ABBEY COLLEGE, RAMSEY

DATA PROTECTION & FREEDOM OF INFORMATION POLICY

Document Control

Committee:	Operations Committee
Approved By Committee On:	5th November 2019
Review Cycle:	2 Years
Date of Next Review:	Autumn term 2021
Staff member responsible for drafting and reviewing the policy:	Katie Dodsley

[1] This policy has been adapted from a policy originally developed by CMAT

Contents

The General Data Protection Regulation (GDPR) 3

1. Introduction 3
2. Definition Table 3
3. The Data Controller 4
4. Roles and Responsibilities 4
5. The data protection principles 5
6. Collecting personal data 6
7. Use of personal data by the academy 6
8. Security of personal data 8
9. Disclosure of personal data to third parties 8
10. Confidentiality of pupil concerns 9
11. Subject Access Requests 9
12. Exemptions to access by data subjects 10
13. Other rights of individuals 10
14. Breach of the GDPR legislation 12
15. Data security and Storage 13
16. Disposal of data 14
17. Training 14
18. Biometric systems 14
19. CCTV 14
20. Photographs and Videos 14
21. Contact 15

Freedom of Information 16

1. The Freedom of Information Act 16
2 Time limit for Compliance 16
3 How we deal with an FOI request 17
4 How to make an FOI request 18
5 How you can receive the information 18
6 If your request is turned down, what can you do about it? 18

Abbey College – Publication Scheme 19

Additional Information 20

The General Data Protection Regulation (GDPR)

1. Introduction

1.1. Abbey College collects and uses certain types of personal information about staff, pupils, parents and other individuals who come into contact with the Academy in order to provide education and associated functions. The Academy may be required by law to collect and use certain types of information to comply with statutory obligations related to employment, education and safeguarding, and this policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the General Data Protection Regulation and other related legislation.

1.2. The GDPR applies to all computerised data and manual files if they come within the definition of a filing system. Broadly speaking, a filing system is one where the data is structured in some way that it is searchable on the basis of specific criteria (so you would be able to use something like the individual's name to find their information), and if this is the case, it does not matter whether the information is located in a different physical location.

1.3. This policy will be updated as necessary to reflect best practice, or amendments made to data protection legislation, and shall be reviewed every two (2) years.

1.4. This policy meets the requirements of the GDPR and the 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. It 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.

1.5. It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of Biometric data

1.6. It also reflects the ICOs code of practice for the use of surveillance cameras and personal information

1.7. This policy complies with the regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the rights of access to their child's educational record

2. Definition Table

Term	Definition
Personal Data	'Personal data' is information that identifies an individual, and includes information that would identify an individual to the person to whom it is disclosed because of any special knowledge that they have or can obtain[1]. This may include • Name (including initials) • Identification Number • Location Data (Address) • Online Identifier (Username) It may also include factors specific to individuals physiological, genetic, mental, economic, cultural or social identity.

[1] This policy has been adapted from a policy originally developed by CMAT

Special Category (Sensitive Data)	A sub-set of personal data is known as 'special category personal data'. This special category data is information that relates to: • race or ethnic origin; • political opinions; • religious or philosophical beliefs; • trade union membership; • physical or mental health; • an individual's sex life or sexual orientation; • genetic or biometric data for the purpose of uniquely identifying a natural person. Special Category information is given special protection, and additional safeguards apply if this information is to be collected and used.
Data Subject	The identifiable individual whose personal data is processed or held
Data controller	The organisation that determines the purpose and the means of processing of personal data
Data processor	A person or organisation who processes personal data on behalf of the data controller (not including the data controller or an employee)
Processing	Anything done to personal data, such as collecting, organising, storing, altering, using, erasing or destroying. Processing data can be a manual or automated process
Data Protection Officer (DPO)	The CMAT Data Protection Officer is responsible for auditing the protection of data in the Academy, liaising with the ICO and responding to requests

3. The Data Controller

3.1. Abbey College processes personal data relating to parents, pupils, staff, governors, visitors and others and therefore is the data controller

3.2. Abbey College is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required

4. Roles and Responsibilities

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

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

4.3. The Business Manager and Headteacher act as representatives of the data controller on a day to day basis.

4.4. Data Protection Officer

4.4.1. The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring compliance with the data protection law, and developing related policies and guidelines where applicable

4.4.2. The DPO is the first point of contact for individuals and organisations.

4.4.3. The DPO will provide a report to the Operations committee for each meeting where relevant, reporting their advice, recommendations and any breaches.

