DATA PROTECTION POLICY
INCLUDING DATA BREACH POLICY AND RESPONSE PROCEDURE

RESPONSIBLE DIRECTOR

Chief Executive Officer

RATIFIED BY BOARD

October 2023

REVIEW DATE

September 2026

Our Vision
"The BCAT vision is to support students to achieve their absolute best whatever their ability or background. We aim to:

1. Work collaboratively to deliver an inclusive and outstanding education to all students, thereby driving up local standards.
2. Maximise social mobility and life chances, through the highest expectations of and aspirations for all students.
3. Encourage and support a range of high performing and distinctive educational establishments for local communities."

Our Values
Student focus - We will seek to achieve a high quality learning experience for every student.
High performance - We will strive for consistently high levels of performance in all aspects of our work.
Respect, openness and honesty - We will treat everyone with respect, encourage openness and honesty, and recognise each other's contribution and achievements.

1. Aims

Our schools aim to ensure that all personal data collected about staff, pupils, parents, board members, LAB members, visitors and other individuals is collected, stored and processed in accordance with the Data Protection Legislation which means the Data Protection Act 2018 (DPA 2018), the United Kingdom General Data Protection Regulation (UK GDPR), the Privacy and Electronic Communications (EC Directive)

Regulations 2003 and any legislation implemented in connection with the aforementioned legislation. Where data is processed by a controller or processor established in the European Union or comprises the data of people in the European Union, it also includes the EU General Data Protection Regulation (EU GDPR). This includes any replacement legislation coming into effect from time to time.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the UK GDPR and the expected 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 also reflects the ICO's code of practice for the use of surveillance cameras and personal information. In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental · • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

BCAT schools process personal data relating to parents, pupils, staff, LAB members, visitors and others, and therefore is a data controller.

Each school is registered as a data controller with the ICO and will renew this registration as legally required.

5. Roles and responsibilities

This policy applies to all staff employed by our schools, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 BCAT Board

The board has overall responsibility for ensuring that both schools comply with all relevant data protection obligations.

5.2 Data protection officer

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

They will provide an annual report of their activities directly to the Trust board and, where relevant, report to the board their advice and recommendations on school data protection issues. Our DPO is Natalie Robertson, Trust HR and Governance Manager contactable via email on nrobertson@bcat.co.uk.

5.3 Principal/Headteacher

The Principal/Headteacher act as the representative of the data controller on a day-to-day basis.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure.
    - If they have any concerns that this policy is not being followed.
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way.
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK.
    - If there has been a data breach.
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals.

- If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The GDPR is based on data protection principles that our schools must comply with.

The principles state that personal data must be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed.
- Accurate and, where necessary, kept up to date.
- Kept for no longer than is necessary for the purposes for which it is processed.
- Processed in a way that ensures it is appropriately secure.

This policy sets out how the schools aim to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

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

- The data needs to be processed so that the school can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract.
- The data needs to be processed so that the school can comply with a legal obligation.
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life.
- The data needs to be processed so that the school, as a public authority, can perform a task in the public interest, and carry out its official functions.
- The data needs to be processed for the legitimate interests of the school or a third party (provided the individual's rights and freedoms are not overridden).
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent.

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK GDPR and Data Protection Act 2018.

7.2 Limitation, minimisation and accuracy

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.

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.

Staff must only process personal data where it is necessary in order to do their jobs. 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 the school's record retention schedule.

8. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk.
- We need to liaise with other agencies – we will seek consent as necessary before doing this.
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law.
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share.
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

We routinely share pupil information with:

- schools that the pupils attend after leaving us.
- our local authority.
- the Department for Education (DfE).

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

Subject access requests can be submitted in writing, either by letter, email or fax to the Data Protection Officer. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

Appendix A of this document contains a Data Subject Access request form and associated guidance. This form is not mandatory and subject access requests made in other formats will be accepted, but the form is designed to help the requester in providing us with the information we need to process the request in the swiftest possible manner.

