
# DATA PROTECTION INCLUDING FREEDOM OF INFORMATION POLICY

**SEPTEMBER 2025**

**AUTHOR: KATE TAGUE**

# BOA GROUP

# DATA PROTECTION INCLUDING FREEDOM OF INFORMATION POLICY

| | | | |
|---|---|---|---|
| **Author:** | Kate Tague | **Version:** | 1.0 |
| **Date Approved:** | September 2025 | **Date for Review:** | September 2027 |
| **Monitoring, Review and Evaluation:** To be reviewed every 2 years by the Trust Board on the advice of the Data Protection Officer and subject to Trust Board approval. | | | |

*This policy supersedes any previous data protection policy or arrangements and was written to bring together the Trust's data protection, freedom of information, and data retention policies.*

**1. Aims**

BOA Group aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018). 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 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 meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data. It also 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.

**3. Definitions**

- **Personal Data -** Any information relating to an identified, or identifiable, individual. This may include the individual's name (including initials), identification number, location data or 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.
- **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**

BOA Group processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller. The Trust is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

**5. Roles and Responsibilities**

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

- **Trust Board** - overall responsibility for ensuring that our academy complies with all relevant data protection obligations.
- **Data Protection Officer (DPO)** - 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 governing board and, where relevant, report to the board their advice and recommendations on academy data protection issues. The DPO is also the first point of contact for individuals whose data the academy processes, and for the ICO.
- **Chief Executive Officer** - acts as the representative of the data controller on a day-to-day basis.
- **All staff** - responsible for:
    - Collecting, storing and processing any personal data in accordance with this policy
    - Informing the academy 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 European Economic Area
        - 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 BOA Group must comply with and this policy sets out how BOA Group complies with these principles. The principles say 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

**7. Collecting Personal Data**

*7.1 Lawfulness, fairness and transparency*

BOA Group 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 academy can **fulfil a contract** with the individual, or the individual has asked the academy to take specific steps before entering into a contract
- The data needs to be processed so that the academy 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 academy, 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 academy 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, BOA Group will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If BOA Group offers online services to pupils, such as classroom apps, 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). Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

*7.2 Limitation, Minimisation and Accuracy*

BOA Group 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 BOA Group's record retention schedule/records management policy.

**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 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. 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 academy 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 must be submitted in writing, by either letter or email to the DPO. They should include the name of the individual making the request, a correspondence address, contact number and email address and a summary of the information requested.

If staff receive a subject access request they must immediately forward it to the DPO.

*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 our academy 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.

Children aged 12 and above are generally 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 our academy may not 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 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.

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*

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 DPO. If staff receive such a request, they must immediately forward it to the DPO.

**10. Parental Requests to See the Educational Record**

Within academies, there is no automatic right for parental access to educational records, however BOA Group will grant access for an administration charge. Please refer to contact details in appendix 1.

**11. Privacy Notices**

The Data Protection Officer regularly reviews and updates the BOA Group privacy notices. These are published on the Trust's website or available on request from the DPO.

**12. Freedom of Information Requests**

Freedom of Information requests are provided for the Freedom of Information Act 2000 and more information can be found in Appendix 1. Freedom of Information requests are designed to remove unnecessary secrecy between the public and statutory organisations and should not be confused with a Subject Access Request which enables a data subject to request access to their own personal data.

**13. Data Retention**

More information about BOA Group's retention of personal data can be found in Appendix 2.

**14. Biometric Recognition Systems**

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive academy dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers, or students if over the age of 16, will be notified before any biometric recognition system is put in place or before their child first takes part in it. The academy will get written consent from at least one parent or carer before we take any biometric data from their child and first process it. Parents/carers and pupils have the right to choose not to use the academy's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils, including use of student photo cards as proof of identification when purchasing from the canteen. Parents/carers and pupils can object to participation in the academy's biometric recognition system(s), or withdraw consent, at any time, and we 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, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the academy's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the academy will delete any relevant data already captured.

**15. CCTV**

BOA Group use CCTV in various locations around the academy sites to ensure they remain safe. 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.

**16. Photographs and Videos**

As part of our academy activities, we may take photographs and record images of individuals within our academy.

We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

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 pupil how the photograph and/or video will be used.

Uses may include:

- Within academy on notice boards and in academy magazines, brochures, newsletters, etc.
- Outside of academy by external agencies such as the academy photographer, newspapers, campaigns
- Online on our academy 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.