4.4.4. Abbey College has appointed the CMAT DPO to act as its Data Protection Officer who can be contacted via dpo@cmatrust.net.

4.5. Staff are responsible for:

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

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

4.5.3. Contacting the DPO if they have any queries or questions regarding the use of and the protection of data within Abbey College, including;

4.5.3.1. Concerns that the policy is not being followed

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

4.5.3.3. If there has been a data breach

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

4.5.3.5. Whenever 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

4.5.3.6. If they need to apply a GDPR principle to processing data

5. The data protection principles

5.1. The GDPR is based on data protection principles that Abbey College must comply with:

5.1.1. personal data shall be processed fairly, lawfully and in a transparent manner, and processing shall not be lawful unless one of the processing conditions can be met;

5.1.2. Personal data shall be collected for specific, explicit, and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes;

5.1.3. personal data shall be adequate, relevant, and limited to what is necessary for the purpose(s) for which it is being processed;

5.1.4. personal data shall be accurate and, where necessary, kept up to date;

5.1.5. personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose / those purposes;

5.1.6. personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

5.2. In addition to this, Abbey College is committed to ensuring that at all times, anyone dealing with personal data shall be mindful of the individual's rights under the law (as explained in more detail in paragraphs 7 and 8 below).

5.3. Abbey College is committed to complying with the principles at all times.
This means that Abbey College will:

5.3.1. inform individuals as to the purpose of collecting any information from them, as and when we ask for it;

5.3.2. be responsible for checking the quality and accuracy of the information;

5.3.3. regularly review the records held to ensure that information is not held longer than is necessary, and that it has been held in accordance with the data retention policy;

5.3.4. ensure that when information is authorised for disposal it is done appropriately;

5.3.5. ensure appropriate security measures to safeguard personal information whether it is held in paper files or on our computer system, and follow the relevant security policy requirements at all times;

[1] This policy has been adapted from a policy originally developed by CMAT

5.3.6. share personal information with others only when it is necessary and legally appropriate to do so;
5.3.7. set out clear procedures for responding to requests for access to personal information known as subject access requests;
5.3.8. report any breaches of the GDPR in accordance with the procedure in paragraph 9 below.

6. Collecting personal data

6.1. Lawfulness, fairness and transparency

6.1.1. We will only process personal data where we have one of the 6 'lawful bases' (legal reasons) to do so under the data protection law:

6.1.1.1. The data needs to be processed so that Abbey College can fulfil a contract with the individual, or the individual has asked Abbey College to take specific steps before entering into a contract

6.1.1.2. The data needs to be processed so that Abbey College can comply with a legal obligation

6.1.1.3. The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life

6.1.1.4. The data needs to be processed so that Abbey College, as a public authority, can perform a task in the public interest, and carry out its official functions

6.1.1.5. The data needs to be processed for the legitimate interests of Abbey College or a third party (provided the individual's rights and freedoms are not overridden)

6.1.1.6. The individual (or their/parent when appropriate in the case of a pupil) has freely given clear consent

6.1.2. 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.

6.1.3. If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services)

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

6.2. Limitation, minimisation and accuracy

6.2.1. 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

6.2.2. 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

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

6.2.4. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with Abbey College's Records Management Policy and Retention Schedule.

7. Use of personal data by the academy

7.1. Abbey College holds personal data on pupils, staff and other individuals such as visitors. In each case, the personal data must be treated in accordance with the data protection principles as outlined in this policy.

Pupils

7.2. The personal data held regarding pupils includes contact details, assessment / examination results, attendance information, characteristics such as ethnic group, special educational needs, any relevant medical information, and photographs.