If staff receive a subject access request, they must immediately forward it to the Data Protection Manager/Lead.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore,

most subject access requests from parents or carers of pupils at a Trust Primary School may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification.
- May contact the individual via phone to confirm the request was made.
- Will respond without delay and within 1 month of receipt of the request.
- Will provide the information free of charge.
- May tell the individual we will comply 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.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual.
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests.
- Is contained in adoption or parental order records.
- Is given to a court in proceedings concerning the child.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account 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.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time.
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances).
- Prevent use of their personal data for direct marketing.
- Challenge processing which has been justified on the basis of public interest.

- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area.
- Object to decisions based solely on automated decision making or profiling. (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress.
- Be notified of a data breach in certain circumstances.
- Make a complaint to the ICO.
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

Individuals should submit any request to exercise these rights to the Data Protection Officer. If staff receive such a request, they must immediately forward it to the Data Protection Officer.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

11. CCTV

We use CCTV in various locations around the school sites to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the School Business Manager.

12. Photographs and videos

As part of our school activities, and for the purpose of assessing pupils we take photographs and record images of individuals within our schools.

At the point of enrolment to the school, we will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

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

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns.
- Online on our school website or social media pages.

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

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

See our Child protection and safeguarding, ICT and e-safety policies for more information on our use of photographs and videos.

13. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge.
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6).
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will be contacted and advised on this process).
- Integrating data protection into internal documents including this policy, any related policies and privacy notices.
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters.
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our schools and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices).
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

14. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use.
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access · Where personal information needs to be taken off site, staff must sign it in and out from the school office and use locked zip wallets.
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.
- Staff, pupils or LAB members who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our e- safety policy, ICT policy, mobile phone policy and acceptable use agreement).
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8).

15. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

16. Personal data breaches

The schools will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in the Data Breach Policy.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context could include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium.
- Safeguarding information being made available to an unauthorised person.
- The theft of a school laptop containing non-encrypted personal data about pupils.

17. Training

All staff and LAB members are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

18. Monitoring arrangements

The Data Protection Officer is responsible for monitoring and reviewing this policy.

19. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- E-safeguarding Policy
- IT Policy
- Child protection Policy
- Looked after Children Policy
- Guidelines for voluntary adult helpers and students
- Single central record
- Assessment Policy
- Early Years Policy
- SEN Policy

DATA BREACH POLICY

1. Aims

- BCAT is committed to the protection of all personal data and special category personal data for which we are the data controller.
- The law imposes significant fines for failing to lawfully process and safeguard personal data and failure to comply with this policy may result in those fines being applied.
- All members of our workforce must comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary or other action.

2. About this policy

- This policy informs all of our workforce on dealing with a suspected or identified data security breach.
- In the event of a suspected or identified breach, BCAT must take steps to minimise the impact of the breach and prevent the breach from continuing or reoccurring.
- Efficient internal management of any breach is required, to ensure swift and appropriate action is taken and confidentiality is maintained as far as possible.
- BCAT must also comply with its legal and contractual requirements to notify other organisations including the Information Commissioners Office ("the ICO") and where appropriate data subjects whose personal data has been affected by the breach. This includes any communications with the press.
- Failing to appropriately deal with and report data breaches can have serious consequences for BCAT and for data subjects including:
    - identity fraud, financial loss, distress or physical harm.
    - reputational damage to BCAT.
    - fines imposed by the ICO.

3. Definition of data protection terms

- All defined terms in this policy are indicated in bold text, and a list of definitions is included in Appendix C to this policy.

4. Identifying a Data Breach

- A data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- This could be the result of a breach of cyber security, such as a hack or virus, or it could be the result of a breach of physical security such as loss or theft of a mobile device or paper records. A data breach includes loss of data and so does not have to be the result of a conscious effort of a third party to access the data. Some examples of potential data breaches are listed below:
    - Leaving a mobile device on a train.
    - Theft or loss of a bag containing paper documents.
    - Destruction of the only copy of a document.
    - Sending an email or attachment to the wrong recipient.
    - Using an unauthorised email address to access personal data.