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

**17. 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
- Completing privacy impact assessments where BOA Group's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise 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; we will also keep a record of attendance
- 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 academy 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

**18. 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 academy office
- Passwords that are at least 8 characters long containing letters and numbers are used to access academy 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 governors who store personal information on their personal devices are expected to follow the same security procedures as for academy-owned equipment (see our 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.

**19. 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 academy's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

In line with Appendix 2 of this policy, all data relating to safeguarding of young people at BOA Group, including some personnel and employee data, will be retained in accordance with our statutory duty to safeguard children and young people. This is provided for in Article 6, Section C of the UK GDPR.

**18. Personal Data Breaches**

BOA Group 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 Appendix 3 and, when appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a academy context may include, but are not limited to:

- A non-anonymised dataset being published on the academy 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 academy laptop containing non-encrypted personal data about pupils

**19. Training**

All staff and governors 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 academy's processes make it necessary.

**20. Monitoring and Review**

This policy will be reviewed every two years by the Trust Board and subject to Trust Board approval. Changes in technology, legislation or other external factors may result in this policy being reviewed earlier.

**Appendix 1 – Freedom of Information**

All students graduating from the BOA Group will be positioned at all levels of leaving to pursue potential learning and employment opportunities in world class advanced engineering and manufacturing. Our graduates will have a range of technical and analytical skills that are transferable to employment in other sectors or progression into further and higher education.

This publication scheme is a means of showing how we are pursuing this mission.

This model publication scheme has been prepared by the Information Commissioner. This commits the BOA Group to make information available to the public as part of its normal business activities The Trust is committed to protecting the personal data of our staff and students.

**I. Statement of Commitments**

The BOA Group commits:

- To proactively publish or otherwise make available as a matter of routine, information, including environmental information, which is held by the Trust and falls within the classes below.
- To specify the information which is held by the Trust and falls within the classifications below.
- To proactively publish or otherwise make available as a matter of routine, information in line with the statements contained within this policy.
- To produce and publish the methods by which the specific information is made routinely available so that it can be easily identified and accessed by members of the public.
- To review and update on a regular basis the information the trust makes available under the scheme.
- To produce a schedule of any fees charged for access to information which is made proactively available.
- To make this publication scheme available to the public.
- To publish any dataset held by the Trust that has been requested, and any updated versions it holds, unless the Trust is satisfied that it is not appropriate to do so;
- To publish the dataset to make the information available for re-use under the terms of the Re-use of Public Sector Information Regulations 2015, if they apply, and otherwise under the terms of the Freedom of Information Act section 19. The term 'dataset' is defined in section 11(5) of the Freedom of Information Act. The term 'relevant copyright work' is defined in section 19(8) of the Act.

**II. Classes of Information**

- **Who we are and what we do -** Organisational information, locations and contacts, constitutional and legal governance.
- **What we spend and how we spend it -** Financial Information relating to projected and actual income and expenditure, tendering, procurement and contracts.
- **What our priorities are and how we are doing -** Strategy and performance information, plans, assessments, inspections and reviews.

- **How we make decisions -** Policy proposals and decisions. Decision making processes, internal criteria and procedures, consultations.
- **Our policies and procedures -** Current written protocols for delivering our functions and responsibilities.
- **Lists and registers -** Information held in registers required by law and other lists and registers relating to the functions of the trust.
- **The services we offer -** Advice and guidance, booklets and leaflets, transactions and media releases. A description of the services offered.

The classes of information will not generally include:

- Information the disclosure of which is prevented by law, or except under the Freedom of Information Act, or is otherwise properly considered to be protected from disclosure.
- Information in draft form.
- Information that is no longer readily available as it is contained in files that have been placed in archive storage, or is difficult to access for similar reasons.

**III. Classes of Information Currently Published**

| Class | Description |
|---|---|
| Academy Prospectus | The statutory contents of the academy prospectus are as follows, (other items may be included in the prospectus at the academy's discretion).<br>• The name, address and telephone number of the academy, and the type of academy.<br>• The names of the Trust Board, Associate Principal(s), Chair of the Trust Board and the Chair of Governor(s).<br>• Information regarding the academy's policy on admissions.<br>• A statement of the academy's ethos and values.<br>• Details of any affiliations with a particular religion or religious denomination about the academy's policy on providing for students with special educational needs.<br>• Number of students on roll and rates of students' authorised and unauthorised absences.<br>• National curriculum assessment results for appropriate key stages, with national summary figures.<br>• The arrangements for visits to the academy by prospective parents/guardians. |
| Instruments and Articles of Government and related Governance documentation | This section sets out the information published regarding the governing bodies.<br>• The name and category of the Academy<br>• The manner in which the governing body is constituted<br>• The terms of office of each category of governor if less than four years.<br>• The names of those entitled to appoint any category of governor.<br>• If the academy has religious character, a description of the ethos.<br>• Names of governors<br>• Declaration of business and pecuniary interests.<br>• Attendance at meetings. |

