GDPR Policy and Privacy Notices

AUTHOR:	Chief Operations Officer
APPROVED BY:	Board of Trustees
DATE:	May 2018
LAST REVIEWED ON:	May 2018
NEXT REVIEW DUE BY:	May 2020

Contents

1. Aims

Bedfordshire Schools Trust (BEST) aims to ensure that all personal data collected about staff, pupils/students, parents/carers, governors, trustees, visitors and other individuals is collected, stored and processed in accordance with the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill. This policy applies to all 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 expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects 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

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 • Criminal convictions
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 for which, and the manner in which, personal data is processed.
Data Protection Officer (DPO)	A person whose role is to oversee data compliance, advise and recommend improvements and be the point of contact for data protection. The DPO has overall responsibility and oversight but does not carry out all duties personally. See Role of DPO on page 5.
Data Protection Lead (DPL)	A person in each school with responsibility, delegated by the DPO and Principal, for data protection compliance. Whilst the Data Protection Lead manages the day to day data protection compliance, the overall responsibility for the school remains with the Principal.
Data Processor	A person, other than an employee of the data controller, who processes the data on behalf of the data controller

4. The Data Controller

BEST processes personal information relating to pupils/students, parents/carers, staff, governors, trustees, visitors and others, and, therefore, is a data controller. BEST delegates the responsibility of data protection to the DPO (Chief Operations Officer).

BEST is registered as a data controller with the Information Commissioner's Office (ICO) and renews this registration annually or as otherwise legally required.

5. Roles and Responsibilities

BEST has overall responsibility for ensuring that all entities of BEST comply with its obligations under the Data Protection Act 2018.

Day-to-day responsibilities rest with the Principal of each school, or Deputy Principal in their absence. The Principal may delegate the management of this to the Data Protection Lead in their school.

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

Responsibilities of Trustees

The Trustees are responsible for:

- overall responsibility for ensuring that the Trust and it's entities comply with the current legislation and statutory requirements
- approval of the implementation plan and policy

Responsibilities of Data Protection Officer (DPO)

The DPO is responsible for:

- setting the principles of data protection compliance
- informing and advising the school and its employees about GDPR obligations and other data protection laws
- informing and advising any processor engaged with the school
- monitoring the implementation and application of the GDPR and data protection policies
- advise on queries relating to privacy impact assessments and breaches
- ensuring that consistent training is taking place throughout the Trust (including Data Protection Leads and staff)
- ensuring that internal audits are carried out by the Data Protection Lead
- being the point of contact for the Information Commissioner's Officer (ICO)
- providing a compliance report to Trustees at six monthly intervals (audit carried out annually)

The DPO is accountable to the Trustees.

Responsibilities of the Principal

The Principal is accountable for GDPR within their school and will ensure that:

- all staff are aware of their data protection obligations
- GDPR/data protection is appropriately resourced
- the school is GDPR compliant and that this policy is adhered to
- there is a nominated Data Protection Lead for the school
- that they are always available to the Data Protection Lead
- GDPR/data protection compliance is reported to the Local Governing Body at regular intervals

The Principal is accountable to the CEO and Local Governing Body.

Responsibilities of Data Protection Lead (DPL)

The Data Protection Lead is responsible for:

- overseeing GDPR/data protection compliance within their school in accordance with this policy
- ensuring that impact risk assessments are carried out as appropriate

- informing and advising the school and its employees about GDPR obligations and other data protection laws
- informing and advising any processor engaged with the school
- monitoring the implementation and application of the GDPR and data protection policies within their school
- carry out internal audits
- being the point of contact for the DPO
- dealing with any data breach issues and ensuring that these are reported up to the DPO in accordance with this policy
- ensuring that staff receive training as instructed by the DPO
- providing reports to Principal and DPO as appropriate – the Principal will present the report to the Local Governing Body

The Data Protection Lead is accountable to the Principal and DPO.

Responsibilities of the Local Governing Body (LGB)

The LGB are responsible for:

- ensuring that their school complies with all relevant data protection obligations
- ensuring that they receive a regular report on GDPR/data protection and challenge the Principal as appropriate

The Local Governing Body are accountable to the CEO and Trustees.

Responsibilities of Staff

Staff are responsible for:

- ensuring that they collect, store and process any personal data in accordance with this policy
- informing the school of any changes to their personal data, such as a change of address
- ensuring that they are aware of the name and contact details for the DPO and DPL
- contacting the DPO or DPL 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 BEST schools/entities 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 BEST and its entities aim to comply with these principles.

