BORDESLEY MULTI ACADEMY TRUST

T1-09 DATA PROTECTION POLICY (Updated for GDPR)

Tier 1 – Bordesley MAT Central Policy
Approved by the Trust on 15/03/2023

Document control

Prepared by	Shaw Goodwin
Authorised by	CEO
Approved by	Full Board of Trustees
Adopted by local governing body	HFF BMS THS
Published location	BMAT Central – Policies>>Tier 1 Policies
Other documents referenced	T1-05 Freedom of Information Policy T2-03 Safeguarding and Child Protection Policy T3-03 Protection of Biometric Information Policy
Review date	2 Year – 15/03/2025
Related documents	

Version control

Version Number	Date Issued	Author	Update Information
Approved v1.1	23/02/2021	S Goodwin	Approved by Trustees
Draft v23.1	09/03/3023	S Goodwin	Draft based on previous version
Approved v23.1	15/03/2023	S Goodwin	Approved by Trustees O&C committee

Contents

1. Bordesley Multi Academy Trust Mission Statement

We believe that success is achieved by working in partnership with parents, carers and the wider community. We are committed to working with our partners to ensure the very best outcomes for all our learners, from 3 to 19.

The significant guiding principles of the MAT are based around autonomy, trust, respect, equity and outstanding relationships. We believe that positive and constructive relationships are at the heart of every successful school. This allows the entire community to be valued and challenged to be their best, raising aspirations for all.

2. Aims

Our Trust and schools aim 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 expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

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

3. Legislation & Guidance

This policy meets the requirements of the 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.

If the School uses CCTV: 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.

In addition, this policy complies with our funding agreement and articles of association.

4. 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.

5. The Data Controller

The Trust 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.

6. Roles & Responsibilities

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

Local Governing board

The local governing board, on behalf of the Trust, has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

Trust 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 Trustees and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO's contact details are below:

BMAT Data Protection Officer
Shaw Goodwin
Bordesley Multi-Academy Trust
C/O Trinity High school,
Easemore Road,
Redditch,
Worcestershire,
B98 8HB.

Email: goodwins@bmat.net
Telephone: 01527 330001

Headteacher
The headteacher acts as the representative of the data controller on a day-to-day basis.

School Data protection officer
The school data protection officer is responsible for overseeing the implementation of this policy within its setting, monitoring compliance with data protection law, and developing related policies and guidelines where applicable.

They will laise with the Trust's DPO report on school data protection issues.

Operationally the school DPO will process any subject access request and inform the Trust's DPO of actions taken.

When receiving FOI requests the school DPO's will check with the Trust DPO to see if more than one Trust school has received a similar request. The Trust DPO will then determine if the school school process the FOI request themselves of provide to them the details so that a summarised response can be made by the Trust.

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 United Kingdom
- 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

7. Data Protection Principles

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

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

This policy sets out how the school aims to comply with these principles.

8. Collecting Personal Data

8.1 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 GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (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.

8.2 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 Information and Records Management Society's toolkit for schools.

9. 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.

10. Subject Access Requests and other Rights of Individuals

10.1 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 must be submitted in writing, either by letter or email to the DPO. They should include:

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

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

10.2 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 (Primary School):
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 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.

Children aged 12 and above (Secondary School):
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 school 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.

10.3 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.

10.4 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 8), 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 United Kingdom
- 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 school DPO. If staff receive such a request, they must immediately forward it to the school DPO.

11. Parental requests to see an Educational Record

The Bordesley Multi-Academy Trust policy for academies is that whilst not legally required, in a similar way to maintained schools, we give the right for parental access 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.

12. Biometric Recognition Systems

If and where the School uses pupils' biometric data as part of an automated biometric recognition system (for example, pupils use fingerprints to receive school dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school 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 school's biometric system(s). If a biometric system is introduced we will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners in cash at each transaction if they wish.

Parents/carers and pupils can object to participation in a school'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 school'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 school will delete any relevant data already captured.

See the T3-03 Protection of Biometric Information Policy for more information.

13. CCTV

The School may use CCTV in various locations around the school site to ensure it remains safe. If we use CCTV we will adhere to the ICO's code of practice for the use of CCTV.

<<Delete as appropriate>>
This school does not have any CCTV.
or
The school uses Close Circuit Television ("CCTV") within the premises of the School. This policy applies to all members of our Workforce, visitors to the School premises and all other persons whose images may be captured by the CCTV system.

