Abbey College

Data Protection Policy Header

Policy Review frequency: At least every two years (last Reviewed Jan 2017)

Governors to review in May 2018 - following the implementation of General Data Protection Regulation (GDPR)

Legislation: The Data Protection Act 1998 with consideration to the eight data protection principles.

Approval: Governing body free to determine how to implement.

Schools are 'Data Controllers' under the Data Protection Act 1998 and must 'Notify' (register with), the Information Commissioner's Office. Registration is annual.

Information Commissioner's Office Registration Number: Z290129X

Date Registered: 19 October 2011 Registration Expires: **18 October 2018**

Data Controller: ABBEY COLLEGE, RAMSEY (Trustees and Governors)

Address:
ABBEY ROAD
RAMSEY
HUNTINGDON
CAMBRIDGESHIRE
PE26 1DG

This register entry describes, in very general terms, the personal data being processed by:

ABBEY COLLEGE RAMSEY

Nature of work - Education Academy

Description of processing

The following is a broad description of the way this organisation/data controller processes personal information. To understand how your own personal information is processed you may need to refer to any personal communications you have received, check any privacy notices the organisation has provided or contact the organisation to ask about your personal circumstances.

Reasons/purposes for processing information

We process personal information to enable us to provide education, training, welfare and educational support services; to administer school property; to maintain our own accounts and records; to undertake fundraising and to support and manage our employees. We also use CCTV for security and the prevention and detection of crime.

Type/classes of information processed

We process information relevant to the above reasons/purposes. This may include:

- personal details
- family details
- lifestyle and social circumstances
- education and employment details
- financial details
- goods and services
- disciplinary and attendance records
- vetting checks
- visual images, personal appearance and behaviour

We also process sensitive classes of information that may include:

- physical or mental health details
- racial or ethnic origin
- religious or other beliefs
- trade union membership
- sexual life
- information about offences and alleged offences

Who the information is processed about

We process personal information about:

- employees
- students
- professional experts and advisers
- members of school boards
- sponsors and supporters
- suppliers and service providers
- complainants, enquirers
- individuals captured by CCTV images

Who the information may be shared with

We sometimes need to share the personal information we process with the individual themself and also with other organisations. Where this is necessary we are required to comply with all aspects of the Data Protection Act (DPA). What follows is a description of the types of organisations we may need to share some of the personal information we process with for one or more reasons. Where necessary or required we share information with:

- family, associates and representatives of the person whose personal data we are processing
- educators and examining bodies
- careers service
- school boards
- local and central government
- academy trusts
- healthcare, social and welfare organisations
- police forces, courts
- current, past or prospective employers
- voluntary and charitable organisations
- business associates, professional advisers
- suppliers and service providers
- financial organisations
- press and the media

Transfers

It may sometimes be necessary to transfer personal information overseas. When this is needed information may be transferred to countries or territories around the world. Any transfers made will be in full compliance with all aspects of the Data Protection Act.

Data Protection Policy

This document is a statement of the aims and principles of the Academy, for ensuring the confidentiality of sensitive information relating to staff, pupils, parents and governors.

Introduction

Abbey College needs to keep certain information about its employees, students and other users to allow it to monitor performance, achievements, safeguarding and health and safety, for example. It is necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with.

To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, Abbey College must comply with the 8 Data Protection Principles which are set out in the Data Protection Act 1998. In summary these state that:

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Abbey College and all staff or others who process or use personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the Academy has developed this Data Protection Policy.

Status of this Policy

This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the Academy from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

The Data Controller and the Designated Data Controllers

The Academy as a body incorporate the Data Controller under the 1998 Act, and the Academy Trustees and Governors are therefore ultimately responsible for implementation. However, the Designated Data Controllers will deal with day to day matters.

The Academy has 2 Designated Data Controllers: They are the Headteacher and the Director of Operations.

Any member of staff, parent or other individual who considers that the Policy has not been followed in respect of personal data about himself or herself or their child should raise the matter with the appropriate Designated Data Controller, who would be the Director of Operations.

Responsibilities of Staff

All staff are responsible for:

- Checking that any information that they provide to the Academy in connection with their employment is accurate and up to date.
- Informing the Academy of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently. The Academy cannot be held responsible for any errors unless the staff member has informed the Academy of such changes.