- Leaving paper documents containing personal data in a place accessible to other people.

5. Internal Communication

Reporting a data breach upon discovery:

- If any member of our workforce suspects, or becomes aware, that a data breach may have occurred (either by them, another member of our workforce, a data processor, or any other individual) then they must contact the Data Protection Officer, Natalie Robertson immediately at: nrobertson@bcat.co.uk. In the absence of Natalie Robertson, please contact either the Principal or Headteacher.
- The data breach may need to be reported to the ICO, and notified to data subjects. This will depend on the risk to data subjects. The DPO must always be consulted in making a decision as to whether to report a data breach to the ICO. Initial investigations will inform as to whether the data breach should be reported.
- If it is considered necessary to report a data breach to the ICO then BCAT must do so within 72 hours of discovery of the breach.
- BCAT may also be contractually required to notify other organisations of the breach within a period following discovery.
- It is therefore critically important that whenever a member of our workforce suspects that a data breach has occurred, this is reported internally to the DPO immediately.
- Members of our workforce who fail to report a suspected data breach could face disciplinary or other action.

Investigating a suspected data breach:

- In relation to any suspected data breach the following steps must be taken as soon as possible. These do not have to be carried out as individual tasks, and the most appropriate way of dealing with any breach will depend on the nature of the breach and the information available at any time.

Breach minimisation:

- The first step must always be to identify how the data breach occurred, the extent of the data breach, and how this can be minimised. The focus will be on containing any data breach and recovering any personal data. Relevant departments must be involved, such as IT, to take technical and practical steps where appropriate to minimise the breach. Appropriate measures may include:
  - remote deactivation of mobile devices where possible.
  - shutting down IT systems.
  - contacting individuals to whom the information has been disclosed and asking them to delete the information.
  - Recovering lost data.

Breach investigation:

- When BCAT has taken appropriate steps to minimise the extent of the data breach it must commence an investigation as soon as possible to understand how and why the data breach occurred. This is critical to ensuring that a similar data breach does not occur again and to enable steps to be taken to prevent this from occurring.

- Technical steps are likely to include investigating, using IT forensics where appropriate, to examine processes, networks and systems to discover:
    - what data/systems were accessed;
    - how the access occurred;
    - how to fix vulnerabilities in the compromised processes or systems;
    - how to address failings in controls or processes.
- Other steps are likely to include discussing the matter with individuals involved to appreciate exactly what occurred and why, and reviewing policies and procedures.

Breach analysis:

- In order to determine the seriousness of a data breach and its potential impact on data subjects, and so as to inform BCAT as to whether the data breach should be reported to the ICO and notified to data subjects, it is necessary to analyse the nature of the data breach.
- Such an analysis must include:
    - the type and volume of personal data which was involved in the data breach;
    - whether any special category personal data was involved;
    - the likelihood of the personal data being accessed by unauthorised third parties;
    - the security in place in relation to the personal data, including whether it was encrypted;
    - the risks of damage or distress to the data subject.

The breach notification form in Appendix B of this policy must be completed in every case of a suspected breach, and retained securely, whether or not a decision is ultimately made to report the data breach. This will act as evidence as to the considerations of BCAT in deciding whether or not to report the breach.

6. External communication

- All external communication is to be managed and overseen by the DPO.

Law Enforcement:

- The DPO will assess whether the data breach incident requires reporting to any law enforcement agency, including the police. This will be informed by the investigation and analysis of the data breach, as set out above.
- DPO shall coordinate communications with any law enforcement agency.

Other organisations

- If the data breach involves personal data which we process on behalf of other organisations then we may be contractually required to notify them of the data breach.
- BCAT will identify as part of its investigation of the data breach whether or not this is the case and any steps that must be taken as a result.

Information Commissioner's Office

A data breach is notifiable unless it is unlikely to result in a risk to the rights and freedoms of any individual. The DPO will make an assessment of the data breach

against the following criteria taking into account the facts and circumstances in each instance:

- the type and volume of personal data which was involved in the data breach;
- whether any special category personal data was involved;
- the likelihood of the personal data being accessed by unauthorised third parties;
- the security in place in relation to the personal data, including whether it was encrypted;
- the risks of damage or distress to the data subject.