The policy takes account of all applicable legislation and guidance, including:

- General Data Protection Regulation ("GDPR")
- [Data Protection Act 2018] (together the Data Protection Legislation)
- CCTV Code of Practice produced by the Information Commissioner
- Human Rights Act 1998

Purpose of CCTV

The School uses CCTV for the following purposes:

(a) To provide a safe and secure environment for pupils, staff and visitors

(b) To prevent the loss of or damage to the School buildings and/or assets
(c) To assist in the prevention of crime and assist law enforcement agencies in apprehending offenders

Description of system
The School has two separate systems:
System 1, which includes 19-fixed wall and ceiling cameras, attached to either the outside walls (8) of the School building and indoor cameras (11) fixed to watch the corridors of the School. The cameras have no sound ability. All nineteen fixed cameras are hardwired to the recording boxes. The main School system has two recording boxes, each one being attached to a dedicated monitor.
System 2, which includes six, fixed outside wall cameras to the bungalow positioned to observe all entrances to the building. Again, each camera is hardwired to the recorder. These images are viewed on a monitor.

Siting of Cameras
All CCTV cameras will be sited in such a way as to meet the purpose for which the CCTV is operated. Cameras will be sited in prominent positions where they are clearly visible to staff, pupils and visitors.

Cameras will not be sited, so far as possible, in such a way as to record areas that are not intended to be the subject of surveillance. The School will make all reasonable efforts to ensure that areas outside of the School premises are not recorded.

Signs will be erected to inform individuals that they are in an area within which CCTV is in operation.

Cameras will not be sited in areas where individuals have a heightened expectation of privacy, such as changing rooms or toilets.

Privacy Impact Assessment
Prior to the installation of any new CCTV camera, or system, a privacy impact assessment will be conducted by the School to ensure that the proposed installation was and remains compliant with legislation and ICO guidance.

The School will adopt a privacy by design approach when installing new cameras and systems, taking into account the purpose of each camera to avoid recording and storing excessive amounts of personal data.

Management and Access
The CCTV system will be managed by XXX.

On a day-to-day basis, the CCTV system will be operated by XXX.

The viewing of live CCTV images in the main office will be restricted to Senior Leadership Team (SLT), Business Manager, Office staff, Caretaker, Learning Mentor, (teachers as appropriate with supervision from SLT). The live CCTV images in the Learning mentors office will be restricted to Learning mentor and assistant Learning mentor and SLT (when appropriate).

Recorded images which are stored by the CCTV system will be restricted to access by SLT, Business Manager, Caretaker and appropriate staff being supervised.

No other individual will have the right to view or access any CCTV images unless in accordance with the terms of this policy as to disclosure of images.

The CCTV system is checked weekly by XXX to ensure that it is operating effectively.

Storage and Retention of Images
Any images recorded by the CCTV system will be retained only for as long as necessary for the purpose for which they were originally recorded.

Recorded images are stored only for a period of 14 days unless there is a specific purpose for which they are retained for a longer period.
The School will ensure that appropriate security measures are in place to prevent the unlawful or inadvertent disclosure of any recorded images. The measures in place include:

(a) CCTV recording systems being located in restricted access areas;
(b) The CCTV system being password protected;
(c) Restriction of the ability to make copies to specified members of staff

A log of any access to the CCTV images, including time and dates of access, and a record of the individual accessing the images, will be maintained by the School.

Disclosure of Images to Data Subjects
Any individual recorded in any CCTV image is a data subject for the purposes of the Data Protection Legislation, and has a right to request access to those images.

Any individual who requests access to images of themselves will be considered to have made a subject access request pursuant to the Data Protection Legislation. Such a request should be considered in the context of the School's Subject Access Request Procedures included in this policy.

When such a request is made a member of the SLT will review the CCTV footage, in respect of relevant time periods where appropriate, in accordance with the request.

If the footage contains only the individual making the request then the individual may be permitted to view the footage. This must be strictly limited to that footage which contains only images of the individual making the request. The member of SLT must take appropriate measures to ensure that the footage is restricted in this way.

If the footage contains images of other individuals then the School must consider whether:

(a) The request requires the disclosure of the images of individuals other than the requester, for example whether the images can be distorted so as not to identify other individuals;
(b) The other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained; or
(c) If not, then whether it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.

A record must be kept, and held securely, of all disclosures which sets out:

(a) When the request was made;
(b) The process followed by the member of SLT in determining whether the images contained third parties;
(c) The considerations as to whether to allow access to those images;
(d) The individuals that were permitted to view the images and when; and

(e) Whether a copy of the images was provided, and if so to whom, when and in what format.

