Abbey College, Ramsey

(In conjuction with Meridian Trust)

Data Protection Policy

Policy Developed by: Meridian Trust/DPO
Reviewing committee: Operations
Frequency of Review: 3 Yearly
Date last reviewed: May 2025
Date Approved: 1st July 2025
Due for Review: Spring 2028

Introduction

1. Abbey College collects, processes, holds and shares personal data, and treats it in an appropriate and lawful manner.
2. This policy complies with data protection laws, including the Data Protection Act 2018, the UK General Data Protection Regulation (UK GDPR), and other legal requirements such as the Protection of Freedoms Act 2012.
3. This policy outlines data protection requirements and legal conditions for obtaining, handling, processing, storing transporting and destructing personal information.
4. To support this policy, staff shall apply associated policies and procedures and participate in all training if requested to do so by Abbey College.
5. Staff should raise any concerns with the implementation of this policy, this should be raised with the Senior Leadership Team.
6. This policy may be amended at any time. Any breach of this policy will be taken seriously and may result in disciplinary action.
7. This policy will be implemented in conjunction with the following policies:
    - CCTV Policy
    - Freedom of Information Policy
    - Records Management Policy

Aims

8. To ensure Abbey College fulfils its statutory responsibilities.
9. To ensure effective security and protection for data that has been provided by individuals to Abbey College which is required for the management and operation of its establishments.
10. To support the mission, vision and values of Abbey College and its establishments.

Who is responsible for the policy?

11. Abbey College is responsible for ensuring compliance with the policy, but delegates day-to-day responsibility to the senior management team of each establishment.
12. Abbey College's Governing Body and Senior Leadership Team are responsible for fairly applying the policy, while all staff members must support colleagues and ensure its success.

Data protection definitions

13. Data is information which is stored electronically or in paper-based filing systems.
14. Personal data refers to information about a living individual who can be identified either solely from that data or in combination with other data held by the trust. Personal data can include factual details e.g., name, address, date of birth or it can be subjective information e.g., performance appraisal.
15. Special category data comprises information regarding racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health condition, sexual orientation, sex life as well as genetic and biometric data. Processing of special category data should only be done so with explicit consent from the individual.
16. Data subjects are the individuals about whom the personal data is held.
17. Processing refers to using, obtaining, recording, holding, organising, amending, retrieving, disclosing, erasing, destroying or transferring data to third parties.
18. Biometric data is personal information about an individual's physical or behavioural characteristics that can be used to identify that person, including their fingerprints, facial shape, retina, and iris patterns.

Within Abbey College, only fingerprints are used.

19. An Automated biometric recognition system uses electronic equipment to measure an individual's physical or behavioural characteristics. It automatically compares the individual's information with stored biometric data to identify any matches.
20. Data Controller – Abbey College is registered with the Information Commissioner's Office as the Data Controller for all of its establishments. As the Data Controller, it determines the purpose for which, and the manner in which, any personal data is processed.

Data protection principles

21. Data protection principles are a set of guidelines that outline how personal data should be handled and protected, ensuring its confidentiality, integrity, and availability.
22. Data protection principles aim to ensure that personal data is handled responsibly and in accordance with individuals' rights. The principles include processing data lawfully and transparently, limiting data collection to necessary purposes, minimising the amount of data collected, ensuring data is accurate and up to date, storing data for only as long as necessary, securing data from unauthorised access, and being accountable for data protection compliance. These principles are essential for protecting individuals' personal information and maintaining their privacy.
23. Abbey College, as the Data Controller, is responsible for, and able to demonstrate, compliance with the principles.
24. In applying data protection law, Abbey College will also apply data protection exemptions that are provided within the law.

Accountability

25. Abbey College, with support from Meridian Trust, will implement appropriate technical and organisational measures to demonstrate that data is processed in line with data protection law.
26. Abbey College will provide comprehensive, clear and transparent Privacy Notices.
27. A Record of Processing will be maintained by Abbey College, containing information about the organisation, the purposes of processing, categories of personal data, retention schedules, recipients of personal data, security measures, and details of transfers to third countries with safeguards.
28. Abbey College will take steps to ensure the privacy and security of data, including using techniques like reducing data, making data anonymous, being open about data use, giving individuals the ability to oversee how their data is handled, and continuously improving safety measures.
29. Data Protection Impact Assessments (DPIA) are completed when considering using new technologies for the storage, accessing or processing of personal data, or if a new requirement for processing is likely to result in a high risk to the rights and freedoms of individuals.

