THE BLANDFORD SCHOOL

Data Protection Policy

Policy Reviewing

Policy Status/Review Programme	Annual
Reviewed by SLT	Summer 2025
Ratified by Governors	18 June 2021
Effective from	Summer 2025
Review scheduled for	Autumn 2025
Responsible Person	Data Protection Officer/JOA
Responsible Governor Committee	Resources Committee

Contents:

Statement of intent

The Blandford School is required to keep and process certain information about its staff members, Governors, students and regular visitors or volunteers to the school in accordance with its legal obligations under the GDPR.

The school may, from time to time, be required to share personal information about these individuals with other organisations, mainly the LA, other schools and educational bodies, and potentially children's services.

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

Organisational methods for keeping data secure are imperative, and The Blandford School believes that it is good practice to keep clear practical policies, backed up by written procedures.

1. Legal framework

1.1. This policy has due regard to legislation, including, but not limited to the following:

- The UK General Data protection Regulation (GDPR)
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998
- The Data Protection Act 2018

1.2. This policy also has regard to the following guidance:

- ICO (2021) 'Guide to the General Data Protection Regulation (GDPR)'
- DfE (2018) 'Data protection: a toolkit for schools'

1.3. This policy will be implemented in conjunction with the following other school policies:

- E-Safety
- Freedom of Information Policy
- Child Protection Policy

1.4. By following this Policy TBS will be able to meet their legal and best practice obligations and as such reduce the risk of reputational damage or financial penalty by the Information Commissioner's Office (ICO). The ICO is the UK body

responsible for monitoring compliance with data protection law and can impose penalties on organisations that are found to be non-compliant.

2. Applicable data

2.1. For the purpose of this policy, **personal data** refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. an IP address. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

2.2. **Sensitive personal data** is referred to in the UK GDPR as 'special categories of personal data', and is defined as:

- Genetic data.
- Biometric data.
- Data concerning health.
- Data concerning a person's sex life.
- Data concerning a person's sexual orientation.
- Personal data which reveals:
  - Racial or ethnic origin.
  - Political opinions.
  - Religious or philosophical beliefs.
  - Trade union membership.

2.3. Data Processed by The Blandford School

2.3.1. The School processes the following categories of data:

- Staff Data
- Student Data (including data on student contacts)
- Education Data
- Safeguarding Data
- Information about ex-students to manage the alumni web site may be collected
- Governors Data (not Safeguarding)

3. Principles

3.1. In accordance with the requirements outlined in the GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.

- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3.2. The GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

4. Accountability

4.1. The Blandford School will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

4.2. The school will provide comprehensive, clear and transparent privacy policies.

4.3. Records of activities relating to higher risk processing will be maintained, such as the processing of activities that:

- Are not occasional.
- Could result in a risk to the rights and freedoms of individuals.
- Involve the processing of special categories of data or criminal conviction and offence data.

4.4. Internal records of processing activities will include the following:

- Name and details of the organisation

- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

4.5. The school will also document other aspects of compliance with the UK GDPR and Data Protection Act where this is deemed appropriate in certain circumstances by the DPO, including the following:

- Information required for privacy notices, e.g. the lawful basis for the processing
- Records of consent
- Controller-processor contracts
- The location of personal data
- Data Protection Impact Assessment (DPIA) reports
- Records of personal data breaches
-

4.6. The school will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Minimising the processing of personal data.
- Pseudonymising personal data as soon as possible.
- Ensuring transparency in respect of the functions and processing of personal data.
- Allowing individuals to monitor processing.
- Continuously creating and improving security features.

4.7. Data protection impact assessments will be used, where appropriate.

5. Data protection officer (DPO)

5.1. A DPO has been appointed in order to:

- Inform and advise the school and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor the school's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

- Cooperate with the ICO and act as the first point of contact for the ICO and for individuals whose data is being processed.