| | |
|---|---|
| Policies and related information | This section sets out the information published regarding policies and other related documents.<br>• Academy and Trust wide policies.<br>• Home/Academy agreements<br>• Accessibility Plans<br>• Collective Worship – statements for the arrangements for the required daily act of collective worship.<br>• Published reports from Ofsted relating expressly to the academy.<br>• Post Ofsted Inspection and Action Plan.<br>• Session times and term dates |

**IV. How to request information.**

Information is readily available on the academy and trust websites and also available via a request under the Freedom of Information Act 2000 to principal@wmgacademy.org.uk

To help process your request, please clearly mark any correspondence "Freedom of Information Request".

Information held that is not published under this scheme can be requested in writing, when the provision will be considered in accordance with the provisions of the Freedom of Information Act.

In some exceptional circumstances some information may be available only by viewing in person. Where this manner is specified, contact details will be provided. An appointment to view the information will be arranged within a reasonable timescale.

Information will be provided in the language in which it is held or in such other language that is legally required. Where the Trust is legally required to translate any information, it will do so.

Obligations under disability and discrimination legislation and any other legislation to provide information in other forms and formats will be adhered to when providing information in accordance with this scheme.

**V. Charges which may be made for information published under this scheme.**

The purpose of this scheme is to make the maximum amount of information readily available at minimum inconvenience and cost to the public. Charges made for routinely published material will be justified and transparent and kept to a minimum.

Material which is published and accessed on a website will be provided free of charge, however charges may be made for actual disbursements incurred such as:

- Photocopying
- Postage and packaging
- The costs directly incurred as a result of viewing information.

Charges may also be made for making datasets (or parts of datasets) that are relevant copyright works available for re-use. These charges will be in accordance with the terms of the Re-use of Public Sector

Information Regulations 2015, where they apply, or with regulations made under section 11B of the Freedom of Information Act, or with other statutory powers of the trust.

If charges are to be made, confirmation of the payment due will be given before the information is provided and payment will be requested prior to the provision of the information.

**VI. Responses to Freedom of Information Act Requests**

The Trust will adhere to the deadline in producing information under the act. It will reply promptly and, in any event, will respond within 20 working days following the date of receipt.

**Appendix 2 – GDPR Data Retention Protocol**

1. Under the General Data Protection Regulations (GDPR) and the Data Protection Act (DPA 2018) academys need a policy setting out the retention periods for the personal data they hold. The Data Retention Protocol will identify the different sections of data that BOA Group for Young Engineers controls and processes and how long this should be retained.

| **2. Governing Body** | | | | | |
|---|---|---|---|---|---|
| | **Basic File Description** | **Retention Period** | **Action at End of the Administrative Life of the Record** | **Personal Information** | **Justification** |
| 2.1 | Principal copy of meeting minutes and agenda | Life of academy | Archives | Potential | All papers circulated to, reported by or relevant to the governing bodies or Trust Board and its committees should be held on file for audit purposes and to ensure compliance with Companies House regulations for the retention of management records. |
| 2.2 | Additional copies of meeting minutes and agenda | Date of meeting | Secure Disposal | Potential | |
| 2.3 | Records of election of governors | 6 months after election or until appeals window closed. | Secure Disposal | Yes | |
| 2.4 | Records of election of chair and vice-chair | Until minutes of appointment approved | Secure Disposal | Yes | |
| 2.5 | Scheme of delegation and terms of reference for committee | Whilst relevant | Standard Disposal | No | |
| 2.6 | Reports, registers and papers referenced in the minutes. | Life of academy | Archives | Potential | |
| 2.7 | Records of governor's monitoring visits | 3 years after date of visit | Secure Disposal | Yes | |
| 2.8 | Annual reports required by DfE | 10 years after date of report | Secure Disposal | Yes | |

