

Data Protection Policy

Birchwood Community Academy Trust

Policy owner (Name):	Alan O'Reilly
Policy owner (Job Title):	School Business Manager
Governing body oversight:	Policy Review Committee
Date of approval:	
Date of next review:	

Eight data protection principles

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be obtained only for one or more specified and lawful purposes.
3. Personal data shall be adequate, relevant and not excessive.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purposes shall not be kept for longer than is necessary.
6. Personal data shall be processed in accordance with the rights of data subjects.
7. Personal data shall be protected against unauthorised or unlawful access or processing.
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 data protection.

Policy statement

9. Birchwood Community Academy Trust (BCAT) is committed to maintaining the eight principles above at all times. The trust will:
 - Inform individuals why the information is being collected when it is collected
 - Inform individuals when their information is shared, and why and with whom it was shared
 - Check the quality and the accuracy of the information it holds
 - Ensure that information is not retained for longer than is necessary
 - Ensure that when obsolete information is destroyed that it is done so appropriately and securely
 - Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
 - Share information with others only when it is legally appropriate to do so
 - Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests
 - Ensure all staff are aware and understand the trust's policies and procedures

Scope and purpose

10. This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act. It covers the collection, storing, editing, retrieving, disclosure, archiving, and destruction of personal data including electronic data

(emails, databases, biometric data, videos, photos, and electronic files and records), paper files or other formats (such as photos and microfiche).

Registration with information commissioner's office (ICO)

11. Data protection laws are enforced in the UK by the Information Commissioner's Office ("ICO"). The academy maintains a notification with the ICO which sets out how it processes personal data and for what purposes. Our notification can be viewed by visiting <https://ico.org.uk/ESDWebPages/Entry/ZA015563> and the academy's registration number is ZA015563.

Privacy Notice

12. The academy provides a Privacy Notice to all individuals from whom it collects personal data. The Privacy Notice informs individuals of the following:
- The academy is responsible for the processing of their personal data
 - The purposes for which personal data provided to the academy will be used
 - Information on any disclosures or transfers of that information to third parties
13. The academy's privacy notice is available on its website in the Our Policies section or by visiting https://docs.wixstatic.com/ugd/94bb20_d35a20af90584405b152438392594773.pdf

Data storage

14. Personal Data will be stored in a secure and safe manner. The following measures are taken to help ensure this:
- electronic data will be protected through secure password, encryption software and firewall systems operated by the academy.
 - PC, laptop and tablet workstations will be positioned so that they are not visible to casual observers.
 - Paper files including personal data will be stored securely away from anyone that does not have a legitimate reason to view or process the data.
 - Particular attention will be paid to the need for security of sensitive personal data, for example, health and medical records or child protection information will be kept in a locked cupboard.
 - Personal data will not be left out visible on desks
 - the physical security of academy buildings and storage systems will be regularly reviewed.
 - Staff will be trained on this policy and related data protection procedures.

The academy retains acknowledges that it retains responsibility for processing and storage of personal data using cloud services and will only do so where a written contract is in place with a supplier and sufficient guarantees have been received in respect of the technical and organisational security measures.

Data disclosure

15. Personal data will only be disclosed to organisations or individuals for whom consent has been given to receive their data, or organisations that have a legal right to receive the data without consent being given.
16. When requests to disclose personal data are received by telephone, the academy will ensure that the caller is entitled to receive the data and that they are who they say they are. In some circumstances the academy may call the caller back to check the identity of the caller.
17. Personal data will not be included on the website, social media, in newsletters or to other media without consent of the individual (or his/her parents where appropriate). Routine consent may be requested from parents to avoid the need for frequent, similar requests for consent being made by the academy.
18. Personal data will only be disclosed to the police if they are able to supply a WA170 form which notifies of a specific, legitimate need to have access to specific personal data.

Subject access request procedures

19. Any individual whose personal data is held by the academy is entitled to ask for this information. This is known as a subject access request in the Data Protection Act. The request must be made in writing and the right is to view or be given a copy of the personal data, rather than to the whole document which contains their personal data.
20. There are some exceptions to this right of access such as to examination scripts and legal advice.
21. When a subject access request is received by a member of staff, it should be passed to the academy's Data Protection Officer without delay. A response must be provided as soon as possible and no later than within 40 calendar days from the date the request was received.
22. The academy may make a charge of £10 for responding to a request for personal data under the Data Protection Act and will need to confirm the requester's identity. Parents can make data subject access requests on their child's behalf if their children are deemed too young to look after their own affairs.

Use of CCTV

23. CCTV is used on academy premises to promote the safety and welfare of all individuals accessing the facilities. Images of people are covered by the Data Protection Act, this includes the information that can be derived from images. The CCTV system will only capture images of individuals and will not be used for audio recording.
24. All reasonable steps will be taken to ensure that individuals are aware that CCTV is in operation in specific areas.

25. Cameras have been sited so that they provide clear images and so that they avoid capturing the images of individuals whom it is not intended to capture. Regular checks will be carried out to ensure that the system is working properly and produces high quality images, this will include a check that the date and time stamp recorded on the images is accurate.
26. Images from the CCTV system are securely stored and only a limited number of authorised personnel may have access to them. The viewing of live images on monitors will be restricted to the operator unless the monitor displays a scene which is also in plain sight from the monitor location.
27. The images will, in most instances, not be provided to any third parties with the exception of law enforcement bodies. Requests for copies of an individual's own images will be dealt with as a Subject Access Request as detailed elsewhere in this policy. We have discretion to refuse any request for information unless there is an overriding legal obligation to do so. If images are disclosed then the method of disclosing them will be secure, ensuring that they are only seen by the intended recipient.
28. Once there is no reason to retain the recorded images, they will be deleted. The recorded images will only be retained long enough for:
 - Any incident to come to light
 - And the incident to be investigated

Appendix One: Some Helpful Definitions from the Data Protection Act

<p>Data means information which –</p> <ul style="list-style-type: none">a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,b) is recorded with the intention that it should be processed by means of such equipment,c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68, ore) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).
<p>Personal data means data which relate to a living individual who can be identified –</p> <ul style="list-style-type: none">a) from those data, orb) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.
<p>Sensitive personal data means personal data consisting of information as to -</p> <ul style="list-style-type: none">a) the racial or ethnic origin of the data subject,b) his political opinions,c) his religious beliefs or other beliefs of a similar nature,d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),e) his physical or mental health or condition,f) his sexual life,g) the commission or alleged commission by him of any offence, orh) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.
<p>Processing, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including –</p> <ul style="list-style-type: none">a) organisation, adaptation or alteration of the information or data,b) retrieval, consultation or use of the information or data,c) disclosure of the information or data by transmission, dissemination or otherwise making available, ord) alignment, combination, blocking, erasure or destruction of the information or data.
<p>Data subject means an individual who is the subject of personal data.</p>
<p>Data controller means ... a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.</p>
<p>Data processor, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.</p>