If a notification to the ICO is required then see part 7 of this policy below.

Other supervisory authorities

- If the data breach occurred in another country or involves data relating to data subjects from different countries then the DPO will assess whether notification is required to be made to supervisory authorities in those countries.

Data subjects

- When the data breach is likely to result in a high risk to the rights and freedoms of the data subjects then the data subject must be notified without undue delay. This will be informed by the investigation of the breach by BCAT.
- The communication will be coordinated by the DPO and will include at least the following information:
    - a description in clear and plain language of the nature of the data breach;
    - the name and contact details of the DPO;
    - the likely consequences of the data breach;
    - the measures taken or proposed to be taken by BCAT to address the data breach including, where appropriate, measures to mitigate its possible adverse effects.

- There is no legal requirement to notify any individual if any of the following conditions are met:
    - appropriate technical and organisational protection measures had been implemented and were applied to the data affected by the data breach, in particular, measures which render the data unintelligible to unauthorised persons (e.g. encryption);
    - measures have been taken following the breach which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise;
    - it would involve disproportionate effort to contact individuals. In which case a public communication or similar equally effective measure of communication to the data subject shall be issued.

For any data breach, the ICO may mandate that communication is issued to the data subject, in which case such communication must be issued.

Press

- Staff shall not communicate directly with the press and shall treat all potential data breaches as confidential unless otherwise instructed in writing by the DPO.
- All press enquiries shall be directed to the DPO and BCAT press officer.

7. Producing an ICO Breach Notification Report

- All members of our workforce are responsible for sharing all information relating to a data breach with the DPO, which will enable the Breach Notification Report Form to be completed (Appendix B).
- When completing the attached Breach Notification Report Form all mandatory (*) fields must completed, and as much detail as possible should be provided.
- The DPO may require individuals involved in relation to a data breach to each complete relevant parts of the Breach Notification Form as part of the investigation into the data breach.
- If any member of our workforce is unable to provide information when requested by the DPO then this should be clearly reflected in the Breach Notification Form together with an indication as to if and when such information may be available.
- In the wake of a data protection breach, swift containment and recovery of the situation is vital. Every effort should be taken to minimise the potential impact on affected individuals, and details of the steps taken to achieve this should be included in this form.
- The ICO requires that BCAT send the completed Breach Notification Form to casework@ico.org.uk, with 'DPA breach notification form' in the subject field, or by post to: The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

8. Evaluation and response

- Reporting is not the final step in relation to a data breach. BCAT will seek to learn from any data breach.
- Therefore, following any breach an analysis will be conducted as to any steps that are required to prevent a breach occurring again. This might involve a step as simple as emailing all relevant members of our workforce to reinforce good practice, or providing additional training, or may in more serious cases require disciplinary processes, new technical systems and processes and procedures to be put in place.

APPENDIX A – Data Subject Access Request Form

Article 15 of the EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) grants you the right to access your personal data, if any, held by a Bedford College Academies Trust School.

Please complete this form if you wish to make a request in relation to your personal data.

NOTE: This is not a mandatory form – Subject Access Requests made in other formats will also be accepted but this form is designed to help you in providing us with the information we need to deal with your request and speed up the process.

Subject Access Request Guidance

(Please read before filling in the Subject Access Request Form)

Which sections should I complete?

Sections **1, 2, 3 and 4**	**Data Subject Details** Should be completed for ALL applications.
Sections **5, 6 and 7**	**Representative Details and Authority to Release Information to a Representative:** Should only be completed if the application is being made by a representative (i.e. someone other than the data subject themselves).
Sections **2**	**Proof of the applicant's identity:** If you do not have any of the forms of identity listed, we may in exceptional circumstances accept alternatives for consideration. (Current employees and pupils, you may visit the school office to confirm verification of your identity by an authorised member of staff).
Sections **6**	**Proof of the representative's identity:** If you do not have any of the forms of identity listed, we may in exceptional circumstances accept alternatives for consideration.