If and when, as part of their responsibilities, staff collect information about other people (e.g. about a student's course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines for staff set out in this policy.

Data Collection

There should be a valid purpose for collecting the information, and if there is a possibility that we might want to use the data at a later date for a different purpose, then we should inform the individual. If the purpose for collecting the data is for marketing reasons, then the individual should be given the opportunity to opt out.

When collecting personal data, consider the following:

- Would the person know why you are collecting that particular personal information, and if they fully knew the implications of it, would they object?

In the case of sensitive personal data, the positive informed consent of the individual may need to be gained.
The collection of personal data may, however, be essential if we are to provide the service or carry out the transaction that the individual has requested or requires. In those cases seeking consent is meaningless. It is, though, good practice to give as much information to the person concerned as possible.
If the data is to be released to an external organisation or person, whether it be as a matter of routine, or on request for safeguarding purposes, it may be necessary to get the individual's consent.

Data Security

All staff are responsible for ensuring that:

- Any personal data that they hold is kept securely.
- Personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Personal information should be kept in a locked filing cabinet, drawer, or safe; or if it is computerised, and stored on a local hard drive and on a network drive that is regularly backed up, be coded, encrypted or password protected.

- If a copy is kept on a removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

Rights to Access Information

All staff, parents and other users are entitled to:

- Know what information the Academy holds and processes about them or their child and why.

  The Academy will, upon request, provide all staff and parents and other relevant users with a statement regarding the personal data held about them. This will state all the types of data the Academy holds and processes about them and the reasons for which they are processed. Subject to safeguarding disclosure or other legislation.
- Know how to gain access to it.

  All staff, parents and other users have a right under the 1998 Act to access certain personal data being kept about them or their child either on computer or in certain files. Any person who wishes to exercise this right should make a Subject Access Request to the Designated Data Controller.
- Know how to keep it up to date.

  Parents, staff and other users are responsible for advising the Academy of any changes to their personal information held by the Academy.

  Staff and other users are required to fulfil their obligation to check and update information following Academy policies and processes.
- Know what the Academy is doing to comply with its obligations under the 1998 Act.

  This Policy document identifies what the Academy is doing to comply with its obligations under the 1998 Act.

The Academy will make a charge of £10 on each occasion that access is requested, although the Academy has discretion to waive this. The Academy aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days, as required by the 1998 Act.

Subject Consent

In many cases, the Academy can only process personal data with the consent of the individual.

In some cases, if the data is sensitive, as defined in the 1998 Act, express consent must be obtained. Agreement to the Academy processing some specified classes of personal data is a condition of employment for staff. This includes information about previous criminal convictions.

Jobs will bring the applicants into contact with children. The Academy has a duty under the Children Act 1989 and other enactments to ensure that staff are suitable for the job. The Academy has a duty of care to all staff and students and must therefore make sure that employees and those who use Academy facilities do not pose a threat or danger to other users.

The Academy may also ask for information about particular health needs, such as allergies to particular forms of medication, or any medical condition such as asthma or diabetes. The Academy will only use this information in the protection of the health and safety of the individual, but will need consent to process this data in the event of a medical emergency, for example.

Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, or race. This may be to ensure that the Academy is a safe place for everyone, or to operate other Academy policies, such as the Sick Pay Policy or the Equal Opportunities Policy. Because this information is considered sensitive under the 1998 Act, staff (and students where appropriate) will be asked to give their express consent for the Academy to process this data. An offer of employment may be withdrawn if an individual refuses to consent to this without good reason.

Publication of Academy Information

Certain items of information relating to Academy staff will be made available via searchable directories on the public Website, in order to meet the legitimate needs of researchers, visitors and enquirers seeking to make contact with the Academy.

Retention of Data

The Academy has a duty to retain some staff and student personal data for a period of time following their departure from the Academy, mainly for legal reasons, but also for other purposes such as being able to provide references or academic transcripts. Different categories of data will be retained for different periods of time.

Conclusion

Compliance with the 1998 Act is the responsibility of all members of the Academy. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or even to a criminal prosecution.

Governors to review in May 2018 - following the implementation of General Data Protection Regulation (GDPR)