| | | | | | |
|---|---|---|---|---|---|
| 2.9 | Records relating to complaints investigated by governing body or SLT | Minor complaints: 5 years post investigation.<br><br>Negligence: 15 years post investigation.<br><br>Child protection: 40 years after date of investigation. | Secure Disposal | Yes | |
| 2.10 | Actions plans administered by governing body | Whilst relevant | Secure Disposal | Yes | |
| 2.11 | Policies | Until reviewed and updated. Good practice: archive previous versions of policies | Standard Disposal | No | |
| 2.12 | Record of appointment of Clerk | 6 years after appointment ceases | Secure Disposal | Yes | |
| 2.13 | Governor code of conduct | Until reviewed and updated. Good practice: archive previous versions of code of conduct | Standard Disposal | No | |
| 2.14 | Governors personnel file, including training DBS records, induction and declarations of interest | 6 years after appointment ceases | | | |

| 3. Academy Management | | | | | |
|---|---|---|---|---|---|
| | **Basic File Description** | **Retention Period** | **Action at End of the Administrative Life of the Record** | **Personal Information** | **Justification** |
| 3.1 Trust Board and Senior Leaders | | | | | |
| 3.1.1 | Minutes of Senior Management Meetings | 3 years after the date of meeting | Secure Disposal | Potential | Kept on file to ensure any discussions relating to regulated matters, i.e. finance, HR and Health and Safety are documented for audit purposes.<br><br>Kept to maintain paper trail for inspections purposes. |
| 3.1.2 | Reports created by the Trust Board or their SLT | Review every 3 years whilst relevant | Secure Disposal | Potential | |
| 3.1.3 | Records created by managers with administrative responsibilities | Review every 3 years whilst relevant | Secure Disposal | Potential | |
| 3.1.4 | Correspondence created by managers with administrative responsibilities | 3 years after the date of correspondence | Secure Disposal | Potential | |
| 3.1.5 | Professional development plans | In line with the retention of employee's personnel file | Secure Disposal | Yes | |
| 3.1.6 | Academy development plan | 3 years after plan completion date | Secure Disposal | Potential | |
| 3.2 Operational Administration | | | | | |
| 3.2.1 | Academy Privacy Notice | Until reviewed and updated. Good practice: archive previous versions of Privacy Notice | Standard Disposal | No | |

| | | | | | |
|---|---|---|---|---|---|
| 3.2.2 | Consents relating to academy activities | Until student leaves Academy. | Secure Disposal | Yes | Kept on file whilst still relent. I.E whilst child is still a student. |
| 3.2.3 | Circulars and memorandums sent to staff, parents, students or stakeholders | Current academic year | Secure Disposal | Potentially | |
| 3.2.4 | Newsletters and documents relating to their production | Current academic year | Standard Disposal | No | In line with recognised best practice for continuity |
| 3.2.5 | Prospectuses and brochures and documents relating to their production | Current academic year | Standard Disposal | No | |
| 3.2.6 | Documents relating to visitor management systems | 6 years after date of last entry | Secure Disposal | Yes | Kept on file in case on investigations into allegations against any visitor |
| 3.3 Human Resources | | | | | |
| 3.3.1 | All records leading up the appointment of a member of staff – unsuccessful candidates | 6 months after the date of appointment | Secure Disposal | Yes | Retained as evidence of fair recruitment process |
| 3.3.2 | All records leading up the appointment of a member of staff – successful candidates | All documents to be retained on personnel file | Secure Disposal | Yes | Retained to ensure staff meet minimum requirements in terms of safeguarding, qualifications |
| 3.3.3 | Documents relating to pre-employment checks, including right to work and DBS | All documents to be retained on personnel file | Secure Disposal | Yes | |

| | | | | | |
|---|---|---|---|---|---|
| 3.3.4 | Records relating to performance management/appraisal | All documents to be retained on personnel file | Secure Disposal | Yes | and child protection. |
| 3.3.5 | Records relating to staff absence/sickness | All documents to be retained on personnel file | Secure Disposal | Yes | Retained to show paper trail and justification for subsequent pay increments. |
| 3.3.6 | Records of staff training and continued professional development | All documents to be retained on personnel file | Secure Disposal | Yes | |
| 3.3.7 | Employee's personnel file | 6 years after employment ends, unless employee is dismissed or under investigation, then retain records for duration of investigation and 15 years for negligence or 40 years for child protection | Secure Disposal | Yes | Retained for auditing purposes. |
| 3.3.8 | Records of employees' salary, pay and personal bank details | Until updated or 6 years after employment ends | Secure Disposal | Yes | |
| 3.3.9 | Employees' tax information | 6 years after employment ends | Secure Disposal | Yes | |
| 3.3.10 | Records relating to maternity, paternity, and sick pay | 3 years after date of absence | Secure Disposal | Yes | |
| 3.3.11 | Records relating to advancements, loans | 6 years after date of payment | Secure Disposal | Yes | |