Data Protection Officer and establishment leads

30. The Meridian Trust Data Protection Officer (DPO), who acts on behalf of Abbey College, can be contacted at the following address: Data Protection Officer
    Meridian Trust Head Office, Fen Lane, Sawtry, PE28 5TQ
    or Email: dpo@meridiantrust.co.uk
31. The Data Protection Officer has responsibilities such as informing and advising the trust and its establishments about data protection laws, monitoring compliance, managing internal activities, conducting audits, and providing training to staff.
32. The DPO will act independently and will not be dismissed or penalised for performing their role.
33. The DPO will be given sufficient resources to fulfil their obligations under the law.
34. Abbey College has a Data Protection Lead who supports the DPO. This is the PA to the Headteacher who is the first point of contact for guidance and support.

35. The Data Protection Lead's role is to support the trust in complying with the Data Protection Act and ensuring that the establishment follows the trust's data protection policies and procedures.

36. In the event of a data subject looking to exercise their rights, which are listed in this policy, the Data Protection Lead should ensure that these requests are forwarded to the Meridian Trust Central team within 24 hours of receipt.

Roles and Responsibilities

37. This policy applies to all staff, including any external organisations or individuals working on behalf of Abbey College. Staff who do not comply with this policy may face disciplinary action.

38. The Operations Committee have overall responsibility for ensuring that Abbey College complies with all relevant data protection obligations.

39. The Headteacher acts as representatives of the data controller on a day to day basis.

40. Staff are responsible for:

40.1 Collecting, storage, processing, publishing any personal data in accordance with this policy.

40.2 Informing HR of any changes to their living arrangements, personal data (I.e: New address, phone number, home e-mail, living status)

40.3 Contacting the DPO if they have any queries or questions regarding the use of and the protection of data within the School, including;

40.3.1.1 Concerns that the policy is not being followed

40.3.1.2 If they are unsure how to process a piece of personal data, including how they can store and transmit/receive data from external sources

40.3.1.3 If there has been a data breach

40.3.1.4 If they are unsure whether there is a lawful basis to collect and/or store information

40.3.1.5Whenever they are engaging in a new activity that may affect the privacy rights of an individual, including the use of a new data processor and the upload of data to 3rd party companies such as new learning platforms where students need to login

40.3.1.6If they need to apply a UK GDPR principle to processing data

Lawful processing

41. Data will only be lawfully processed if one of the following conditions is satisfied:

- meeting legal obligations
- performing tasks in the public interest or exercising official authority
- carrying out contracts
- protecting vital interests
- pursuing legitimate interests unless these interests' conflict with the rights and freedoms of the data subject. This does not apply to processing carried out by the establishment in the performance of its tasks.
- consent of the data subject has been obtained

42. The legal basis for processing data will be identified and documented within the Record of Processing prior

to the data being processed.

43. Due to its sensitive nature, to lawfully process special category data, a lawful basis under Article 6 of the UK GDPR and a condition for processing under Article 9 of the UK GDPR must both be identified.
44. Abbey Colege will meet the requirement to identify the relevant legal basis for processing special category data as set out in the UK GDPR and DPA 2018.

Consent

45. Consent will only be asked for before processing any data that cannot be done for any other lawful reason.
46. Consent must be clear and not be assumed from silence, inactivity or pre-selected options.
47. Consent will only be accepted if it is freely given, specific, informed, and unambiguous.
48. A record of consent will be kept to document how, when, and what type of consent was given.
49. Where the standard of consent cannot be met, processing will cease.
50. Consent provided under previous data protection legislation is reviewed to ensure it meets current standards. Consent will not be reobtained if it was acceptable under previous laws.
51. Consent can be withdrawn by the individual at any time.
52. Pupils who can understand their rights under data protection legislation will provide their own consent; this will supersede any parental consent.
53. The age, maturity, and mental capacity of the student will be considered when determining if they can understand and exercise their rights.
54. Pupils aged 13 or over will provide their own consent, including for photos and videos, except where the criteria in point 53 cannot be met, in which case, the parental consent will stand.
55. When obtaining consent from students, Meridian Trust will ensure they understand what they are agreeing to and will not use any power imbalance between students and the trust.
56. According to the Protections of the Freedoms Act 2012, consent for processing biometric data will be obtained from parents of children under 18.
57. Consent will be valid for the duration of a student's attendance unless it is withdrawn or there is a change in parental responsibility.
58. If there is a disagreement over consent or no response to a consent request, it will be assumed that consent has not been given.
59. The designated safeguarding lead will work with a student's social worker, carers, or adoptive parents to determine where to seek consent for 'looked after children' or adopted students, considering any risk to their security.