The new provisions are designed to develop the protection of children's personal data and rights for individuals. These rights are as follows.

- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in automated decision-making and profiling

7. Collecting & Sharing Personal Data

BEST and its entities will only process personal data when one of six 'lawful bases' (legal reasons) to do so under data protection law occur.

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

For primary age pupils - If online services are offered to pupils, such as classroom apps, and the school intends to rely on consent as a basis for processing, the school will get parental consent (except for online counselling and preventive services).

For secondary age pupils - If online services are offered to pupils, such as classroom apps, and the school intends to rely on consent as a basis for processing, the school will get parental consent where the pupil is under 13 (except for online counselling and preventive services).

Whenever BEST and its entities collect personal data directly from individuals, relevant information required by data protection law will be provided.

Limitation, minimisation and accuracy

BEST and its entities will only collect personal data for specified, explicit and legitimate reasons. The reasons will be explained to the individuals when data is first collected.

If personal data is used for reasons other than those given, the individuals concerned will be informed prior to any action being taken, and consent will be sought 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 Trust retention schedule.

Sharing personal data

BEST and its entities 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
- They need to liaise with other agencies and schools – they will seek consent as necessary before doing this
- Suppliers or contractors need data to enable them to provide services to the staff and pupils – for example, IT companies. When doing this, BEST and its entities will:
    - Only appoint suppliers or contractors who 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 shared
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with BEST and its entities

BEST and its entities will also share personal data with law enforcement and government bodies where they 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 safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

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

Where personal data is transferred to a country or territory outside the European Economic Area, this will be carried out in accordance with data protection law.

BEST and its entities will adhere to the following when consent is obtained.

- Consent must be freely given, specific, informed and unambiguous, and a positive affirmation of the individual's agreement
- Consent will not be 'bundled in' with other consent – it will be specific and clear

- Withdrawal of consent will be as easy as granting of consent

8. Privacy/Fair Processing Notice

BEST and its entities hold Privacy Notices for the following (see Appendix A).

- How we use pupil/student information
- How we use pupil information – parent/carer notice
- How we use staff information

9. External Contractors / Third Parties

BEST and its entities will ensure that all suppliers who process personal information have demonstrated GDPR compliance and technical and organisational security measures. A GDPR policy should be sought from all suppliers. BEST and its entities will keep a schedule of suppliers including date policy received.

10. Subject Access Requests

Under the Data Protection Act 2018 and GDPR legislation, individuals have a right to request access to information the school holds about them. This is known as a subject access request.

Subject access requests must be submitted in writing, either by letter or email (see Appendix B for Access Request Form).

BEST and its entities will seek to confirm the identity of the person making the request by:

- asking for two forms of identification
- contacting the individual by telephone to confirm the request

BEST and its entities **will** provide the following to data subjects on request:

- 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

BEST and its entities will **not** reveal the following information in response to subject access requests:

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

If staff receive a subject access request they must immediately forward it to the DPL for their school/entity.

Subject access requests for all or part of the pupil/student's educational record will be provided within one month of the request being received. However, BEST reserves the right to extend this deadline by a further two months should the request be complex.

There is no fee for subject access requests. However, manifestly unfounded or excessive requests may be charged a reasonable fee. Additional copies requested may be charged depending on administrative costs involved.

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 13 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 BEST schools 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 13 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 BEST schools 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.

If a request is refused, BEST and its entities will tell the individual why and tell them they have the right to complain to ICO.

11. Biometric recognition systems

Where BEST and its entities use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash or library book loans), the school/entity 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/entity will get written consent from at least one parent or carer before taking any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the biometric system(s). The school/entity will provide alternative means of accessing the relevant services for those pupils.

Parents/carers and pupils can object to participation in the biometric recognition system(s), or withdraw consent, at any time, and the school/entity 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, the school/entity 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 biometric system(s), the school/entity 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/entity will delete any relevant data already captured.

12. CCTV

CCTV is used on various BEST sites to ensure they remain safe. BEST and its entities will adhere to ICO's code of practice for the use of CCTV.

BEST and its entities do not need to ask individuals' permission to use CCTV, but will 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 DPL.

13. Photographs and videos

As part of Trust and school activities, photographs may be taken and images recorded of individuals within the Trust.

For primary age pupils - written consent will be obtained from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. A clear explanation of how the photograph and/or video will be used will be given to both the parent/carer and pupil.