7.3. The data is used in order to support the education of the pupils, to monitor and report on their progress, to provide appropriate pastoral care, and to assess how well the academy as a whole is doing, together with any other uses normally associated with this provision in a school environment.

7.4. Abbey College may make use of limited personal data (such as contact details) relating to pupils, and their parents or guardians for fundraising, marketing or promotional purposes and to maintain relationships with pupils of the academy.

7.5. In particular, Abbey College may:

7.5.1. transfer information to any association society or club set up for the purpose of maintaining contact with pupils or for fundraising, marketing or promotional purposes relating to the academy but only where consent has been obtained first.

7.5.2. make personal data, including sensitive personal data, available to staff for planning curricular or extra-curricular activities;

7.5.3. keep the pupil's previous school informed of his / her academic progress and achievements e.g. sending a copy of the school reports for the pupil's first year at the Academy to their previous school;

7.5.4. Use photographs of pupils in accordance with the paragraph 20.

7.6. Any wish to limit or object to any use of personal data should be notified to the CMAT Data Protection Officer (DPO) in writing, which notice will be acknowledged by the Academy in writing. If, in the view of the DPO the objection cannot be maintained, the individual will be given written reasons why the Academy cannot comply with their request.

Staff

7.7. The personal data held about staff will include contact details, employment history, information relating to career progression, performance, information relating to DBS checks and photographs.

7.8. The data is used to comply with legal obligations placed on the Academy in relation to employment, and the education of children in a school environment. The Academy may pass information to other regulatory authorities where appropriate, and may use names and photographs of staff in publicity and promotional material. Personal data will also be used when giving references.

7.9. Staff should note that information about disciplinary action may be kept for longer than the duration of the sanction. Although treated as "spent" once the period of the sanction has expired, the details of the incident may need to be kept for a longer period.

7.10. Any wish to limit or object to the uses to which personal data is to be put should be notified to the CMAT Data Protection Officer (DPO) who will ensure that this is recorded, and adhered to if appropriate. If the DPO is of the view that it is not appropriate to limit the use of personal data in the way specified, the individual will be given written reasons why the Academy cannot comply with their request.

Other Individuals

[1] This policy has been adapted from a policy originally developed by CMAT

7.11. Abbey College may hold personal information in relation to other individuals who have contact with the school, such as volunteers and guests. Such information shall be held only in accordance with the data protection principles, and shall not be kept longer than necessary.

8. Security of personal data

8.1. Abbey College will take reasonable steps to ensure that members of staff will only have access to personal data where it is necessary for them to carry out their duties. All staff will be made aware of this Policy and their duties under the GDPR. Abbey College will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

8.2. For further details as regards security of IT systems, please refer to the IT Acceptable Use Policy.

9. Disclosure of personal data to third parties

9.1. The following list includes the most usual reasons that Abbey College will authorise disclosure of personal data to a third party:

9.1.1. Where we have outlined in our privacy notices;
9.1.2. Where there is an issue with a pupil or parent/carer that puts the safety of our staff or students at risk
9.1.3. To give a confidential reference relating to a current or former employee, volunteer or pupil;
9.1.4. for the prevention or detection of crime;
9.1.5. for the assessment of any tax or duty;
9.1.6. where it is necessary to exercise a right or obligation conferred or imposed by law upon the Academy (other than an obligation imposed by contract);
9.1.7. for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings);
9.1.8. for the purpose of obtaining legal advice;
9.1.9. for research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress);
9.1.10. to publish the results of public examinations or other achievements of pupils of the Academy;
9.1.11. to disclose details of a pupil's medical condition where it is in the pupil's interests to do so, for example for medical advice, insurance purposes or to organisers of school trips;
9.1.12. to provide information to another educational establishment to which a pupil is transferring;
9.1.13. to provide information to the Examination Authority as part of the examination process; and
9.1.14. to provide information to the relevant Government Department concerned with national education. At the time of the writing of this Policy, the Government Department concerned with national education is the Department for Education (DfE). The Examination Authority may also pass information to the DfE.

9.2. The DfE uses information about pupils for statistical purposes, to evaluate and develop education policy and to monitor the performance of the nation's education service as a whole. The statistics are used in such a way that individual pupils cannot be identified from them. On occasion the DfE may share the personal data with other Government Departments or agencies strictly for statistical or research purposes.