Disclosure of Images to Third Parties
The School will only disclose recorded CCTV images to third parties where it is permitted to do so in accordance with the Data Protection Legislation.

CCTV images will only be disclosed to law enforcement agencies in line with the purposes for which the CCTV system is in place.

If a request is received from a law enforcement agency for disclosure of CCTV images then a member of the SLT must follow the same process as above in relation to subject access requests. Detail should be obtained from the law enforcement agency as to exactly what they want the CCTV images for, and any particular individuals of concern. This will then enable proper consideration to be given to what should be disclosed, and the potential disclosure of any third party images.

The information above must be recorded in relation to any disclosure.

If an order is granted by a Court for disclosure of CCTV images then this should be complied with. However very careful consideration must be given to exactly what the Court order requires. If there are any concerns as to disclosure then the Data Protection Officer should be contacted in the first instance and appropriate legal advice may be required.

Misuse of CCTV systems
The misuse of CCTV system could constitute a criminal offence.
Any member of staff who breaches this policy may be subject to disciplinary action.

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 Data Protection Officer (DPO)

14. Photographs & Videos

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

At XXX, we use imagery and videos for a variety of purposes, including prospectuses, display boards, educational purposes, conferences, the school website and school subject twitter accounts. We understand that parents may also wish to take videos or photos of their children participating in school events for personal use.

Whilst we recognise the benefits of photography and videos to our school community, we also understand that these can have significant risks for those involved. Under the legal obligations of the General Data Protection Regulation (GDPR), the school has specific responsibilities in terms of how photos and videos are taken, stored and retained.

The school has implemented a policy on the safe use of cameras and videos by staff and parents to reflect the protective ethos of the school with regard to pupils' safety.

In order to ensure that, as far as possible, the use of photography and video is used safely at all times, the policy provided below should be followed. This policy is applicable to all forms of visual media, including film, print, video, DVD and websites.

This policy has due regard to legislation, including, but not limited to, the following:

(a) The General Data Protection Regulation (GDPR)
(b) The Freedom of Information Act 2000
(c) The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
(d) The School Standards and Framework Act 1998
(e) The Children Act 1989
(f) The Children Act 2004
(g) The Equality Act 2010

This policy has been created with regard to the following guidance:

(a) Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
(b) Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'

This policy also has due regard to the school's policies, including, but not limited to, the following:

(a) SEND Policy
(b) Behavioural Policy
(d) Social Media Policy

Roles and responsibilities

The headteacher is responsible for:

(a) Submitting consent forms to parents/carers at the beginning of the academic year with regards to photographs and videos being taken whilst at school.
(b) Ensuring that all photos and videos are stored and disposed of correctly, in line with the GDPR.
(c) Deciding whether parents are permitted to take photographs and videos during school events.
(d) Communicating this policy to all the relevant staff members and the wider school community, such as parents/carers.

The designated safeguarding lead (DSL) is responsible for:

(a) Liaising with the data protection officer (DPO), to ensure there are no data protection breaches.
(b) Informing the headteacher (if not already the DSL) of any known changes to a pupil's security, e.g. child protection concerns, which would mean that participating in photography and video recordings would put them at significant risk.

The designated child looked after lead (CLA lead) is responsible for:

(a) Liaising with social workers to gain consent for photography and videos of LAC pupils.

Parents are responsible for:

(a) Completing the Consent Form on entry of their child to the school.
(b) Informing the school in writing where there are any changes to their consent.
(c) Updating the consent form if there is a change to their views by letting the school know in writing of this change.
(d) Acting in accordance with this policy.

The DPO is responsible for:

(a) Informing and advising the school and its employees about their obligations to comply with the GDPR in relation to photographs and videos at school.
(b) Monitoring the school's compliance with the GDPR in regards to processing photographs and videos.

(c) Advising on data protection impact assessments in relation to photographs and videos at school.
(d) Conducting internal audits, in regards to the school's procedures for obtaining, processing and using photographs and videos.
(e) Providing the required training to staff members, in relation to how the GDPR impacts photographs and videos at school.

Parental consent

The school understands that consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.
Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

Where consent is given, a record will be kept documenting how and when consent was given and last updated.

The school ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data will be found, or the processing will cease.

Where a child is under the age of 13, the consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child.