5.2. The DPO is responsible for:

- Coordinating a proactive and preventative approach to data protection.
- Calculating and evaluating the risks associated with the school's data processing.
- Having regard to the nature, scope, context, and purposes of all data processing.
- Prioritising and focussing on more risky activities, e.g. where special category data is being processed.
- Promoting a culture of privacy awareness throughout the school community.

5.3. An existing employee will be appointed to the role of DPO provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests.

- The Data Protection Officer for the School is the Business Manager on behalf of the Headteacher.

5.4. The individual appointed as DPO will have professional experience and be highly knowledgeable about data protection law, particularly that in relation to schools.

5.5. The DPO will report to the highest level of management at the school, which is the governing board.

5.6. The DPO will operate independently and will not be dismissed or penalised for performing their duties.

5.7. Staff will ensure that they involve the DPO in all data protection matters closely and in a timely manner.

5.8. Sufficient resources and appropriate access will be provided to the DPO to enable them to meet their UK GDPR obligations.

6. Lawful processing

6.1. The legal basis for processing data will be identified and documented prior to data being processed.

6.2. Under the GDPR, data will be lawfully processed under one of the following conditions:

- The consent of the data subject has been obtained
- Processing is necessary for a contract held with the individual, or because they have asked the school to take specific steps before entering into a contract
- Processing is necessary for compliance with a legal obligation (not including contractual obligations)

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- Processing is necessary for protecting vital interests of a data subject or another person, i.e. to protect someone's life
- Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (This condition is not available to processing undertaken by the school in the performance of its tasks.)

6.3. The school will only process personal data without consent where any of the above purposes cannot reasonably be achieved by other, less intrusive means or by processing less data.

6.4. Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.
- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for:
  - Carrying out obligations under employment, social security or social protection law, or a collective agreement.
  - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
  - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
  - Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards.
  - The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.
  - Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
  - Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with article 89(1).

6.5. Where the school relies on:

- ‘Performance of contract’ to process a child’s data, the school considers the child’s competence to understand what they are agreeing to, and to enter into a contract.
- ‘Legitimate interests’ to process a child’s data, the school takes responsibility for identifying the risks and consequences of the processing, and puts age-appropriate safeguards in place.
- Consent to process a child’s data, the school ensures that the requirements outlined in 7.7 and 7.8 are met, and the school does not exploit any imbalance of power in the relationship between the school and the child.

7. Consent

7.1. Consent must be a positive indication expressly confirmed in words. It cannot be inferred from silence, inactivity, a positive action without words or pre-ticked boxes.

7.2. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual’s wishes.

7.3. Where consent is given, a record will be kept documenting how and when consent was given, and what the data subject was told. .

7.4. The school ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

7.5. Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

7.6. Consent can be withdrawn by the individual at any time.

7.7. Where the school opts to provide an online service directly to a child, the child is aged 13 or over, and the consent meets the requirements outlined in 7.2, the school obtains consent directly from that child; otherwise, consent is obtained from whoever holds parental responsibility for the child, except where the processing is related to preventative or counselling services offered directly to children.

7.8. In all other instances with regards to obtaining consent, an appropriate age of consent is considered by the school on a case-by-case basis, taking into account the requirements outlined in 7.2.

8. The right to be informed

8.1. Adults and children have the same right to be informed about how the school uses their data.

8.2. The privacy notices supplied to individuals, including children, in regard to the processing of their personal data will be written in clear, plain, age-appropriate language which is concise, transparent, easily accessible and free of charge.

8.3. In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller, the controller's representative, where applicable, and the DPO.
- The purpose of, and the lawful basis for, processing the data.
- The legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to third countries and the safeguards in place.
- The retention period of criteria used to determine the retention period.
- The existence of the data subject's rights, including the right to:
  - Withdraw consent at any time.
  - Lodge a complaint with a supervisory authority.
- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

8.4. Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided.

8.5. Where data is not obtained directly from the data subject, information regarding the categories of personal data that the school holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.

8.6. For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

8.7. In relation to data that is not obtained directly from the data subject, this information will be supplied:

- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- If the data are used to communicate with the individual, at the latest, when the first communication takes place.