For secondary age pupils - written consent will be obtained from parents/carers, or pupils aged 13 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where parental consent is required, a clear explanation of how the photograph and/or video will be used will be given to both the parent/carer and pupil. Where parental consent is not required, a clear explanation will be given to the pupil about how the photograph and/or video will be used.

Uses may include:

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

Consent can be refused or withdrawn at any time. If consent is withdrawn, BEST and its entities will make reasonable endeavours to delete the photograph or video and not distribute it further.

When using photographs and videos, personal information about the child will not be supplied, to ensure they cannot be identified, unless consent has been given.

See the school Safeguarding/Child Protection Polices for more information on our use of photographs and videos.

BEST and its entities do not take responsibility for images copied or saved by individuals once information is in the public domain.

14. Storage and security of records

All staff and pupils must follow the guidelines set out below.

Personal computing and storage devices including downloading personal information	**Emails** - may be accessed via personal computing devices (such as mobile phones, iPads or tablets) as long as: • Device is password protected and password is not shared (mandatory requirement) • Emails or app is password protected and password is not shared (if device has the required functionality) **Personal laptops/computers** – may be used to access school files/emails as long as:

	• Device/machine is password protected and password is not shared • Emails or apps is password protected and password is not shared • Preferred method of access to information is via VPN, remote access or cloud • Device/machine must have adequate anti-virus software installed • Information may only be downloaded if the device has been secured as stated above – it is recommended that downloaded information is removed as soon as possible • Staff should only access information on personal devices / off site if absolutely necessary – schools may choose to have a 'school laptop' available for such occasions **Personal storage devices (such as USBs) –** preferred method of storage is cloud storage. However, personal storage devices may be used as long as the device has been encrypted. IT are able to encrypt USBs if necessary.
Social Media (accessed via mobile phone, tablet etc)	Any Trust or school related social media may only be accessed via personal computing devices if the device has been secured as stated above. Any personal information saved to the device to upload (such as photographs) should be deleted immediately once posted.
Cloud storage	Only Trust/school cloud storage should be used to store information. The cloud will be password protected. However, if a short cut is saved to the machine/device, the machine/device must be secured as stated above. Personal cloud storage should not be used.
Sending personal information electronically (such as email)	**Personal email accounts** should not be used, only school email accounts. Emails should not be forwarded to personal accounts. **Personal information sent by email outside of BEST** - should be sent via a secure method. IT are able to advise as to the most appropriate method. **Email retention**: • Deleted email box – will be automatically set to delete every 90 days • Sent email box – will be automatically set to delete between 18 months to 2 yearly – any emails staff wish to retain should be moved to a subfolder of the main inbox **Trustees/governors –** should only receive anonymised information. No names of staff or children should be included in documents circulated. **Information downloaded from emails –** staff should be made aware of how to download information safely.
Password security	**Regularity of password change –** rules for passwords and regularity of password updates will be enforced: • Staff – complexity rules will be enforced with 180 day updates – this applies to machines and emails

	• Pupils/students – annual password update **Screen locked –** all screens must be locked when the user leaves the room.
Retention of electronic data after a staff member has left	It is the responsibility of the line manager/head of department to liaise with the IT provider concerning the retention/handover of data from a leaver. Leavers will not be provided with a copy of any data once they have left.
Paper storage	Staff must always: • Ensure personal information is not visible on their desk and that the desk is clear when the room is unoccupied • All personal information to be securely stored if the office is unoccupied • Noticeboards – information to be discretely positioned and mindful that sensitive information may not be appropriate for display • Taking files containing personal information off site – if personal information is taken off site, it must be: o Securely stored – covered/locked o Only taken off site if absolutely necessary Any breach will be reportable and may result in disciplinary action. Preferred method of removal of personal information from site is electronic not paper.

15. Retention and disposal of records

Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely.

For example, BEST and its entities will shred or incinerate paper-based records, and override electronic files. An outside company may be used to safely dispose of records.

See the Retention Schedule in Appendix C for details of timescales and method of disposal.

16. Data breaches

BEST and its entities will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, the procedure set out in Appendix D will be followed.

When appropriate, the data breach will be reported 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

17. Training

BEST 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 or the school's processes make it necessary.

18. Monitoring arrangements

The DPL is responsible for overseeing the GDPR/data protection compliance within their school in accordance with this policy. The DPL will provide an annual report to the Local Governing Body including audit outcomes and the number of breaches/near misses that have occurred during that year.

