Data Protection Policy

Owner	M Bowman & K Truesdale	
Version	9 Oct 2018 10.2.2020 15 .3.2021	V1.1 Minor amends; S3: definitions amended to align with BET V1.2 Minor formatting alterations V1.3 Closer alignment with BET DP Policy V7.1 and Model policy from solicitors Browne Jacobson 1. Statement of intent instead of Aims, 3. Definition of personal data defined as data of a living person in line with the Act; special category examples specify biometric and genetic and health matters; new definitions added 4. Data Controller named: Bourne Education Trust 5. Governors replaced with Trustees 5.2 skills and experience requirements of the DPO are stated, 7. GDPRiS platform used to record lawful basis of processing. 9.1 SAR's: Role of DPO Leads; school holidays and excessive information 9.4, Complaints to the ICO 10 Biometrics section updated 12. Photos and recordings updated 13. Live streaming and recording of lessons 14. DPIA and what is included added 14 Data security updated extensively to align with BET Policy and requirements 15. Storage of records moved from 14 to 15 16. Definition of Personal breach and biometrics added 19. Monitoring arrangements updated 20. Linked policies added
Approved FTB	V1.0 :May 2018 V1.3 :13 July 2021	
Review	May Mar 2023	

Contents

1. Statement of intent

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

The school may, from time to time, be required to share personal information about students, parent(s)/carer(s) or staff, including volunteers and governors, with other organisations, including the Local Authority, other schools and educational bodies,and various commercial organisations with whom they have contracted services.

This policy is in place to ensure all staff and governors are aware of their responsibilities andoutlines how the school complies with the following core principles of the GDPR.

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

2. Legislation and guidance

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

As the UK transitional arrangements expired on 31 December 2020, there are some practical changes for Data Protection and the GDPR. To comply with the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 please note that every policy, notice and procedural guide that refers to 'GDPR' shall now be read as 'UK GDPR'.

The rights, responsibilities and data protection that the Data Protection Act 2018 and the GDPR are not changed. Our procedures and arrangements will not change.

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 code of practice for the use of surveillance cameras and personal information.

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

3. Definitions

Term	Definition
Biometric data	Information about a person's physical or behavioural characteristics or features that can be used to identify them and is obtained or recorded for the purposes of a biometric recognition system and can include fingerprints, hand shapes, features of the eye or information about a person's voice or handwriting.
Biometric Recognition Systems	A system that operates automatically (electronically) and: • obtains or records information about a person's physical or behavioural characteristics or features; and • compares or otherwise processes that information with stored information in order to establish or verify the identity of the person or otherwise determine whether they are recognised by the system.

Data	Information which is stored electronically, on a computer, or in certain paper-based filing systems.
Data controller	The people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes.
Data minimisation	The collection, storage and use of personal data will be limited to that which is relevant, adequate and necessary for carrying out the purpose for which the data is processed
Data processors	Any person or organisation that is not a data user that processes personal data on our behalf and on our instructions.
Data Protection Officer	The person responsible for overseeing the data protection strategy and implementation to ensure compliance with GDPR requirements
Data subject	For the purpose of this policy include all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.
Data Users	Those of our workforce (including trustees and volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.
Personal data	Any information relating to an identified or identifiable living natural person (a data subject); an identifiable living natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Processing	Any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties.
Profiling	Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects, in particular to analyse or predict aspects concerning a person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements
Pseudonymisation	The process of separating personal data from direct identifiers so that identification is not possible without additional information, held separately

Sensitive personal data (Special Category Data)	• Information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data.
Transparency	Personal data will only be used for the purposes stated in this policy and the relevant Privacy Notice(s)
Workforce	Includes any individual employed by Robert May's School such as staff and those who volunteer in any capacity including trustees, members/parent helpers

4. The data controller

Our school processes personal data relating to parents/carers, students, staff, trustees, visitors and others, and therefore is a data controller.

The school has appointed the Bourne Education Trust as the registered data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to **Members, Trustees and 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 Trustee board

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

5.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to schools.

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

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

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

Our DPO is contactable via info@rmays.com.