The right to be informed

60. Privacy Notices will be given to people to inform them about how their personal data is being used. They are written in plain English and tailored to the audience they relate to. Privacy Notices contain all the information that the law requires us to give to people about their data.
61. When collecting data directly from the data subject, Abbey College will inform the data subject if providing this data is obligatory by law or a contractual requirement, or entirely voluntary. Abbey College will also inform them about what may happen if they do not provide their data.
62. If Abbey College does not get data directly from a data subject, they will provide information about the categories of personal data they hold, where it came from, and if it was from publicly accessible sources. They will provide this information before disclosing the data to someone else or when they first communicate with the individual.

The right of access

63. Individuals have the right to obtain confirmation that their data is being processed.
64. Individuals have the right to request their personal data through a Subject Access Request (SAR).
65. A request must be made to the Data Protection Officer. Meridian Trust also has a Subject Access Request (SAR) Form, available on school website, that can be used to ensure all the required information is included.
66. The Data Protection Lead should forward any SARs to the Meridian Trust team at dpo@meridiantrust.co.uk within 24 hours of receipt, with the exception of requests for letters regarding enrolment or attendance.
67. Establishments should handle requests for letters from parents, staff or other data subjects in line with the Standard Operating Procedures.
68. For SARs from parents/guardians regarding pupils deemed to be aware of their data rights, establishments will seek, and record, the consent of the pupil using the appropriate consent form before releasing the information.
69. Meridian Trust or Abbey College will undertake an ID check for the requestor before any information is released.
70. Requests are considered in line with data subject's legal rights and Meridian Trust' legal obligations.
71. If a SAR has been made electronically, the response will be provided in a commonly used electronic format.
72. Any information supplied is free, however a fee may be charged for additional copies.
73. Where a request is manifestly unfounded, excessive or repetitive, a fee may be charged.
74. All fees will be based on the administrative cost of providing the information.
75. All requests will be responded to without delay and ordinarily within one month of receipt.
76. If there are many or complex requests, the response time may be extended by up to two months. The individual will be informed of this extension and the reason within one month.
77. If a request is unfounded or excessive or may cause safeguarding concerns to a child or vulnerable person, Meridian Trust/Abbey College may decline to respond. The individual will be informed of this decision, the reasoning, and their right to complain to the Information Commissioner's Office (ICO) and to a judicial remedy, within one month of the refusal.
78. If a large quantity of information is being processed about an individual, Meridian Trust/Abbey College will ask the individual to specify the information the request is in relation to.
79. In England, Wales and Northern Ireland, the parent's automatic right of access to their child's 'educational record' is only applicable in maintained schools and not in academies.

Exemptions to access by data subjects

80. Where a claim to legal professional privilege could be maintained in legal proceedings, the information is likely to be exempt from disclosure unless the privilege is waived.
81. There are other exemptions from the right of subject access. If we intend to apply any of them to a request, then we will usually explain which exemption is being applied and why.
82. The Academy will not disclose information if it:

    i. Might cause serious harm to the physical or mental health of the individual or another individual
    ii. Would reveal that a pupil is at risk of abuse or where the disclosure of that information would not be in the child's best interests
    iii. Is detailed in the court orders
    iv. Is information where disclosure would result in revealing personal information about another pupil, staff member, volunteer or visitor

The right to rectification

83. Individuals are entitled to have any inaccurate or incomplete personal data rectified.
84. Meridian Trust/Abbey College will inform any third parties of the data rectification where necessary and possible. Where appropriate, Meridian Trust/Abbey College will inform the individual about third parties that data has been disclosed to.
85. Requests for rectification will be responded to within one month. If complex, this will be extended by up to two months.
86. Meridian Trust/Abbey College may refuse to act on a request for rectification. The individual will be informed of this decision, the reasoning, and their right to complain to the Information Commissioner's Office (ICO) and to a judicial remedy, within one month of the refusal.