9.3. Abbey College may also share personal data with emergency services and local authorities to help them respond in an emergency that affects any of our pupils, staff, volunteers, governors or customers.

9.4. Abbey College may receive requests from third parties (i.e. those other than the data subject, the Academy, and employees of the Academy) to disclose personal data it holds about pupils, their parents or guardians, staff or other individuals. This information will not generally be disclosed unless one of the specific exemptions under data protection legislation which allow disclosure applies; or where necessary for the legitimate interests of the individual concerned or the Academy.

9.5. All requests for the disclosure of personal data must be sent to the Data Protection Officer (DPO) who will review and decide whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of that third party before making any disclosure.

10. Confidentiality of pupil concerns

10.1. Where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents or guardian, the Academy will maintain confidentiality unless it has reasonable grounds to believe that the pupil does not fully understand the consequences of withholding their consent, or where the Academy believes disclosure will be in the best interests of the pupil or other pupils.

10.2. The safety of the child within Abbey College's care is paramount. Abbey College's Child Protection policy will always override any confidentiality concerns.

11. Subject Access Requests

11.1. Anybody who makes a request to see any personal information held about them by Abbey College is making a subject access request. All information relating to the individual, including that held in electronic or manual files should be considered for disclosure, provided that they constitute a "filing system" (see clause 1.5).

11.2. All requests should be sent to the Data Protection Officer (DPO) within 3 working days of receipt, and must be dealt with in full without delay within 1 month of receipt.

11.3. Abbey College may tell the individual the request will be dealt 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.

11.4. Subject access requests must be submitted in writing, either by letter, email or fax to the Data Protection Officer There is a template available on the Abbey College website which includes:

11.4.1. Name of the individual

11.4.2. Correspondence address

11.4.3. Contact Number and email address

11.4.4. Details of the information requested

11.5. If staff receive a subject access request they must immediately forward the to the Data Protection Officer

11.6. Where a child or young person does not have sufficient understanding to make his or her own request (usually those under the age of 12, or over 12 but with a special educational need which makes understanding their information rights more difficult), a person with parental responsibility can make a request on their behalf. The DPO must, however, be satisfied that:

11.6.1. the child or young person lacks sufficient understanding; and
11.6.2. the request made on behalf of the child or young person is in their interests.

11.7. Any individual, including a child or young person with ownership of their own information rights, may appoint another person to request access to their records. In such circumstances Abbey College must have written evidence that the individual has authorised the person to make the application and the DPO must be confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates.

[1] This policy has been adapted from a policy originally developed by CMAT

11.8. Access to records will be refused in instances where an exemption applies, for example, information sharing may place the individual at risk of significant harm or jeopardise police investigations into any alleged offence(s).

11.9. Abbey College will provide the information free of charge, unless it is an unfounded or excessive request. If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which considers administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

11.10. The requester may be asked to provide 2 forms of identification to prove who they are and to allow the Abbey College to ensure they are eligible to access the information and to ensure information is not released to the wrong parties.

11.11. An individual only has the automatic right to access information about themselves, and care needs to be taken not to disclose the personal data of third parties where consent has not been given, or where seeking consent would not be reasonable, and it would not be appropriate to release the information. Particular care must be taken in the case of any complaint or dispute to ensure confidentiality is protected.

11.12. All files must be reviewed by the DPO before any disclosure takes place. Access will not be granted before this review has taken place.

11.13. Where all the data in a document or file cannot be disclosed a permanent copy should be made and the data obscured or retyped if this is more sensible. A copy of the full document and the altered document should be retained, with the reason why the document was altered.

12. Exemptions to access by data subjects

12.1. 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.

12.2. 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.

12.3. Abbey College will not disclose information if it:

12.3.1. Might cause serious harm to the physical or mental health of the individual or another individual

12.3.2. 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

12.3.3. Is detailed in the court orders

12.3.4. Is information where disclosure would result in revealing personal information about another pupil, staff member, volunteer or visitor

13. Other rights of individuals

13.1. Abbey College has an obligation to comply with the rights of individuals under the law, and takes these rights seriously. The following section sets out how the academy will comply with the rights to:

13.1.1.1. object to Processing;

13.1.1.2. rectification;

13.1.1.3. erasure; and

13.1.1.4. data Portability.