Children as young as 13 may be permitted to provide consent to the processing of their data. However, the school will also seek the consent of the parents as well.

All parents will be asked to complete the Consent Form on an annual basis, which will determine whether or not they allow their child to participate in photographs and videos.

The Consent Form will be valid for the full academic year, unless the pupil's circumstances change in any way, e.g. if their parents separate, or consent is withdrawn. Additional consent forms will be required if the pupil's circumstances change.

If there is a disagreement over consent, or if a parent does not respond to a consent request, it will be treated as if consent has not been given, and photographs and videos will not be taken or published of the pupil whose parents have not consented.

All parents are entitled to withdraw or change their consent at any time during the school year.

Parents will be required to confirm on the Consent Form, in writing, that they will notify the school if their child's circumstances change in any way, or if they wish to withdraw their consent.

For any LAC pupils, or pupils who are adopted, the CLA lead will liaise with the pupil's social worker, carers or adoptive parents to establish where consent should be sought. Consideration will be given as to whether identification of an LAC pupil, or pupils who are adopted, would risk their security in any way.

Consideration will also be given to any pupils for whom child protection concerns have been raised. Should the DSL believe that taking photographs and videos of any pupils would put their security at further risk, greater care will be taken towards protecting their identity.

A list of all the names of pupils for whom consent was not given will be created by the DPO and will be circulated to all staff members via the school office. This list will be updated annually, when new consent forms are provided.

If any parent withdraws or changes their consent, or the CLA Lead / DSL reports any changes to a pupil's security risk, or there are any other changes to consent, the list will also be updated and re-circulated.

General procedures
Photographs and videos of pupils will be carefully planned before any activity.

The DPO will oversee the planning of any events where photographs and videos will be taken. Where photographs and videos will involve LAC pupils, adopted pupils, or pupils for whom there are security concerns, the headteacher will liaise with the DSL to determine the steps involved.

When organising photography and videos of pupils, the headteacher, as well as any other staff members involved, will consider the following:

(a) Can general shots of classrooms or group activities, rather than individual shots of pupils, be used to fulfil the same purpose?
(b) Could the camera angle be amended in any way to avoid pupils being identified?
(c) Will pupils be suitably dressed to be photographed and videoed?
(d) Will pupils of different ethnic backgrounds and abilities be included within the photographs or videos to support diversity?
(e) Would it be appropriate to edit the photos or videos in any way? E.g. to remove logos which may identify pupils?
(f) Are the photographs and videos of the pupils completely necessary, or could alternative methods be used for the same purpose? E.g. could an article be illustrated by pupils' work rather than images or videos of the pupils themselves?

The list of all pupils of whom photographs and videos must not be taken will be checked prior to the activity. Only pupils for whom consent has been given will be able to participate.

The staff members involved, alongside the headteacher and DPO, will liaise with the DSL/CLA lead if any LAC pupil, adopted pupil, or a pupil for whom there are security concerns is involved.

School equipment will be used to take photographs and videos of pupils. Exceptions to this are outlined in below.

Staff will ensure that all pupils are suitably dressed before taking any photographs or videos.

Where possible, staff will avoid identifying pupils. If names are required, only first names will be used.

The school will not use images or footage of any pupil who is subject to a court order.

The school will not use photographs of children or staff members who have left the school, without parental consent.

Photos and videos that may cause any distress, upset or embarrassment will not be used.

Any concern relating to inappropriate or intrusive photography or publication of content is to be reported to the DPO.

Additional safeguarding procedures
The school understands that certain circumstances may put a pupil's security at greater risk and, thus, may mean extra precautions are required to protect their identity.

The DSL / CLA lead will, in known cases of a pupil who is an LAC or who has been adopted, liaise with the pupil's social worker, carers or adoptive parents to assess the needs and risks associated with the pupil.

Any measures required will be determined between the DSL / CLA Lead (for LAC pupils), social worker, carers, DPO and adoptive parents with a view to minimise any impact on the pupil's day-to-day life. The measures implemented will be one of the following:

(a) Photos and videos can be taken as per usual school procedures.
(b) Photos and videos can be taken within school for educational purposes and official school use, e.g. on registers, but cannot be published online or in external media.
(c) No photos or videos can be taken at any time, for any purposes.

Any outcomes will be communicated to all staff members via a staff meeting and the list outlining which pupils are not to be involved in any videos or photographs, held in the school office, will be updated accordingly.

