent.sch.uk](mailto:dpcoord@bordengrammar.kent.sch.uk)

**Data Subject Details** *please include information of the child you are making a SAR for below*

Name of data subject	
Address	
Telephone	
Email address	
Date of birth	
Details of identification provided to confirm name of data subject in question	
Details of data requested - <i>please be specific to help us quickly locate the information</i>	

**Declaration to be signed by Parent/Legal Guardian and by the named Student to give consent for their data to be shared**

I hereby request that Borden Grammar School provide me with the information I have requested about the data subject above. I understand that the School has one calendar month (30 days) to respond to this request.

Parent Name: ..... Signature:.....  
Date: .....

Student Name: ..... Signature:.....  
Date: .....

---

**DPO/Co-ordinator Use**

Date request received : ..... Member of staff initials: .....  
Proof of ID checked (if appl):.....