13.2. 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

Right to object to processing

13.3. An individual has the right to object to the processing of their personal data on the grounds of pursuit of a public interest or legitimate interest (grounds 4.5 and 4.6 above) where they do not believe that those grounds are made out.

13.4. Where such an objection is made, it must be sent to the DPO within 2 working days of receipt, and the DPO will assess whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the individuals, or whether the information is required for the establishment, exercise or defence of legal proceedings.

13.5. The DPO shall be responsible for notifying the individual of the outcome of their assessment within 30 working days of receipt of the objection.

Right to rectification

13.6. An individual has the right to request the rectification of inaccurate data without undue delay. Where any request for rectification is received, and where adequate proof of inaccuracy is given, the data shall be amended as soon as reasonably practicable, and the individual notified.

13.7. Where there is a dispute as to the accuracy of the data, the DPO should be notified within 2 days of receipt. The request and reasons for refusal shall be noted alongside the data, and communicated to the individual by the Data Protection Officer (DPO). The individual shall be given the option of a review under the complaints procedure, or an appeal direct to the Information Commissioner.

13.8. An individual also has a right to have incomplete information completed by providing the missing data, and any information submitted in this way shall be updated without undue delay.

Right to erasure

13.9. Individuals have a right, in certain circumstances, to have data permanently erased without undue delay. This right arises in the following circumstances:

13.9.1. where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed;
13.9.2. where consent is withdrawn and there is no other legal basis for the processing;
13.9.3. where an objection has been raised under the right to object, and found to be legitimate;
13.9.4. where personal data is being unlawfully processed (usually where one of the conditions for processing cannot be met);
13.9.5. where there is a legal obligation on Abbey College to delete.

13.10. The DPO will make a decision regarding any application for erasure of personal data, and will balance the request against the exemptions provided for in the law. Where a decision is made to erase the data, and this data has been passed to other data controllers, and / or has been made public, reasonable attempts to inform those controllers of the request shall be made.

Right to restrict processing

13.11. In the following circumstances, processing of an individual's personal data may be restricted:

13.11.1. where the accuracy of data has been contested, during the period when the Academy is attempting to verify the accuracy of the data;

[1] This policy has been adapted from a policy originally developed by CMAT

13.11.2. where processing has been found to be unlawful, and the individual has asked that there be a restriction on processing rather than erasure;

13.11.3. where data would normally be deleted, but the individual has requested that their information be kept for the purpose of the establishment, exercise or defence of a legal claim;

13.11.4. where there has been an objection made under para 8.2 above, pending the outcome of any decision.

Right to portability

13.12. If an individual wants to send their personal data to another organisation they have a right to request that Abbey College provides their information in a structured, commonly used, and machine readable format. As this right is limited to situations where Abbey College is processing the information on the basis of consent or performance of a contract, the situations in which this right can be exercised will be quite limited. If a request for this is made, it should be forwarded to the DPO within 2 working days of receipt, and the DPO will review and revert as necessary.

14. Breach of the GDPR legislation

14.1. Any and all breaches of the GDPR, including a breach of any of the data protection principles shall be reported as soon as it is discovered, to the Data Protection Officer (DPO).

14.2. Once notified, the DPO shall assess:

14.2.1. the extent of the breach;

14.2.2. the risks to the data subjects as a consequence of the breach;

14.2.3. any security measures in place that will protect the information;

14.2.4. any measures that can be taken immediately to mitigate the risk to the individuals.

14.3. Unless the DPO concludes that there is unlikely to be any risk to individuals from the breach, it must be notified to the Information Commissioner's Office within 72 hours of the breach having come to the attention of the Abbey College, unless a delay can be justified.

14.4. The Information Commissioner shall be told:

14.4.1. details of the breach, including the volume of data at risk, and the number and categories of data subjects;
14.4.2. the contact point for any enquiries (which shall usually be the DPO);
14.4.3. the likely consequences of the breach;
14.4.4. measures proposed or already taken to address the breach.