School-owned devices

Staff are encouraged to take photos and videos of pupils using school equipment; however, they may use other equipment, such as school-owned mobile devices, where the DPO has been consulted and consent has been sought from the headteacher prior to the activity.

Where school-owned devices are used, images and videos will be provided to the school at the earliest opportunity, and removed from any other devices.

Staff will not use their personal mobile phones, or any other personal device, to take images and videos of pupils.

Photographs and videos taken by staff members on school visits may be used for educational purposes, e.g. on displays or to illustrate the work of the school, where consent has been obtained.

Digital photographs and videos held on the school's drive are accessible to staff only. Photographs and videos are stored in labelled files, annotated with the date, and are only identifiable by year group/class number – no names are associated with images and videos. The folder containing these files is password protected, and only staff members have access to this password(s) – these are updated termly to minimise the risk of access by unauthorised individuals.

Use of a professional photographer

If the school decides to use a professional photographer for official school photos and school events, the headteacher will:

(a) Provide a clear brief for the photographer about what is considered appropriate, in terms of both content and behaviour.
(b) Issue the photographer with identification, which must be worn at all times.
(c) Let pupils and parents know that a photographer will be in attendance at an event and ensure they have previously provided consent to both the taking and publication of videos or photographs.
(d) Not allow unsupervised access to pupils or one-to-one photo sessions at events.
(e) Communicate to the photographer that the material may only be used for the school's own purposes and that permission has not been given to use the photographs for any other purpose.
(f) Ensure that the photographer will comply with the requirements set out in GDPR.
(g) Ensure that if another individual, such as a parent or governor, is nominated to be the photographer, they are clear that the images or videos are not used for any other anything other than the purpose indicated by the school.

Permissible photography and videos during school events

If the headteacher permits parents to take photographs or videos during a school event, parents will:

(a) Remain seated while taking photographs or videos during concerts, performances and other events.
(b) Minimise the use of flash photography during performances.
(c) In the case of all school events, make the focus of any photographs or videos their own children.
(d) Avoid disturbing others in the audience or distracting pupils when taking photographs or recording video.
(e) Ensure that any images and recordings taken at school events are exclusively for personal use and are not uploaded to the internet, posted on social networking sites or openly shared in other ways.
(f) Refrain from taking further photographs and/or videos if and when requested to do so by staff.

Storage and retention

Images obtained by the school will not be kept for longer than necessary.

Hard copies of photos and video recordings held by the school will be annotated with the date on which they were taken and will be stored securely. They will not be used other than for their original purpose, unless permission is sought from the headteacher and parents of the pupils involved and the DPO has been consulted.

Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

The DPO will review stored images and videos on a termly basis to ensure that all unwanted material has been deleted.

Parents must inform the school in writing where they wish to withdraw or change their consent. If they do so, any related imagery and videos involving their children will be removed from the school drive immediately.

When a parent withdraws consent, it will not affect the use of any images or videos for which consent had already been obtained. Withdrawal of consent will only affect further processing.

Where a pupil's security risk has changed, the DSL will inform the headteacher immediately. If required, any related imagery and videos involving the pupil will be removed from the school drive immediately. Hard copies will be removed by returning to their parents or by shredding, as appropriate.

Official school photos are held on the school's MIS alongside other personal information, and are retained for the length of the pupil's attendance at the school, or longer, if necessary, e.g. due to a police investigation.

Some educational records relating to former pupils of the school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

See our Safeguarding and Child Protection Policy for more information on our use of photographs and videos.

15. Data Protection by Design & 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 7)
- 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 advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- 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 school 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

16. Data Security & 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 will be mindful of keeping it safe.
- Secure passwords 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 where personal information is stored
- Staff, pupils or governors 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 on acceptable use)
- 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 9)

17. 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.

18. Personal Data Breaches

The school 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 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may 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

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 school's processes make it necessary.

Appendix 1 – 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
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the headteacher and the chair of governors
- 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 by the DPO on the Trust's central systems.
- 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
    - 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 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
    - Effects
    - 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 by the DPO on the Trust's central systems.
- The DPO and headteacher 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

We 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 school website
- Non-anonymised pupil exam results or staff pay information being shared with governors
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- The school's cashless payment provider being hacked and parents' financial details stolen

Appendix 2 – Model Privacy Notices

Privacy notice for parents/carers

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about **pupils**. The school is the 'data controller' for the purposes of data protection law.

Our data protection officer and contact details are below(see 'Contact us' below).