| | | | | | |
|---|---|---|---|---|---|
| | and expenses, including payslips | | | | |
| 3.4 Health and Safety | | | | | |
| 3.4.1 | Health and Safety policies and statements | Until reviewed and updated. Good practice: archive previous versions of policies | Secure Disposal | No | Retained to allow for monitoring, audit and reporting of health and safety practices and incidents. |
| 3.4.2 | Health and Safety risk assessments | Until reviewed and updated. Good practice: archive previous versions of risk assessments | Secure Disposal | No | |
| 3.4.3 | Accident reports relating to individuals over 18 years of age | 3 years after last entry in accident book | Secure Disposal | Yes | |
| 3.4.4 | Accident reports relating to individuals under 18 years of age | 3 years after last entry in accident book | Secure Disposal | Yes | |
| 3.4.5 | Records relating to RIDDOR | 40 years after date of incident | Secure Disposal | Yes | |
| 3.4.6 | Records relating to COSHH | 40 years after date of incident | Secure Disposal | Yes | |
| 3.4.7 | Records of fire prevention or evacuation measures | 3 years after date of action | Secure Disposal | Potentially | |
| 3.4.8 | Records of alterations to buildings | Life of building – transferred to new owners | Secure Disposal | Potentially | |
| 3.5 Finance | | | | | |
| 3.5.1 | Employers' Liability Insurance certificate | 40 years after academy closure | Secure Disposal | No | In line with recognised |

| | | | | | |
|---|---|---|---|---|---|
| 3.5.2 | Inventory of furniture and equipment and reports of theft or vandalism | 6 years after report/completion of inventory | Secure Disposal | Potentially | best practice and Academies Financial Handbook |
| 3.5.3 | Annual Accounts | 6 years after current financial year | Standard Disposal | No | |
| 3.5.4 | Details of loans managed by Academy | 12 years after final payment | Secure Disposal | Yes | |
| 3.5.5 | Records relating to budget creation and management | 3 years after life of budget | Secure Disposal | Yes | |
| 3.5.6 | Records of invoices, receipts, orders, monies banked and identification and collection of loans or debts | 6 years after date of record | Secure Disposal | Yes | |
| 3.5.7 | Records relating to Pupil Premium | 6 years after student leaves | Secure Disposal | Yes | |
| 3.5.8 | Records relating to contracts | 12 years after end date of contract | Secure Disposal | Potentially | |
| 3.5.9 | All records relating to academy fund | 6 years after current financial year | Secure Disposal | Yes | |
| 3.5.10 | Records relating to FSM and academy meals | 6 years after current financial year | Secure Disposal | Yes | |
| 4.6 Property | | | | | |
| 3.6.1 | Title deeds of properties and plans | Life of building - transferred to new owners | Secure Disposal | Yes | In line with recognised best practice and Academies |
| 3.6.2 | Records relating to leases of property (Academy as tenant) | 6 years after expiry of lease | Secure Disposal | Yes | |

| | | | | | |
|---|---|---|---|---|---|
| 3.6.3 | Records relating to leases of property (Academy as landlord) | 6 years after expiry of lease | Secure Disposal | Yes | Financial Handbook |
| **4. Pupil Management** | | | | | |
| | **Basic File Description** | **Retention Period** | **Action at End of the Administrative Life of the Record** | | |
| 4.1 Admissions | | | | | |
| 4.1.1 | All records relating to unsuccessful admissions | 1 year after admission date or until closure of appeals process | Secure Disposal | Yes | Common practice |
| 4.1.2 | All records relating to successful admissions | Retained on student file until student leaves Academy | Secure Disposal | Yes | Common practice |
| 4.2 Attendance | | | | | |
| 4.2.1 | All data | 3 years after student leaves | Secure Disposal | Yes | Common practice |
| 4.3 Attainment | | | | | |
| 4.3.1 | All data | 1 year after student leaves | Secure Disposal | Yes | Common practice |
| 4.4 Behaviour | | | | | |
| 4.4.1 | All data | 1 year after student leaves | Secure Disposal | Yes | Common practice |
| 5.5 Exclusions | | | | | |
| 4.5.1 | All data | As per attendance unless child protection issue, then 40 years | Secure Disposal | Yes | Common practice |