14.5. If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals then the DPO shall notify data subjects of the breach without undue delay unless the data would be unintelligible to those not authorised to access it, or measures have been taken to mitigate any risk to the affected individuals.

14.6. Data subjects shall be told:
14.6.1. the nature of the breach;
14.6.2. who to contact with any questions;
14.6.3. measures taken to mitigate any risks.

14.7. The DPO shall then be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented. Any recommendations for further training or a change in procedure shall be reviewed by the Executive Principals Board and the Directorate Board and a decision made about implementation of those recommendations.

15. Data security and Storage

15.1. Abbey College will protect data from unauthorised or unlawful access, processing or disclosure and against accidental or unlawful loss, destruction, communication or damage.

15.2. Abbey College will ensure that:
15.2.1. Paper records and portable electronic devices (such as laptops and storage devices) that contain personal data are kept locked away when not in use
15.2.2. Documents containing confidential personal data will not be left on display in offices/classrooms, in staffrooms, pinned to display boards or left anywhere where there is general public access
15.2.3. Personal data, where displayed in classrooms will confirm to protection guidelines regarding sensitive information and the approval of its use
15.2.4. Where personal data is displayed in a room where members of the public are invited, information will be hidden out of view or covered when not in use
15.2.5. Where Abbey College owned personal data needs to be taken off site, this must be done with the consent of the data controller and/or the DPO
15.2.6. IT system passwords will be strong and changed regularly
15.2.7. Encryption software is used to protect all laptops
15.2.8. Staff, pupils, governors or other volunteer who stores or processes personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment, as per the IT Policy
15.2.9. Staff, governors and other volunteers are not permitted to remove/copy/download/publish/print data from an Abbey College device or system without the explicit permission from a member of the Executive Principals or the Directorate board. Data must stay on Abbey College owned devices and may only be accessed on personal devices using an approved method as described in the IT Policy.
15.2.10. Where data is shared with a third party, Abbey College will carry out due diligence and take reasonable steps to ensure it is stored and transmitted securely
15.2.11. Where a member of staff no longer works for Abbey College, they will be asked to permanently delete any personal data they may hold on staff, students or parents and return any IT hardware or software provided by Abbey College. To be clear this includes but is not exclusive to:

[1] This policy has been adapted from a policy originally developed by CMAT

markbooks, registers, pupil reports, assessment/attainment data, child protection/ safeguarding records and photos of students.

16. Disposal of data

16.1. Personal data that is no longer needed will be disposed of securely. Data that has become inaccurate or out of date will be updated if we have a legal basis to maintain it, or deleted if not longer needed.

16.2. The disposal of data will be undertaken in accordance with the Abbey College's data retention policy.

16.3. Data marked for disposal will be securely destroyed, by shredding for paper based records. Abbey College may use a third party to safely dispose of records on their behalf, ensuring that the third party complies with the data protection law.

17. Training

17.1. All staff, trustees and academy councillors are provided with data protection training as part of their induction.

17.2. Data protection training is also part of the CPD process for staff each year.

17.3. Where significant changes are applied to legislation, Abbey College will make the necessary training available to ensure all staff are updated.

18. Biometric systems

18.1. Where Abbey College uses pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger scans to receive school dinners instead of paying with cash) it will comply with the requirements of the Protection of Freedoms Act 2012.

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

18.3. Parents/carers and pupils have the right to choose not to use the biometric system(s). Abbey College will provide alternative means of accessing the relevant services for those pupils.

18.4. Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and the academy will make sure that any relevant data already captured is deleted. As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, the academy will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

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

19. CCTV

19.1. Abbey College uses CCTV in various locations to ensure the staff, students and site resources remain safe and secure.

19.2. Abbey College does not need to ask individuals' permission to use CCTV, however it should ensure clear signage informing users that the site has CCTV and how to ask for more information.