The right to erasure

87. Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.
88. Individuals have the right to have their personal data erased in certain situations. These situations include when the personal data is no longer needed for its original purpose, when the individual withdraws consent, when there are no overriding legitimate reasons for continuing the processing, when the personal data is used for direct marketing and the individual objects, when the personal data is unlawfully processed, when there is a legal obligation to erase the data, and when the data is processed in relation to information society services offered to a child.
89. Meridian Trust/Abbey College can refuse a request to erase personal data if it is being processed for certain reasons, such as exercising the right of freedom of expression and information, complying with a legal obligation for performance of a public interest task or exercise of official authority, public health purposes in public interest, for archiving purposes in public interest, scientific, historical or statistical research, or to defend legal claims.
90. Special attention will be given to existing situations where a child has given consent to processing and later requests erasure of the data, regardless of age at the time of the request.
91. Where personal data has been disclosed to third parties, they will be informed about the erasure of personal data, unless it is impossible or involves disproportionate effort to do so.
92. Where personal data has been made public within an online environment, the establishment will inform other organisations who process the personal data to erase links to and copies of the personal data in question, unless it is impossible or involves disproportionate effort to do so.

The right to restrict processing

93. Individuals have the right to block or suppress Abbey College's processing of their own personal data.
94. If processing is restricted, Abbey college will retain the personal data but refrain from using any further. They will only keep enough information to make sure the restriction is followed in the future.
95. Abbey College will restrict the processing of personal data in the following circumstances:
    a. If the accuracy of data is contested, further processing will be restricted until accuracy is verified
    b. Where an objection is raised for processing and Meridian Trust/Abbey College is considering the legitimate grounds for processing
    c. Where processing is unlawful and the individual requests restriction over erasure
    d. Where Abbey College no longer needs the personal data, but the individual requires the data to establish, exercise or defend a legal claim
96. If the personal data in question has been disclosed to third parties, Meridian Trust/Abbey college will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

97. Meridian Trust/Abbey College will inform individuals when a restriction on processing has been lifted.

The right to data portability

98. Individuals have the right to obtain and reuse their personal data for their own purposes.
99. Personal data can be moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.
100. The right to data portability applies only in the following cases: when an individual has provided their personal data to a controller, and when the processing is based on the individual's consent or a contract, and when the processing is done automatically.
101. Personal data will be provided in a structured, commonly used and machine-readable form.
102. Meridian Trust/Abbey College will provide the information free of charge.
103. If possible, data will be sent directly to another organisation at the request of the individual.
104. Meridian Trust/Abbey College is not required to adopt or maintain processing systems which are technically compatible with other organisations.
105. If the personal data concerns more than one individual, Meridian Trust/Abbey College will consider whether providing the information would prejudice the rights of any other individual.
106. Meridian Trust will respond to any requests for portability within one month.
107. Where the request is complex, or multiple 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.
108. Meridian Trust/Abbey College may refuse to act on a request. The individual will be informed of this decision, the reasoning, and their right to complain to the Information Commissioner's Office (ICO) and to a judicial remedy, within one month of the refusal.

The right to object

109. Meridian Trust/Abbey College will clearly and explicitly inform individuals of their right to object at the first point of communication, and this information will also be clearly outlined in the Privacy Notice.
110. Individuals have the right to object to the following types of processing:
    i. processing based on legitimate interests or the performance of a task in the public interest
    ii. direct marketing
    iii. processing for purposes of scientific or historical research and statistics
111. Where personal data is processed for the performance of a legal task or legitimate interests:
    i. an individual's grounds for objecting must relate to his or her situation; and
    ii. Meridian Trust will only process an individual's personal data if it is necessary for legal claims or if there compelling legitimate grounds that override the individual's interests, rights, and freedoms
112. Where personal data is processed for direct marketing purposes:
    i. processing of personal data for direct marketing purposes will stop when an objection is received
    ii. Meridian Trust cannot refuse an individual's objection regarding data that is being processed
    iii. for direct marketing purposes
113. If personal data is used for research, the person can only object if they have a valid reason. Meridian Trust does not have to stop processing data for research if it is necessary for a public interest task.

Automated decision making and profiling

114. Individuals have the right to not be subjected to a decision that is made by automated processing e.g. profiling and has a significant impact on them legally or otherwise.
115. Meridian Trust will ensure that individuals can seek human help, share their opinion, understand any

decisions made and question these.