The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about pupils includes, but is not restricted to:

- Contact details, contact preferences, date of birth, identification documents
- Results of internal assessments and externally set tests
- Pupil and curricular records
- Characteristics, such as ethnic background, eligibility for free school meals, or special educational needs
- Exclusion information
- Details of any medical conditions, including physical and mental health
- Attendance information
- Safeguarding information
- Details of any support received, including care packages, plans and support providers
- Photographs
- CCTV images captured in school

We may also hold data about pupils that we have received from other organisations, including other schools, local authorities and the Department for Education.

Why we use this data

We use this data to:

- Support pupil learning
- Monitor and report on pupil progress
- Provide appropriate pastoral care
- Protect pupil welfare
- Assess the quality of our services
- Administer admissions waiting lists
- Carry out research
- Comply with the law regarding data sharing

Our legal basis for using this data

We only collect and use pupils' personal data when the law allows us to. Most commonly, we process it where:

- We need to comply with a legal obligation
- We need it to perform an official task in the public interest

Less commonly, we may also process pupils' personal data in situations where:

- We have obtained consent to use it in a certain way
- We need to protect the individual's vital interests (or someone else's interests)

Where we have obtained consent to use pupils' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

Some of the reasons listed above for collecting and using pupils' personal data overlap, and there may be several grounds which justify our use of this data.

Collecting this information
While the majority of information we collect about pupils is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you or your child, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

How we store this data
We keep personal information about pupils while they are attending our school. We may also keep it beyond their attendance at our school if this is necessary in order to comply with our legal obligations.

Please refer to the Information and Records Management Society's toolkit for schools.

Data sharing
We do not share information about pupils with any third party without consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about pupils with:

- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and exclusions
- The Department for Education
- The pupil's family and representatives
- Educators and examining bodies
- Our regulator [specify as appropriate, e.g. Ofsted, Independent Schools Inspectorate]
- Suppliers and service providers – to enable them to provide the service we have contracted them for
- Financial organisations
- Central and local government
- Our auditors
- Survey and research organisations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals
- Professional bodies

National Pupil Database

We are required to provide information about pupils to the Department for Education as part of statutory data collections such as the school and early years census if applicable.

Some of this information is then stored in the National Pupil Database (NPD), which is owned and managed by the Department and provides evidence on school performance to inform research.

The database is held electronically so it can easily be turned into statistics. The information is securely collected from a range of sources including schools, local authorities and exam boards.

The Department for Education may share information from the NPD with other organisations which promote children's education or wellbeing in England. Such organisations must agree to strict terms and conditions about how they will use the data. For more information, see the Department's webpage on how it collects and shares research data.

You can also contact the Department for Education with any further questions about the NPD.

Schools with pupils aged 13 and above - Youth support services
Once our pupils reach the age of 13, we are legally required to pass on certain information about them to [name of local authority or youth support services provider in your area], as it has legal responsibilities regarding the education or training of 13-19 year-olds.

This information enables it to provide youth support services, post-16 education and training services, and careers advisers.

Parents/carers, or pupils once aged 16 or over, can contact our data protection officer to request that we only pass the individual's name, address and date of birth to the relevant local authority or youth support service provider.

Transferring data internationally
Where we transfer personal data to a country or territory outside the United Kingdom, we will do so in accordance with data protection law.

Parents and pupils' rights regarding personal data
Individuals have a right to make a **'subject access request'** to gain access to personal information that the school holds about them.

Parents/carers can make a request with respect to their child's data where the child is not considered mature enough to understand their rights over their own data (usually under the age of 12), or where the child has provided consent.

Parents also have the right to make a subject access request with respect to any personal data the school holds about them.

If you make a subject access request, and if we do hold information about you or your child, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you or your child
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form
  Individuals also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances.
  If you would like to make a request please contact our data protection officer.

Other rights
Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe, including the right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent it being used to send direct marketing
- Object to decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our data protection officer.

Complaints
We take any complaints about our collection and use of personal information very seriously. If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us
If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our **data protection officer**:

BMAT Data Protection Officer
Shaw Goodwin
Bordesley Multi-Academy Trust
C/O Trinity High school,
Easemore Road,
Redditch,
Worcestershire,
B98 8HB.

Email: goodwins@bmat.net
Telephone: 01527 330001

This notice is based on the Department for Education's model privacy notice for pupils, amended for parents and to reflect the way we use data in this school.

Privacy notice for pupils

You have a legal right to be informed about how our school uses any personal information that we hold about you. To comply with this, we provide a 'privacy notice' to you where we are processing your personal data.