9. The right of access

9.1. Individuals, including children, have the right to obtain a copy of their personal data as well as other supplementary information, including confirmation that their data is being processed.

9.2. Individuals, including children, have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

9.3. Where a SAR has been made for information held about a child, the school will evaluate whether the child is capable of fully understanding their rights. If the school determines the child can understand their rights, it will respond directly to the child.

9.4. The school will verify the identity of the person making the request before any information is supplied.

9.5. A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual requests further copies of the same information.

9.6. Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

9.7. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

9.8. All fees will be based on the administrative cost of providing the information.

9.9. All requests will be responded to without delay and at the latest, within one month of receipt.

9.10. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

9.11. Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

9.12. The school will ensure that information released in response to a SAR does not disclose personal data of another individual. If responding to the SAR in the usual way would disclose such data the school will:

- Omit certain elements from the response if another individual's personal data would be disclosed.
- Reject requests that cannot be fulfilled without disclosing another individual's personal data, unless that individual consents or it is reasonable to comply without consent.
- Explain to the individual who made the SAR why their request could not be responded to in full.

9.13. 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 – the time limit for responding to the request will be paused until clarification from the individual is received.

10. The right to rectification

10.1. Individuals, including children, are entitled to have any inaccurate or incomplete personal data rectified.

10.2. Where the personal data in question has been disclosed to third parties, the school will inform them of the rectification where possible.

10.3. Where appropriate, the school will inform the individual about the third parties that the data has been disclosed to.

10.4. Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

10.5. Requests for rectification will be investigated and resolved, where appropriate, free of charge; however, the school may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual makes multiple requests at once.

10.6. The school will take reasonable steps to ensure that data is accurate or are rectified if inaccurate, implementing a proportional response for data that has a significant impact on the individual, e.g. if significant decisions are made using that data.

10.7. The school will restrict processing of the data in question whilst its accuracy is being verified, where possible.

10.8. The school reserves the right to refuse to process requests for rectification if they are manifestly unfounded or excessive or if exemptions apply.

10.9. Where no action is being taken in response to a request for rectification, or where the request has been investigated and the data has been found to be accurate, the school will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

11. The right to erasure

11.1. Individuals, including children, hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

11.2. Individuals, including children, have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent, if this is the legitimate reason for processing
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed

- The personal data is required to be erased in order to comply with a legal obligation

11.3. The school will comply with the request for erasure without undue delay and at the latest within one month of receipt of the request.

11.4. The school has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

11.5. The school has the right to refuse a request for erasure for special category data where processing is necessary for:

- Public health purposes in the public interest, e.g. protecting against serious cross-border threats to health.
- Purposes of preventative or occupational medicine, the working capacity of an employee, medical diagnosis, the provision of health or social care, or the management of health or social care systems or services.

11.6. Requests for erasure will be handled free of charge; however, the school may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual makes multiple requests at once.

11.7. As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

11.8. Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

11.9. Where personal data has been made public within an online environment, the school will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

12. The right to restrict processing

12.1. Individuals, including children, have the right to block or suppress the school's processing of personal data.

12.2. In the event that processing is restricted, the school will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

12.3. The school will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the school has verified the accuracy of the data
- Where an individual has objected to the processing and the school is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where the school no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

12.4. If the personal data in question has been disclosed to third parties, the school will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

12.5. Where the school is restricting the processing of personal data in response to a request, it will make that data inaccessible to others, where possible, e.g. by temporarily moving the data to another processing system or unpublishing published data from a website.

12.6. The school will inform individuals when a restriction on processing has been lifted.

12.7. The school reserves the right to refuse requests for restricting processing if they are manifestly unfounded or excessive or if exemptions apply. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

13. The right to data portability

13.1. Individuals, including children, have the right to obtain and reuse their personal data for their own purposes across different services.