116. Meridian Trust/Abbey College will ensure the necessary safeguards are in place when automatically processing personal data for profiling. This includes providing clear and useful information about the logic used with significance and predicted impact, using appropriate mathematical or statistical procedures, implementing appropriate measures to enable the correction of inaccuracies and minimise the risk of errors, and securing the data in a way that is proportionate to the risk to the interests and rights of individuals and preventing discriminatory effects.
117. Meridian Trust/Abbey College reserves the right to implement artificial intelligence (AI) as developments in the sector arise.
118. Where it is being considered that AI will be implemented and there is the potential for personal data to be impacted, Meridian Trust will undertake a Data Protection Impact Assessment, see below.

Privacy by design and privacy impact assessments

119. Meridian Trust/Abbey College will prioritise privacy and incorporate data protection into their processing activities through a privacy by design approach and implementing technical and organisational measures.
120. Meridian Trust/Abbey College will use Data Protection Impact Assessments (DPIAs) to identify the most effective way to comply with data protection obligations and meet individuals' privacy expectations when new data processing requirements are identified.
121. DPIAs will help Meridian Trust identify and resolve problems early, reducing costs and preventing risks to individuals' rights and the reputation of Meridian Trust and Abbey College.
122. DPIAs will be conducted when using new technologies or when processing is likely to pose a high risk to individuals' rights and freedoms.
123. A DPIA can be used for multiple projects when necessary. High risk processing includes systematic and extensive processing activities, large scale processing of special categories of data or data related to criminal convictions or offenses, and the use of CCTV.
124. Meridian Trust has a template DPIA that Abbey College will use to ensure all necessary information is included and considered correctly.
125. Abbey College will collaborate with the Meridian Trust Central Assurance Team to ensure accurate and thorough completion of DPIAs.
126. If a DPIA indicates high risk data processing, the matter will be referred to the Data Protection Officer, who may consult the ICO to ensure compliance with data protection laws.
127. The information within the DPIA will assist in completing the Record of Processing.

Data breaches

128. A personal data breach is when there is a breach of security that leads to the destruction, loss, alteration, unauthorised disclosure, or access to personal data.
129. The Data Protection Officer (DPO) at Meridian Trust will ensure that all staff are aware of and understand what constitutes a data breach during their data protection training.
130. All data breaches must be notified immediately to the DPO.
131. The Data Breach Reporting Form should be used to report the breach to the DPO. However, if not all information is known, notification to the DPO should not be delayed.
132. Upon receiving the Data Breach Reporting Form, the DPO will complete a Risk Assessment to determine whether the matter needs to be reported to the ICO.
133. If a breach is likely to lead to a risk to the rights and freedoms of individuals, the ICO will be notified.
134. 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.
135. All breaches requiring notification to the ICO must be reported within 72 hours of Meridian Trust becoming

aware of the breach.

136. If a breach is likely to result in a high risk to the rights and freedoms of an individual, Meridian Trust/Abbey College will notify those concerned directly.

137. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

138. If a breach is sufficiently serious, Meridian Trust will notify the public as required.

139. Effective breach detection, investigation, and reporting procedures are to be maintained at Abbey College.

140. Meridian Trust will maintain a log of data protection breaches.

141. Failure to report a notifiable breach to ICO without the statutory timescale may result in a fine, as well as a fine for the breach itself.

Security

142. Abbey College in conjunction with Meridian Trust will protect personal data from unauthorised processing, accidental loss, or damage, and individuals can seek compensation through the courts if they suffer damage from such incidents.

143. Abbey College will have procedures and technologies in place to secure personal data from the point of collection through to destruction.

144. In line with Abbey College Privacy Notices, information will not be shared with third parties without consent unless permitted by law.

145. Personal data shall not be transferred to a country or territory outside of the UK unless that country or territory has a UK "adequacy regulation" or one of the appropriate safeguards, included in the UK GDPR, has been implemented. These countries include countries or territories that have a UK adequacy regulation include all EU member states, the three additional EEA member states (Iceland, Norway, and Liechtenstein), Gibraltar, Andorra, Argentina, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, Uruguay, Japan (private sector organisations only), and Canada (only data that is subject to Canada's Personal Information Protection and Electronic Documents Act)

146. Personal data will only be transferred to a third-party data processor if that party agrees to comply with Abbey College's data transfer policies and procedures.

147. Third parties must undergo a due diligence check before being contracted with and must meet acceptable data security standards. Abbey College reserves the right to terminate the contract if it becomes aware of any data security concerns.