5.4 All staff, trustees and regular visitors

are responsible for:

- Processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed

- If they are unsure whether or not they have a lawful basis to use personal data in a particular way
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The GDPR is based on data protection principles that our school must comply with.

The principles say that personal data **must be**:

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

The principles say that personal data **must not be**:

- transferred to people or organisations situated in other countries without adequate protection

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

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

Data Protection Legislation is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. For personal data to be processed fairly, data subjects must be made aware:

- that the personal data is being processed
- why the personal data is being processed
- what the lawful basis is for that processing (see below)
- whether the personal data will be shared, and if so with whom
- the period for which the personal data will be held
- the existence of the data subject's rights in relation to the processing of that personal data
- the right of the data subject to raise a complaint with the Information Commissioner's Office in relation to any processing.

The legal basis for processing data will be identified and documented within the GDPRiS platform prior to data being processed. We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

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

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

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

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.

Personal data is deleted or anonymised in accordance with the school's Record Retention Schedule, which can be found on the school's website.

8. Sharing personal data

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

- There is an issue with a student 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 students – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

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

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

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

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with 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
- 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

Subject access requests must be submitted in writing, by either letter or email to the DPO. They should include:

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

If staff receive a subject access request they must immediately forward it to the DPO Leads.

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/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 2 forms of identification
- May contact the individual via phone to confirm the request was made
  Will respond without delay and within 1 calendar month of receipt of the request.
  Should a Subject Access Request be made during a school holiday, every attempt will be made to respond within the necessary timeframe, but this cannot be guaranteed
- 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 will not disclose information if it:

- Might cause serious harm to the physical or mental health of the student or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee, which takes into account administrative costs. A request will be deemed unfounded or excessive if it is repetitive, or asks for further copies of the same information.

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

In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to and agree, where appropriate, a specific and relevant subset of the information.

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 have the right to:

- Withdraw their consent to processing at any time, where consent was originally required
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO(Information Commissioner's Office) https://ico.org.uk/
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

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

10. Biometric recognition systems

The School operates a Biometric recognition system for payment of dinner monies and for book loans from the school library).

Before we are able to obtain the biometric data of pupils or the Workforce, we are required to give notification and obtain consent for this Special Category Data due to additional requirements for processing such data under 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 obtain a card, which is topped up with cash then used to pay for food at the canteen 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 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.

11. CCTV

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

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

Any enquiries about the CCTV system should be directed to Data Protection Officer

12. Photographs and videos

As part of our school activities, we may take photographs and record images of students and individuals both in school and on school trips. We use these in the school's prospectus or other printed publications, on the school's website, on display boards around school and in educational presentations.

Photographs in the school environment, which are part of normal school life, fall under 'public task' purposes and do not require consent. We will obtain written consent from adults and parents/carers of students to take photographs or video images for the specific purposes below:

- for our school website
- school prospectus or other printed publications such as school magazines, brochures, newsletters, etc.
- to be used outside of school by external agencies such as the newspapers, on television or published in text books, research papers and education journals

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.

For any other uses outside of the school environment, we will obtain written consent e.g. consent is sought from year 11 students for photographs used for the Leavers' Yearbook.

Consent can be refused or withdrawn at any time. If consent is withdrawn for images on electronic media that the school controls, we will delete images specified by that individual and not distribute it further.

Parents and others attending School events can take photographs and videos of those events for domestic purposes. For example, parents can take video recordings of a school performance involving their child. The School does not prohibit this as a matter of policy.

The School does not however agree to any such photographs or videos being used for any other purpose, but acknowledges that such matters are, for the most part, outside of the ability of the School to prevent.

The School asks that parents and others do not post any images or videos, which include any child other than their own child on any social media or otherwise publish those images or videos.

13. Live streaming and recording of live lessons

The school uses live streaming of classrooms for virtual/online learning. Staff members will be responsible for adhering to the GDPR when teaching remotely and will ensure the confidentiality and integrity of their devices at all times. When accessing personal data for remote learning purposes, all staff members must use a school device or log on through the school network.