13.2. Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

13.3. The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

13.4. Personal data will be provided in a structured, commonly used and machine-readable form.

13.5. The school will provide the information free of charge.

13.6. Where feasible, data will be transmitted directly to another organisation at the request of the individual.

13.7. The school is not required to adopt or maintain processing systems which are technically compatible with other organisations.

13.8. In the event that the personal data concerns more than one individual, the school will consider whether providing the information would prejudice the rights of any other individual.

13.9. The school will respond to any requests for portability within one month.

13.10. Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

13.11. Where no action is being taken in response to a request, the school will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

14. The right to object

14.1. The school will inform individuals, including children, of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

14.2. Individuals, including children, have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing
- Processing for purposes of scientific or historical research and statistics.

14.3. Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- The school will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the school can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.
- The school will respond to objections proportionally, granting more weight to an individual's objection if the processing of their data is causing them substantial damage or distress.

14.4. Where personal data is processed for direct marketing purposes:

- The school will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The school cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.
- The school will retain only enough information about the individual to ensure that the individual's preference not to receive direct marketing is respected in future.

14.5. Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the school is not required to comply with an objection to the processing of the data.

14.6. The DPO will ensure that details are recorded for all objections received, including those made by telephone or in person, and will clarify each objection with the individual making the request to avoid later disputes or misunderstandings.

14.7. Where the processing activity is outlined above, but is carried out online, the school will offer a method for individuals to object online.

14.8. The school will respond to all objections without undue delay and within one month of receiving the objection; this may be extended by a further two months if the request is complex or repetitive.

14.9. Where no action is being taken in response to an objection, the school will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

15. Automated decision making and profiling

15.1 The Blandford School does not carry out any automated decision making and profiling.

16. Data protection by design and default

16.1. The school will act in accordance with the UK GDPR by adopting a data protection by design and default approach and implementing technical and organisational measures which demonstrate how the school has considered and integrated data protection into all aspects of processing activities.

16.2. In line with the data protection by default approach, the school will ensure that only data that is necessary to achieve its specific purpose will be processed.

16.3. The school will implement a data protection by design and default approach by using a number of methods, including, but not limited to:

- Considering data protection issues as part of the design and implementation of systems, services and practices.
- Making data protection an essential component of the core functionality of processing systems and services.
- Automatically protecting personal data in school ICT systems.
- Promoting the identity of the DPO as a point of contact.
- Ensuring that documents are written in plain language so individuals can easily understand what is being done with personal data.

17. Data Protection Impact Assessments (DPIAs

17.1. DPIAs will be used in certain circumstances to identify the most effective method of complying with the school's data protection obligations and meeting individuals' expectations of privacy.

17.2. DPIAs will allow the school to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the school's reputation which might otherwise occur.

17.3. A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

17.4. A DPIA will be used for more than one project, where necessary.

17.5. High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences
- The use of CCTV.

17.6. 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

17.7. Where a DPIA indicates high risk data processing, the school will consult the ICO to seek its opinion as to whether the processing operation complies with the UK GDPR.

18. Data breaches

18.1. The term ‘personal data breach’ refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

18.2. The Headteacher will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.

18.3. Where the school faces a data security incident, the DPO will coordinate an effort to establish whether a personal data breach has occurred, assess the significance of any breach, and take prompt and appropriate steps to address it.

18.4. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

18.5. All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the school becoming aware of it.

18.6. 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.

18.7. 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.

18.8. A ‘high risk’ breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

18.9. In the event that a breach is sufficiently serious, the public will be notified without undue delay.

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

18.11. 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

18.12. Where notifying an individual about a breach to their personal data, the school will provide specific and clear advice to individuals on the steps they can take to protect themselves and their data, where possible and appropriate to do so.

18.13. Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

18.14. The school will ensure all facts regarding the breach, the effects of the breach and any decision-making processes and actions taken are documented in line with the UK GDPR accountability principle and in accordance with school policies.

18.15. The school will work to identify the cause of the breach and assess how a recurrence can be prevented, e.g. by mandating data protection refresher training where the breach was a result of human error.