148. Third parties can access Meridian Trust IT systems if they accept our ICT security policies and procedures.

149. Maintaining data security means guaranteeing:

    i. confidentiality of the data - only people who are authorised to use the data can access it
    ii. integrity of the data - data should be accurate and suitable for the processing purpose
    iii. availability of the data - authorised users should be able to access the data if they need it

150. Meridian Trust and Abbey College employ multiple security procedures to ensure the safety and integrity of its systems. These include but are not limited to controlled entry, locked storage for paper records, multi-layer password protection for electronic data, and encryption for removable storage devices.

151. Before sharing data, staff will ensure they have permission, adequate security measures are in place, and the recipient is specified within a Privacy Notice.

152. Visitors will not be permitted access to confidential or personal information under any circumstances.

153. The physical security of establishments' buildings and storage systems is regularly reviewed with additional measures implemented if required.

154. Visitors to areas of Abbey College containing sensitive information are always supervised.

155. Meridian Trust' Director of IT is responsible for ensuring continuity and recovery measures for data

security.

156. Abbey College will ensure that ICT security policies and procedures are implemented.

Statutory requests for information

157. A statutory request for information is a request for information about a member of staff, pupil or group of pupils from a statutory body.
158. Before information is shared with a statutory body, establishments should ensure they have identified an appropriate lawful basis for processing, or an exemption, and that this is fully recorded.
159. Meridian Trust Central have issued Standard Operating Procedure guidance to ensure compliance by establishments.

Training

160. All staff, trustees and academy councilors are provided with data protection training as part of their induction.
161. Data protection training is also part of the CPD process for staff each year.
162. Where significant changes are applied to legislation, the Trust will make the necessary training available to ensure all staff are updated.

Providing information over the telephone

163. Staff who deal with phone calls should be careful not to unlawfully share personal information. They should make sure to confirm the identity of the caller before giving out any information and follow the correct procedure for handling requests for personal data.
164. If staff encounter difficult situations, they can ask the Data Protection Officer or the senior leadership team for help. It is important that no one is forced, rushed or intimidated into sharing personal information.

Publication of information

165. Abbey College has a Publication Scheme outlining classes of information that are made routinely available. This includes policies, annual reports and financial information.
166. Classes of information specified on the publication scheme are made available upon request.
167. When uploading information to the website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

Images: photography and videos

168. Abbey College understands that recording images of identifiable individuals constitutes processing personal data and should be done in line with data protection principles.
169. Meridian Trust, and its establishments, notifies all pupils, staff and visitors of the purpose for collecting CCTV images via signage.
170. CCTV cameras are only placed where they do not intrude on anyone's privacy and are necessary
171. to fulfil their purpose.
172. CCTV is operated in line with the trust's CCTV Policy.
173. Abbey College will indicate their intentions for taking photographs and/or videos and will verify permission before publishing them. Consent is sought within the admissions pack.
174. Under data protection law, photos and videos may be kept for archival, public interest, and historical research purposes.
175. The Photography and Videos Consent Form is used when using images for publications not covered by the existing form.

176. Images captured by individuals on our premises for recreational/personal purposes made by parents/carers are exempt from data protection law.
177. Meridian Trust Central have issued Standard Operating Procedure guidance to ensure compliance by establishments.

Biometric information

178. Biometric data is a special category of data that is protected under the Data Protection Act 2018 and the UK GDPR.
179. Before processing biometric data or implementing a system that involves biometric data processing, Abbey College will work with the DPO to complete a DPIA. The establishment must handle biometric data carefully and comply with all legal requirements when obtaining consent and processing biometric data.
180. Consent will be obtained from Staff and parents/carers for schools that use a biometric system or processing biometric data.
181. The biometric consent forms will provide information about the type and use of biometric data, the right to refuse or withdraw consent, and alternative arrangements for pupils whose data cannot be processed.
182. If someone objects or withdraws consent, any captured biometric data will be deleted within one month.
183. Biometric data will be managed and retained in accordance with the Abbey College Records Management Policy, and security measures will be implemented to protect the data.

Data retention

184. Data will not be kept for longer than is necessary.
185. Unrequired data will be deleted as soon as practicable.
186. Personal data will be retained and destroyed in line with the trust's Records Management Policy.
187. Some records relating to former pupils or employees of the establishment may be kept for an extended period for legal reasons, and to enable the provision of references or academic transcripts.
188. Personal data will be erased or securely destroyed once it is no longer to be retained.

Disclosure and Barring Service (DBS) data

189. All DBS data will be handled in line with data protection legislation.
190. 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.