This privacy notice explains how we collect, store and use personal data about you. We, the school, are the 'data controller' for the purposes of data protection law.

Our data protection officer is listed below (see 'Contact us' below).

The personal data we hold

We hold some personal information about you to make sure we can help you learn and look after you at school.

For the same reasons, we get information about you from some other places too – like other schools, the local council and the government.

This information includes:

- Your contact details
- Your test results
- Your attendance records
- Your characteristics, like your ethnic background or any special educational needs
- Any medical conditions you have
- Details of any behaviour issues or exclusions
- Photographs
- CCTV images

Why we use this data

We use this data to help run the school, including to:

- Get in touch with you and your parents when we need to
- Check how you're doing in exams and work out whether you or your teachers need any extra help
- Track how well the school as a whole is performing
- Look after your wellbeing

Our legal basis for using this data

We will only collect and use your information when the law allows us to. Most often, we will use your information where:

- We need to comply with the law
- We need to use it to carry out a task in the public interest (in order to provide you with an education)

Sometimes, we may also use your personal information where:

- You, or your parents/carers have given us permission to use it in a certain way
- We need to protect your interests (or someone else's interest)

Where we have got permission to use your data, you or your parents/carers may withdraw this at any time. We will make this clear when we ask for permission, and explain how to go about withdrawing consent.

Some of the reasons listed above for collecting and using your information overlap, and there may be several grounds which mean we can use your data.

Collecting this information
While in most cases you, or your parents/carers, must provide the personal information we need to collect, there are some occasions when you can choose whether or not to provide the data.

We will always tell you if it's optional. If you must provide the data, we will explain what might happen if you don't.

How we store this data
We will keep personal information about you while you are a pupil at our school. We may also keep it after you have left the school, where we are required to by law.

The Information and Records Management Society's toolkit for schools sets out how long we must keep information about pupils.

Data sharing
We do not share personal information about you with anyone outside the school without permission from you or your parents/carers, unless the law and our policies allow us to do so.

Where it is legally required, or necessary for another reason allowed under data protection law, we may share personal information about you with:

- Our local authority – to meet our legal duties to share certain information with it, such as concerns about pupils' safety and exclusions
- The Department for Education (a government department)
- Your family and representatives
- Educators and examining bodies
- Our regulator (the organisation or "watchdog" that supervises us), ([specify as appropriate, e.g. Ofsted, Independent Schools Inspectorate]
- Suppliers and service providers – so that they can provide the services we have contracted them for
- Financial organisations
- Central and local government
- Our auditors
- Survey and research organisations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals
- Professional bodies

National Pupil Database
We are required to provide information about you to the Department for Education (a government department) as part of data collections such as the school census.

Some of this information is then stored in the National Pupil Database, which is managed by the Department for Education and provides evidence on how schools are performing.
This, in turn, supports research.

The database is held electronically so it can easily be turned into statistics. The information it holds is collected securely from schools, local authorities, exam boards and others.

The Department for Education may share information from the database with other organisations which promote children's education or wellbeing in England. These organisations must agree to strict terms and conditions about how they will use your data.

You can find more information about this on the Department for Education's webpage on how it collects and shares research data.

You can also contact the Department for Education if you have any questions about the database.

Schools with pupils aged 13 years and over - Youth support services
Once you reach the age of 13, we are legally required to pass on certain information about you to the relevant local authority as it has legal responsibilities regarding the education or training of 13-19 year-olds.

This information enables it to provide youth support services, post-16 education and training services, and careers advisers.

Your parents/carers, or you once you're 16, can contact our data protection officer to ask us to only pass your name, address and date of birth to the relevant local authority or local youth service provider.

Transferring data internationally
Where we share data with an organisation that is based outside the United Kingdom, we will protect your data by following data protection law.

Your rights

a. How to access personal information we hold about you

You can find out if we hold any personal information about you, and how we use it, by making a **'subject access request'**, as long as we judge that you can properly understand your rights and what they mean.

If we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and using it, and how long we will keep it for
- Explain where we got it from, if not from you or your parents
- Tell you who it has been, or will be, shared with
- Let you know if we are using your data to make any automated decisions (decisions being taken by a computer or machine, rather than by a person)
- Give you a copy of the information

You may also ask us to send your personal information to another organisation electronically in certain circumstances.