Sensitive data will only be transferred between devices if it is necessary to do so for the purpose of remote learning and teaching. Staff members may need to collect/and or share personal data such as phone numbers and personal email addresses as part of the remote learning system. As long as processing is necessary for the school's official functions (i.e. 'public task'), individuals will not need to give permission for this to happen,

Any data that is transferred between devices will be suitably encrypted or have other data protection measures in place so that if the data is lost, stolen, or subject to unauthorised access, it remains safe until recovered.

The School does permit staff to record live lessons for the following reasons and relies on the 'public task' lawful basis to do so;

- Help pupils catch up on missed learning
- Help deal with any concerns about inappropriate staff or pupil behaviour
- Monitor remote teaching practice to help our teachers improve and learn from others

The school will store the recordings in line with the Data Protection Policy and the video/recording should be correctly deleted after use and not stored for longer than necessary.

14. Data protection by design and data protection impact statements (DPIA)

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 privacy 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)
- The school will ensure that all DPIAs include the following information:
    - A description of the processing operations and the purposes
    - An assessment of the necessity and proportionality of the processing in relation to the purpose
    - An outline of the risks to individuals

    - The measures implemented in order to address risk
- Where a DPIA indicates high risk data processing, the school will consult the DPO who may then seek advice from the ICO as to whether the processing operation complies with the GDPR
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

15. Data security

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:

- Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access
- Confidential paper records will not be left unattended or in clear view anywhere with general access
- Personal data held in digital form is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site
- Where personal data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use
- Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted. Memory sticks and portable data storage devices will be phased out as soon as technically feasible
- All electronic devices used to store or process personal data are password-protected to protect the information on the device in case of theft
- Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft or loss
- Staff and trustees will not use their personal laptops, computers or personal email accounts for school purposes without password protection that prevents, for example, family members accessing the data
- All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password
- No sharing of passwords will take place under any circumstances. This is potentially a disciplinary matter

- Emails containing sensitive or confidential information are password-protected

- Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients

- Where personal information that could be considered private or confidential is taken off the premises, for example on a school trip, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping papers/devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data

- Before sharing data, all staff members will ensure:

    - They are allowed to share it
    - That adequate security is in place to protect it
    - The recipient of the data has been outlined in a privacy notice
- Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times, or confidential or personal data on display is covered or removed

- The physical security of the school's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place

- The school takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action

- The Data Protection Officer is responsible for ensuring continuity and recovery measures are in place to ensure the security of protected data

16. Storage and disposal of records

Data will not be kept for longer than is necessary, following the guidance of the Information and Records Management Society, in their School Toolkit: IRMS Schools Toolkit. Unrequired data will be deleted as soon as practicable.

Some educational records relating to former pupils or employees of the school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts. 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.

Paper documents will be shredded or pulped and securely disposed of, and electronic memories scrubbed clean or destroyed to ISO 27001 or equivalent, once the data should no longer be retained.

17. Personal data breaches

The term 'personal data breach' refers to a breach of security that has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

All notifiable breaches will be reported to the ICO within 72 hours of the school becoming aware of it. The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis. In the event that a breach is likely to

result in a high risk to the rights and freedoms of an individual, the school will notify those concerned directly.

Effective and robust breach detection, investigation and internal reporting procedures are in place at each school, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified

Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

18. Training

All staff and trustees 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.

19. Monitoring arrangements

The DPO and the DPO Leads are responsible for monitoring and reviewing this policy **every 2 years** and shared with the Trustee board. We may change this policy at any time. Where appropriate, we will notify data subjects of those changes.

The next scheduled review date is Mar 2023.

20. Linked Polices

Child Protection Policy – Covid19 Annex (Online safety section)

Behaviour Policy

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the headteacher and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure.)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school's network server.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach

    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- Records of all breaches will be stored on the school's network server.

  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

Actions to minimise the impact of data breaches

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

Set out the relevant actions you will take for different types of risky or sensitive personal data processed by your school. For example:

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO will 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 ensure we receive 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

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 student 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'/carers' financial details stolen