19.3. Further information is available within the Abbey College's CCTV policy.

20. Photographs and Videos

20.1. As part of Abbey College activities, we may take photographs and record images of individuals.

20.2. We will obtain written consent from parents/carers, or pupils, for photographs and videos to be taken of them/their child for communication, marketing and promotional materials.

20.3. Where we need parental consent, we will clearly explain how the photograph and/or video will be used to the parent/carer or pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used. Uses may include:

20.3.1. Within the Academy notice boards and in the Academy magazines, brochures/prospectus, newsletters, etc

20.3.2. Outside of academy by external agencies such as Academy photographer, newspapers, campaigns

20.3.3. Online within our Academy website or social media pages

20.4. Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute further

20.5. When using photographs and videos will not accompany them with any other personal information about the child, to reduce the risk of them being identified

20.6. See our child protection and safeguarding policy for more information on our use of photographs and videos

20.7. We will not ask for any sensitive data within our sign-in system other than individuals name & car registration which we ask as part of Health & Safety. We may be asked to support government authorities within any legal investigations, which may require us to provide this information.

21. Contact

21.1. If anyone has any concerns or questions in relation to this policy, they should contact the Data Protection Officer.
Data Protection Officer at CMAT, by email dpo@cmatrust.net or write to Data Protection Officer, CMAT, CMAT Offices, Fen Lane, Sawtry, PE28 5TQ

If at any time you are not happy with how we are processing your personal information then you may raise the issue with the Data Protection Officer and if you are not happy with the outcome you may raise a complaint with the Information Commissioner's Office:

Information Commissioner's Office
Wycliffe House
Water Lane,
Wilmslow, Cheshire,
SK9 5AF
Tel: 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate number.

[1] This policy has been adapted from a policy originally developed by CMAT

Freedom of Information

1. The Freedom of Information Act

1.1 Abbey College is subject to the Freedom of Information Act 2000 (FOI) as a public authority, and as such, must comply with any requests for information in accordance with the principles laid out in the Act.

1.2 The Freedom of Information Act gives you the right to ask us for all the recorded information we have on any subject. Anyone can make a request for information – there are no restrictions on your age, nationality or where you live. Your request will be handled under the Data Protection Act if you ask for information about yourself.

1.3 Any request for any information from the Academy is technically a request under the FOI, whether or not the individual making the request mentions the FOI. However, the ICO has stated that routine requests for information (such as a parent requesting a copy of a policy) can be dealt with outside of the provisions of the Act.

1.4 In all non-routine cases, if the request is simple and the information is to be released, then the individual who received the request can release the information, but must ensure that this is done within the timescale set out below. A copy of the request and response should then be sent to the DPO.

1.5 All other requests should be referred in the first instance to the DPO who may allocate another individual to deal with the request. This must be done promptly, and in any event within 3 working days of receiving the request.

1.6 When considering a request under FOI, you must bear in mind that release under FOI is treated as release to the general public, and so once it has been released to an individual, anyone can then access it, and you cannot restrict access when releasing by marking the information "confidential" or "restricted".

2 Time limit for Compliance

2.1 The Academy must respond as soon as possible, and in any event, within 20 working days of the date of receipt of the request. For an Academy, a "working day" is one in which pupils are in attendance, subject to an absolute maximum of 60 calendar days to respond.
Details of what constitutes a "working day" should be defined from the term dates provided on each Academy website.

3 How we deal with an FOI request

3.1 When a request is received that cannot be dealt with by simply providing the information, it should be referred in the first instance to the DPO, who may re-allocate to an individual with responsibility for the type of information requested.

3.2 The first stage in responding is to determine whether or not the Academy "holds" the information requested. The Academy will hold the information if it exists in computer or paper format. Some requests will require the Academy to take information from different sources and manipulate it in some way. Where this would take minimal effort, the Academy is considered to "hold" that information, but if the required manipulation would take a significant amount of time, the requestor should be contacted to explain that the information is not held in the manner requested, and offered the opportunity to refine their request. For example, if a request required the Academy to add up totals in a spreadsheet and release the total figures, this would be information "held" by the Academy. If the Academy would have to go through a number of spreadsheets and identify individual figures and provide a total, this is likely not to be information "held" by the Academy, depending on the time involved in extracting the information.