General Information

How long will it take to get my data?

Once we are satisfied that you meet the criteria for disclosure of data under the General Data Protection Regulation, and have provided sufficient information for us to confirm your identity and accept your application for processing, you should receive a response within one calendar month from that date.

However, in certain circumstances, the GDPR allows us to extend that deadline depending on the complexity of your request. We will advise you within one month if we need to extend the response deadline.

Records may be held in several different locations in paper and electronic formats. If you only require specific information and you clearly state what that is – for example a specific document or IT-only data – then you are likely to get a quicker response.

Cost

In most cases we will not charge a fee to comply with a Subject Access Request.

However, where the request is manifestly unfounded or excessive we may charge a "reasonable fee" for the administrative costs of complying with the request.

Sending your completed form

Please send your completed form and proof of ID to:

Data Protection Officer

Wixams Academy

Green Lane

Wixams

Bedfordshire

MK42 6BA

Section 1 – Data Subject's Details

Please provide the information in the space provided below.
We will only use the information you provide on this form to identify you and the personal data you are requesting access to, and to respond to your request.

Title (please tick)	**Mr** ☐ **Mrs** ☐ **Miss** ☐ **Ms** ☐ **Other** ☐
Surname	
First name(s)	
Date of birth	
Address	
Address	
City / County	
Postcode	
Telephone (daytime)	
Email address	
Relationship to the School	Employee ☐ Pupil ☐ Supplier ☐ Other ☐

Section 2 - Requests Proof of Data Subject's Identity

We may require proof of your identity before we can respond to your request.

In order to prove the applicant's identity, we may need to see copies of two pieces of identification, one from list A and one from list B below. Please indicate which ones you are supplying.

Please DO NOT send an original passport, driving licence or identity card.

List A (photocopy of one from below)		**List B (photocopy of one from below)**	
Identification that clearly shows your name and date of birth.		Documentation that clearly shows your name and current address.	
Passport/Travel Document		A Council Tax bill	
Photo driving licence		Utility bill showing current home address	
Foreign National Identity Card		Bank Statement or Building Society Book	

We reserve the right to refuse to act on your request if we are unable to identify you.

If you do not have any of these forms of identification available, please contact our DPO for advice on other acceptable forms of identification: nrobertson@bcat.co.uk. Or if you are currently an employee or pupil at the school, you may visit the school office to confirm verification of your identity by an authorised member of staff.

Section 3 – Information Requested

So that we can locate the data you require efficiently, please answer the following questions to the best of your knowledge. Please continue on a separate sheet if necessary.

The Information Commissioner has stated that as much information as possible should be provided to assist with tracing a data subject's information.

Please tell us as much as you can about the information you are requesting about. **For example, if you are requesting access to your personal data which might be in an email or document, it helps in our search to know who might have written it, when and to whom the information might have been sent, and where it may be stored.**

Period attended/worked at the school:

From _____ **To** _____

Specific period, which you request access to the data (complete if different from the period of attendance):

From _____ **To** _____

Section 4 - Declaration

This form must be signed by you (the data subject).

I request a copy of the relevant personal data that are held by Bedford College Academies Trust relating to information provided above. I confirm the information supplied is correct and I declare that I am the individual as indicated above.

Signed _____ **Date** _____

Section 5 - Requests Made on the Data Subject's Behalf

Please complete this section of the form with your name and contact details if you are acting on the data subject's behalf.

First and last name	
Company name	
Address and Postcode	
Date of birth	
Telephone number	

Section 6 - Proof of the Representatives Identity

We may require proof of your identity before we can respond to your access request.
In order to prove the representative's identity, we need may to see copies of two pieces of identification, one from list A and one from list B below. Please indicate which ones you are supplying.

Please DO NOT send an original passport, driving licence or identity card.