19. Data security

19.1. Confidential paper records will be kept in a locked filing cabinet, drawer, safe or office with restricted access.

19.2. Confidential paper records will not be left unattended or in clear view anywhere with general access.

19.3. Digital data is coded and password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site. Consideration will be given to the necessity of encrypting hard drives.

19.4. Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer, safe or office when not in use.

19.5. Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted. Memory sticks will only be used in exceptional circumstances.

19.6. All electronic devices are password-protected to protect the information on the device in case of theft.

19.7. Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.

19.8. Staff and governors will not use their personal laptops or computers for school purposes.

19.9. All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

19.10. Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.

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

19.12. When sending confidential information by fax, staff will always check that the recipient is correct before sending.

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

19.14. Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

19.15. 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.

19.16. 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.

19.17. The school will regularly test, assess and evaluate the effectiveness of any and all measures in place for data security.

19.18. The Blandford School takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

19.19. The Business Manager is responsible for continuity and recovery measures are in place to ensure the security of protected data.

20. Safeguarding

20.1. The school understands that the UK GDPR does not prevent or limit the sharing of information for the purposes of keeping children safe.

20.2. The school will ensure that information pertinent to identify, assess and respond to risks or concerns about the safety of a child is shared with the relevant individuals or agencies proactively and as soon as is reasonably possible.

20.3. Where there is doubt over whether safeguarding information is to be shared, especially with other agencies, the DSL will ensure that they record the following information:

- Whether data was shared
- What data was shared
- With whom data was shared
- For what reason data was shared
- Where a decision has been made not to seek consent from the data subject or their parent
- The reason that consent has not been sought, where appropriate

20.4. The school will aim to gain consent to share information where appropriate; however, will not endeavour to gain consent if to do so would place a child at risk.

20.5. The school will manage all instances of data sharing for the purposes of keeping a child safe in line with the Child Protection and Safeguarding Policy.

21. Publication of information

21.1. The Blandford School publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

- Policies and procedures
- Annual reports

21.2. Classes of information specified in the publication scheme are made available quickly and easily on request.

21.3. The Blandford School will not publish any personal information, including photos, on its website without the permission of the affected individual.

21.4. When uploading information to the school website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

22. Data Processing

22.1. All data will be processed, whether in electronic or paper form, to ensure that no personal data that identifies an individual is shared outside of the school, unless there is an authorised or lawful requirement to do so.

22.2. All processors will protect against unauthorised and unlawful processing and against accidental loss, destruction or damage.

22.3. All electronic data in all categories identified above will be protected using passwords and encryption to stop illegal and unauthorised access to personal data.

22.4. All hard copy data will be maintained in locked cabinets when not being used.

22.5. The Data Protection Officer will ensure that those authorised to access the information are recorded.

22.6. The Data Controllers are to maintain documentation about the date that it is processed. The information to be documented is listed at Appendix B.

23. CCTV and photography

23.1. The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

23.2. The school notifies all students, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.

23.3. Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

23.4. All CCTV footage will be kept for a maximum of 60 days for security purposes; the Business manager is responsible for ensuring the records are stored securely and allowing access.

23.5. The school will always indicate its intentions for taking photographs of students and will retrieve permission before publishing them.

23.6. If the school wishes to use images/video footage of students in a publication, such as the school website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parent of the student.

23.7. Precautions are taken when publishing photographs of students, in print, video or on the school website by ensuring that parental permission has been given for the publication.

23.8. Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

24. Data retention

24.1. Data will not be kept for longer than is necessary.

24.2. Unrequired data will be deleted as soon as practicable.

24.3. Some educational records relating to former students 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.

24.4. Paper documents will be shredded, pulped or disposed of securely via a suitable alternative method, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

24.5. Staff data will be retained while staff are members of the school and in accordance with the local authority's instructions amended from time to time to comply with legal requirements for retention of employment records.

24.6. Education data will be maintained in accordance with the Department for Education and local authority's instructions amended from time to time.