3.3 The second stage is to decide whether the information can be released, or whether one of the exemptions set out in the Act applies to the information. Common exemptions that might apply include:

3.3.1 Section 40 (1) – the request is for the applicants' personal data. This must be dealt with under the subject access regime in the DPA, detailed in paragraph 9 of the DPA policy;

3.3.2 Section 40 (2) – compliance with the request would involve releasing third party personal data, and this would be in breach of the DPA principles as set out in paragraph 3.1 of the DPA policy above;

3.3.3 Section 41 – information that has been sent to the Academy (but not the Academy's own information) which is confidential;

3.3.4 Section 21 – information that is already publicly available, even if payment of a fee is required to access that information;

3.3.5 Section 22 – information that the Academy intends to publish at a future date;

3.3.6 Section 43 – information that would prejudice the commercial interests of the Academy and / or a third party;

3.3.7 Section 38 – information that could prejudice the physical health, mental health or safety of an individual (this may apply particularly to safeguarding information);

3.3.8 Section 31 – information which may prejudice the effective detection and prevention of crime – such as the location of CCTV cameras;

3.3.9 Section 36 – information which, in the opinion of the chair of governors of the Academy, would prejudice the effective conduct of the Academy. There is a special form for this on the ICO's website to assist with the obtaining of the chair's opinion.

3.4 The sections mentioned in italics are qualified exemptions. This means that even if the exemption applies to the information, you also have to carry out a public interest weighting exercise, balancing the public interest in the information being released, as against the public interest in withholding the information.

[1] This policy has been adapted from a policy originally developed by CMAT

4 How to make an FOI request

4.1 You can contact us directly by letter to CMAT DPO, CMAT Offices, Fen Lane, Sawtry, PE28 5TQ or by email to dpo@cmatrust.net to make a freedom of information (FOI) request.

4.2 When making your request, you should include:
- your name
- an address where you can be contacted (including e-mail)
- a detailed description of the recorded information you want

5 How you can receive the information

5.1 You can ask for the information in a number of different formats:
- paper or electronic copies of any documents
- audio format
- large print

5.2 Make sure you check the copyright status of the information you receive if you plan to reproduce it. It is your responsibility to check this. Abbey College, CMAT or any representative shall not be held liable for your failure to check this.

6 If your request is turned down, what can you do about it?

6.1 Some sensitive information might not be available to members of the public. If this is the case, we will tell you why we have withheld some or all of the information you requested.

6.2 We can turn down your request if we think it will cost them more than £450 to deal with your request.

6.3 We might ask you to be more specific so we can provide the information you're looking for.
If we don't provide you with the information you request, you should first contact us asking us to review our decision. If you are still not satisfied, you can complain to the Information Commissioner's Office. – www.ico.org.uk

Abbey College's – Publication Scheme

A publication scheme is a document which describes the information a public authority publishes, or intends to publish.

In this context, 'publish' means to make information available, routinely. These descriptions are called 'classes of information'. The scheme is not a list of the actual publications, because this will change as new material is published or existing material revised. It is, however, the public authority's commitment to make available the information described.

A publication scheme must set out the classes, or categories, of information published. It must also make clear how the information described can be accessed and whether or not charges will be made.

Abbey College is adopting the model publication scheme developed for Academies within the UK education sector and is therefore committed to publishing the information it describes.

The model is designed for Academies across England, Wales and Northern Ireland.

The purpose of the model is to save institutions duplicating effort in producing individual schemes and to assist the public in accessing information from across the sector. However, to reflect the diversity in size and function of an institution, a number of optional classes of information are included.

As a result, models within the sector will vary slightly. Any option classes relevant to us have been included in our scheme. Details of our policy will be published on the website in the near future.

[1] This policy has been adapted from a policy originally developed by CMAT

Additional Information

Contact details:

FOI Request
The Data Protection Officer
Cambridge Meridian Academies Trust
CMAT Offices
Fen Lane, Sawtry, PE28 5TQ

Or by email to : DPO@cmatrust.net

Contact details for all of our academies can be found here: https://www.cmatrust.co.uk/our-schools/