List A (<u>photocopy</u> of one from below)		**List B (<u>photocopy</u> of one from below)**	
Identification that clearly shows your name and date of birth.		Documentation that clearly shows your name and current address.	
Passport/Travel Document		A Council Tax bill	
Photo driving licence		Utility bill showing current home address	

Foreign National Identity Card		Bank Statement or Building Society Book	

We reserve the right to refuse to act on your request if we are unable to identify you.
If you do not have any of these forms of identification available, please contact our DPO for advice on other acceptable forms of identification: nrobertson@bcat.co.uk

Section 7 - Authority to release information to a Representative

A representative needs to obtain authority from the applicant before personal data can be released. The representative should obtain the applicant's signature below, or provide a separate note of authority. This must be an original signature, not a photocopy.

I hereby give my authority for the representative named in Section 6 of this form to make a Subject Access Request on my behalf.	
Signature of Applicant:	Date:
Signature of Representative:	Date:

For office use

Data Access Request Number	
Date request received	

APPENDIX B – ICO Breach Notification Report

1. Organisation details

Name of organisation:	
Data Controller's registration number, if applicable:	
DPO:	
Contact Details:	

2. Details of the data protection breach

Set out the details of the breach and ensure that all fields are completed.

Please describe the incident in as much detail as possible
When did the incident happen?
How did the incident happen?
If there has been a delay in reporting the incident to the ICO, please explain your reasons for this.
What measures did the organisation have in place to prevent an incident of this nature occurring?
Please provide extracts of any policies and procedures considered relevant to this incident, and explain which of these were in existence at the time this incident occurred. Please provide the dates on which they were implemented.

3. Details of the Personal Data placed at risk

Set out the details of the personal data placed at risk as a result of the breach and ensure that all fields are completed.

What personal data has been placed at risk? Please specify if any financial or special category (sensitive) personal data has been affected and provide details of the extent/
How many individuals have been affected?
Are the affected individuals aware that the incident has occurred?
What are the potential consequences and adverse effects on those individuals?
Have any affected individuals complained to the School / Trust about the incident?

4. Containment and recovery

Set out the details of any steps BCAT has taken to contain the breach and/or to recover the personal data and ensure that all fields are completed.

Has the Trust taken any action to minimise/mitigate the effect on the affected individuals? If so, please provide details.
Has the data placed at risk now been recovered? If so, please provide details of how and when this occurred.

What steps has BCAT taken to prevent a recurrence of this incident?

5. Training and guidance

Set out the details of any steps BCAT has taken to contain the breach and/or to recover the personal data and ensure that all fields are completed.

As the data controller, does the Trust provide its staff with training on the requirements of Data Protection Legislation? If so, please provide any extracts relevant to this incident here.
Please confirm if training is mandatory for all staff. Had the staff members involved in this incident received training and if so when?
As the data controller, does BCAT provide any detailed guidance to staff on the handling of personal data in relation to the incident you are reporting? If so, please provide any extracts relevant to this incident here.

6. Previous contact with the ICO

Have you reported any previous incidents to the ICO in the last two years?
YES / NO
If the answer to the above question is yes, please provide: brief details, the date on which the matter was reported and, where known, the ICO reference number.

7. Miscellaneous

Have you notified any other (overseas) data protection authorities about this incident? If so, please provide details.
Have you informed the Police about this incident? If so, please provide further details and specify the Force concerned.
Have you informed any other regulatory bodies about this incident? If so, please provide details.
Has there been any media coverage of the incident? If so, please provide details of this.

This form was completed on behalf of BCAT by:	
Name:	
Job Title:	
Date:	
Time:	

APPENDIX C - DEFINITIONS

Term	Definition
Data	Information which is stored electronically, on a computer, or in certain paper-based filing systems.
Data Subjects	For the purpose of this policy include all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.
Personal Data	Means any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Data Controllers	Are the organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes.
Data Users	Are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.
Data Processors	Include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions.
Processing	Is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties.

Special Category Personal Data	includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data.
Workforce	Includes any individual employed by Bedford College Academies Trust such as staff and those who volunteer in any capacity, including LAB Members.