24.7. Safeguarding data will be retained in accordance with the local authority's instructions amended from time to time.

24.8. Alumni data will be retained whilst consent from the individual is current. If consent is withdrawn or contact with the individual via email has been lost, all data pertaining to the individual will be removed.

24.9. Data can be anonymised and kept for statistical purposes as long as it is required by the school or local authority.

24.10. Contact lists containing name, addresses and telephone numbers only will be retained for contact purposes with the consent of the individual, or as required to ensure the school is able to fulfil its legal obligations. This information is so that the school can contact those who have had an interest in the school and whom the school may wish to contact in the future for invitations to events, for tendering or for volunteering.

25. Data Disposal

25.1. Hard copy personal data will be destroyed by a cross-cut shredder, or via a suitable alternative secure method.

25.2. Electronic data will be deleted from the files in accordance with the disposal arrangements outlined above

25.3. Any hard disks that have contained personal data will be destroyed by ensuring that either the magnetic palters are broken into pieces or if integrated circuit based storage are also broken into pieces.

26. DBS data

26.1. All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

26.2. Data provided by the DBS will never be duplicated.

26.3. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

27. Policy review

27.1. This policy is reviewed every two years by the Business Manager and the Headteacher.

27.2. The next scheduled review date for this policy is February 2023.

Appendix A to the Data Protection Policy

Privacy Notice Information

The following information has to be provided in a Data Protection Privacy Notice under the GDPR ’18:

1. The name and contact details of our organisation.
2. The name and contact details of our representative (if applicable).
3. The contact details of our data protection officer (if applicable).
4. The purposes of the processing.
5. The lawful basis for the processing.
6. The legitimate interests for the processing (if applicable).
7. The categories of personal data obtained (if the personal data is not obtained from the individual it relates to).
8. The recipients or categories of recipients of the personal data.
9. The details of transfers of the personal data to any third countries or international organisations (if applicable).
10. The retention periods for the personal data.
11. The rights available to individuals in respect of the processing.
12. The right to withdraw consent (if applicable).
13. The right to lodge a complaint with a supervisory authority.
14. The source of the personal data (if the personal data is not obtained from the individual it relates to).
15. The details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is collected from the individual it relates to).
16. The details of the existence of automated decision-making, including profiling (if applicable).

Appendix B to the Data Protection Policy

Controller's Documentation Check List

1. Your organisation's name and contact details.

2. If applicable, the name and contact details of your data protection officer – a person designated to assist with GDPR compliance under Article 37.

3. If applicable, the name and contact details of any joint controllers – any other organisations that decide jointly with you why and how personal data is processed.

4. The purposes of the processing – why you use personal data, e.g. customer management, marketing, recruitment.

5. The categories of individuals – the different types of people whose personal data is processed, e.g. employees, customers, members.

6. The categories of personal data you process – the different types of information you process about people, e.g. contact details, financial information, health data.

7. The categories of recipients of personal data – anyone you share personal data with, e.g. suppliers, credit reference agencies, government departments.

8. If applicable, the name of any third countries or international organisations that you transfer personal data to – any country or organisation outside the EU.

9. If applicable, the safeguards in place for exceptional transfers of personal data to third countries or international organisations. An exceptional transfer is a non-repetitive transfer of a small number of people's personal data, which is based on a compelling business need, as referred to in the second paragraph of Article 49(1) of the GDPR.

10. If possible, the retention schedules for the different categories of personal data – how long you will keep the data for. This may be set by internal policies or based on industry guidelines, for instance.

11. If possible, a general description of your technical and organisational security measures – your safeguards for protecting personal data, e.g. encryption, access controls, training.

Appendix C to the Data Protection Policy

Personnel File – Disposal Schedule

Date of Disposal	Name of Employee	Date Employment Ended

Salary Information – Disposal Schedule

Date of Disposal	Name of Employee	Date Employment Started

Other Personal Information (ie H&S or Safeguarding) – Disposal Schedule

Date of Disposal	Name of Employee	Date Record Made	Comments