The DPO is responsible for monitoring and reviewing this policy. The DPO checks that the schools comply with this policy by carrying out an annual audit. An interim and annual report will be presented to the Board of Trustees.

This policy will be reviewed two yearly or as required due to change in legislation, and approved by the Board of Trustees. The policy will be uploaded to the Trust website and shared with all staff and governors internally.

19. Links with other policies

- Freedom of Information Policy and Publication Scheme
- Recruitment and selection
- E-safety
- Safeguarding and child protection
- Social media
- Confidentiality agreement
- Whistleblowing
- IT Acceptable Use Policy

During the cycle of review, all policies will be reviewed to ensure compliance with the GDPR legislation.

20. Appendices

- Appendix A – Privacy Notices
- Appendix B – Access Request Form
- Appendix C – Retention Schedule
- Appendix D – Data Breach Procedure

Appendix A – Privacy Notices – Parent/Carer

Privacy Notice for Parents/Carers (How we use pupil information)

Introduction

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[1].

We, Bedfordshire Schools Trust (BEST), are the 'data controller' for the purposes of Data Protection law. Our Data Protection Officer is Craig Smith, Chief Operating Officer (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, nationality, language, eligibility for free school meals, or special educational needs
- Exclusion information
- Details of any medical conditions, including physical and mental health
- Attendance & behaviour information
- Safeguarding information
- Details of any support received, including care packages, plans and support providers
- Photographs
- CCTV images captured in school
- Fingerprint (biometric systems are not in all our schools)

We may collect additional information about your child if they decide to join us on an educational trip or visit. This might include emergency contact details, passport number or EHIC.

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
- Enable us to carry out educational trips/visits
- To celebrate achievement

[1] For the purposes of this document, pupil refers to both pupils and students

- Comply with the law regarding data sharing
- To enable the use of our biometric food and library services (not available in all our schools)
- For marketing purposes including websites, prospectus and social media

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. Our record retention schedule, which can be found within our GDPR policy, sets out how long we keep information about pupils.

The GDPR policy will become live in May 2018 and will be placed on our Trust website https://www.bestacademies.org.uk/legal/

The record retention schedule is based on 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 – on a statutory basis, under regulation 5 of The Education (Information About Individual Pupil/students) (England) Regulations 2013
- The pupil's family and representatives

- Educators and examining bodies (including all entities of BEST)
- Our regulator, Ofsted
- Suppliers and service providers (including online system suppliers) – 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

Please note that trainee teachers will be treated as staff whilst they complete their placement with us and therefore have access to the same information. Trainee teachers will not include any personally identifiable data within their course work, and sign a confidentiality agreement prior to commencing their placement. If the trainee wishes to include personally identifiable data, they must seek the consent of the parent/carer and, if appropriate, pupil.

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 census and early years census.

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.

Youth support services (pupils aged 13+)

Once our pupils reach the age of 13, we are legally required to pass on certain information about them to our local authority and/or youth support services provider, 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 or the Data Protection Lead in the school to request that we only pass the individual's name, address and date of birth to the local authority and/or youth support services provider.

Transferring data internationally

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.

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 or Data Protection Lead in the school.

There is no automatic parental right of access to their child's educational record. The school will decide on a case-by-case basis whether to grant such requests taking into account the most recent guidance published by the Information Commissioners Office (ICO).

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 or Data Protection Lead in the school.

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:

- Craig Smith, Chief Operating Officer, BEST
  Telephone: 01462 413511

  Email: DPO@bestacademies.org.uk

For general school specific queries, please contact the Data Protection Lead for the school:

School	Contact	Telephone Number	Email
Samuel Whitbread Academy	Ian Butler	01462 629900	SWA-DPL@bestacademies.org.uk
Etonbury Academy	Victoria Lockey	01462 730391	ETA-DPL@bestacademies.org.uk
Robert Bloomfield Academy	Vincent Holmes	01462 628800	RBA-DPL@bestacademies.org.uk
St Christophers Academy	Rebecca Tootell	01582 500960	SCA-DPL@bestacademies.org.uk
Gothic Mede Academy	Nicola Davis/ Michael Warlow	01462 732002	GMA-DPL@bestacademies.org.uk
Gravenhurst Academy	Carol Davison	01462 711257	GHA-DPL@bestacademies.org.uk
Langford Village Academy	Sonia Singh	01462 629000	LVA-DPL@bestacademies.org.uk
BEST Nurseries	Mrs H Hudson	01462 815637	Nursery-DPL@bestacademies.org.uk

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.