| | | | | | |
|---|---|---|---|---|---|
| | | after date of exclusion | | | |
| 4.6 Medical Information | | | | | |
| 4.6.1 | All data | 3 years after student leaves | Secure Disposal | Yes | Common practice |
| 4.7 Photographs | | | | | |
| 4.7.1 | All data | 3 years after student leaves | Secure Disposal | Yes | Common practice |
| 4.8 Safeguarding | | | | | |
| 4.8.1 | All data | 40 years after date of incident | Secure Disposal | Yes | Statutory guidance<br><br>"Safeguarding Children in Education" 2004<br>Keeping Children Safe in Education (Department for Education) |
| 4.9 SEN | | | | | |
| 4.9.1 | All data | Until student turn 40 years of age | Secure Disposal | Yes | Statutory guidance<br><br>Special Educational Needs and Disability Act 2001 |

| 5. Curriculum and Extra-Curricular Activities | | | | | |
|---|---|---|---|---|---|
| | **Basic File Description** | **Retention Period** | **Action at End of the Administrative Life of the Record** | **Personal Information** | **Justification** |
| 5.1 Data Management | | | | | |
| 5.1.1 | Value added and contextual data | 6 years after current academic year | Secure Disposal | Yes | Common practice |
| 5.1.2 | Self evaluation | 6 years after current academic year | Secure Disposal | Yes | Common practice |
| 5.1.3 | Internal moderation | 1 year after current academic year | Secure Disposal | Yes | Common practice |
| 5.1.4 | External moderation | 6 years after current academic year | Secure Disposal | Yes | Common practice |
| 5.2 Implementation of Curriculum | | | | | |
| 5.2.1 | Schemes of work, timetables, markbooks and records of class and homework set | 1 year after current academic year | Secure Disposal | Yes | Common practice |
| 5.2.2 | Student's work | Return to students or dispose at end of academic year | Assessed work – Secure Disposal<br><br>Non-assessed work – Standard Disposal | Potentially | Common practice |

| | | | | | |
|---|---|---|---|---|---|
| 5.3 Educational/Offsite Visits | | | | | |
| 5.3.1 | All records relating to visit where no incident occurred | End of academic year | Secure Disposal | Yes | In line with recognised best practice |
| 5.3.2 | All records relating to visit where major incident occurred | 25 years after date of incident or 40 years for child protection incidents | Secure Disposal | Yes | Retained for purposes of investigations |
| **6. Curriculum and Extra-Curricular Activities** | | | | | |
| | **Basic File Description** | **Retention Period** | **Action at End of the Administrative Life of the Record** | **Personal Information** | **Justification** |
| 6.1 | Attendance returns | 1 year after current academic year | Secure Disposal | Yes | Retained for purposes of academic audits, including LA and OFSTED inspections |
| 6.2 | Academy census returns | 5 years after current academic year | Secure Disposal | Yes | |
| 6.3 | OFSTED reports and papers | Life of report | Secure Disposal | Yes | |
| 6.4 | Returns made to central government | 6 years after current academic year | Secure Disposal | Yes | |
| 6.5 | Circulars and other information from LA or central government | Operational Use | Secure Disposal | Potentially | |

**Appendix 3 - Personal data breach procedure**

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost or Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been made available to unauthorised people
- The DPO will alert the Trust Board.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.
- (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned
    - If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored electronically on BOA Group's IT system
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO o A description of the likely consequences of the personal data breach o A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO

expects to have further information. The DPO will submit the remaining information as soon as possible

- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause o Effects o Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
    - Records of all breaches will be stored electronically on BOA Group's IT system. The DPO and Trust Board will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.
- Actions to minimise the impact of data breaches
    - BOA Group will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.
- Sensitive information being disclosed via email (including safeguarding records)
    - If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
    - Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
    - If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
    - In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
    - The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
    - The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted Other types of breach that you might want to consider could include:
        - Details of pupil premium interventions for named children being published on the academy website
        - Non-anonymised pupil exam results or staff pay information being shared with governors

- A academy laptop containing non-encrypted sensitive personal data being stolen or hacked
- The academy's cashless payment provider being hacked and parents' financial details stolen