If you want to make a request please contact our data protection officer.

b. Your other rights over your data

You have other rights over how your personal data is used and kept safe, including the right to:

- Say that you don't want it to be used if this would cause, or is causing, harm or distress
- Stop it being used to send you marketing materials
- Say that you don't want it used to make automated decisions (decisions made by a computer or machine, rather than by a person)
- Have it corrected, deleted or destroyed if it is wrong, or restrict our use of it

- Claim compensation if the data protection rules are broken and this harms you in some way

Complaints
We take any complaints about how we collect and use your personal data very seriously, so please let us know if you think we've done something wrong.

You can make a complaint at any time by contacting our data protection officer.

You can also complain to the Information Commissioner's Office in one of the following ways:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113 • Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us
If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our data protection officer:

BMAT Data Protection Officer
Shaw Goodwin
Bordesley Multi-Academy Trust
C/O Trinity High school,
Easemore Road,
Redditch,
Worcestershire,
B98 8HB.

Email: goodwins@bmat.net
Telephone: 01527 330001

This notice is based on the Department for Education's model privacy notice for pupils, amended to reflect the way we use data in this school.

Privacy notice for staff

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about individuals we employ, or otherwise engage, to work at our school.

We, the school, are the 'data controller' for the purposes of data protection law.

Our data protection officer is listed below (see 'Contact us' below).

The personal data we hold

We process data relating to those we employ, or otherwise engage, to work at our school. Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Contact details
- Date of birth, marital status and gender
- Next of kin and emergency contact numbers
- Salary, annual leave, pension and benefits information
- Bank account details, payroll records, National Insurance number and tax status information
- Recruitment information, including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process
- Qualifications and employment records, including work history, job titles, working hours, training records and professional memberships
- Performance information
- Outcomes of any disciplinary and/or grievance procedures
- Absence data
- Copy of driving licence
- Photographs
- CCTV footage
- Data about your use of the school's information and communications system

We may also collect, store and use information about you that falls into "special categories" of more sensitive personal data. This includes information about (where applicable):

- Race, ethnicity, religious beliefs, sexual orientation and political opinions
- Trade union membership
- Health, including any medical conditions, and sickness records

Why we use this data

The purpose of processing this data is to help us run the school, including to:

- Enable you to be paid
- Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- Support effective performance management
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Improve the management of workforce data across the sector
- Support the work of the School Teachers' Review Body

Our lawful basis for using this data
We only collect and use personal information about you when the law allows us to. Most commonly, we use it where we need to:

- Fulfil a contract we have entered into with you
- Comply with a legal obligation
- Carry out a task in the public interest

Less commonly, we may also use personal information about you where:

- You have given us consent to use it in a certain way
- We need to protect your vital interests (or someone else's interests)
- We have legitimate interests in processing the data

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you go about withdrawing consent if you wish to do so.

Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds which justify the school's use of your data.

Collecting this information
While the majority of information we collect from you is mandatory, there is some information that you can choose whether or not to provide to us.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

How we store this data
We create and maintain an employment file for each staff member. The information contained in this file is kept secure and is only used for purposes directly relevant to your employment.

Once your employment with us has ended, we will retain this file and delete the information in it in accordance with the Information and Records Management Society's toolkit for schools

Data sharing
We do not share information about you with any third party without your consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about you with:

- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and [maintained schools only] information about headteacher performance and staff dismissals
- The Department for Education
- Your family or representatives
- Educators and examining bodies
- Our regulator [specify as appropriate e.g. Ofsted, Independent Schools Inspectorate]
- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as payroll
- Financial organisations
- Central and local government
- Our auditors
- Survey and research organisations
- Trade unions and associations

- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals
- Professional bodies
- Employment and recruitment agencies

Transferring data internationally
Where we transfer personal data to a country or territory outside the United Kingdom, we will do so in accordance with data protection law.

Your rights

a. How to access personal information we hold about you

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

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact our data protection officer.

b. Your other rights regarding your data

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

- Object to the use of your personal data if it would cause, or is causing, damage or distress
- Prevent your data being used to send direct marketing
- Object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)

- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our data protection officer.

Complaints
We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113 • Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our **data protection officer**:

BMAT Data Protection Officer
Shaw Goodwin
Bordesley Multi-Academy Trust
C/O Trinity High school,
Easemore Road,
Redditch,
Worcestershire,
B98 8HB.

Email: goodwins@bmat.net
Telephone: 01527 330001

This notice is based on the Department for Education's model privacy notice for the school workforce, amended to reflect the way we use data in this school.