Appendix A – Privacy Notices – Pupil

Privacy Notice for Pupils (How we use pupil information)

Introduction

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, Bedfordshire Schools Trust (BEST), are the 'data controller' for the purposes of data protection law. Our Data Protection Officer is Craig Smith, Chief Operating Officer (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 and behaviour records
- Your characteristics, like your ethnic background, language, nationality, country of birth or any special educational needs
- Any medical conditions you have
- Details of any behaviour issues or exclusions
- Photographs
- CCTV images
- Fingerprint (not in all our schools)

We may also collect other information about you if you decide to join us on a trip or visit. This might include your parents or carers contact details, passport number or health information.

Why we use this data

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

- Get in touch with you and your parents or carers 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
- To enable use of our biometric food and library systems (not in all our schools)
- For marketing purposes including websites, prospectus and social media

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 schools. We may also keep it after you have left the school, where we are required to by law.

We have a record retention schedule within our GDPR policy, which sets out how long we must keep information about pupils.

The GDPR policy will become live in May 2018 and will be placed on our Trust website https://www.bestacademies.org.uk/legal/

The record retention schedule is based on the Information and Records Management Society's toolkit for schools.

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 your personal data 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 (including all entities of BEST)
- Our regulator (the organisation or "watchdog" that supervises us), Ofsted
- Suppliers and service providers (including online system suppliers) – 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

Please note that trainee teachers will be treated as staff whilst they complete their placement with us and therefore have access to the same information. Trainee teachers will not include any personally identifiable data within their course work, and sign a confidentiality agreement prior to commencing their placement. If the trainee wishes to include personally identifiable data, they must seek the consent of the parent/carer and, if appropriate, pupil.

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.

Youth support services (pupils aged 13+)

Once you reach the age of 13, we are legally required to pass on certain information about you to our local authority and/or youth support services provider, 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 local authority and/or youth support services provider.

Transferring data internationally

Where we share data with an organisation that is based outside the European Economic Area, we will protect your data by following data protection law.

Your rights

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 or the Data Protection Lead in your school.

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:

- Craig Smith, Chief Operating Officer, BEST
  Telephone: 01462 413511
  Email: DPO@bestacademies.org.uk

For general school specific queries, please contact the Data Protection Lead for the school:

School	Contact	Telephone Number	Email
Samuel Whitbread Academy	Ian Butler	01462 629900	SWA-DPL@bestacademies.org.uk
Etonbury Academy	Victoria Lockey	01462 730391	ETA-DPL@bestacademies.org.uk
Robert Bloomfield Academy	Vincent Holmes	01462 628800	RBA-DPL@bestacademies.org.uk
St Christophers Academy	Rebecca Tootell	01582 500960	SCA-DPL@bestacademies.org.uk
Gothic Mede Academy	Nicola Davis/ Michael Warlow	01462 732002	GMA-DPL@bestacademies.org.uk
Gravenhurst Academy	Carol Davison	01462 711257	GHA-DPL@bestacademies.org.uk
Langford Village Academy	Sonia Singh	01462 629000	LVA-DPL@bestacademies.org.uk
BEST Nurseries	Mrs H Hudson	01462 815637	Nursery-DPL@bestacademies.org.uk

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 (How we use schools workforce information)

Introduction

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, Bedfordshire Schools Trust (BEST), are the 'data controller' for the purposes of Data Protection law. Our Data Protection Officer is Craig Smith, Chief Operating Officer (see 'Contact us' below).

The personal data we hold

We process data relating to those we employ, or otherwise engage, to work in our Multi-Academy Trust. 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
- Vehicle details
- Pecuniary interests
- Data about your use of the school's information and communications system
- Fingerprint (biometric systems are not in all our schools)

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
- Ensure that Bedfordshire Schools Trust are aware of any conflict of interest
- To enable the use of our biometric food and library services (not available in all our schools)
- For marketing purposes including websites, prospectus and social media

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 our record retention schedule, which is within our GDPR policy. This sets out how long we must keep information about staff.

The GDPR policy will become live in May 2018 and will be placed on our Trust website https://www.bestacademies.org.uk/legal/

The record retention schedule is based on 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
- The Department for Education – on a statutory basis under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments
- Your family or representatives
- Educators and examining bodies (including BEST entities)
- Our regulator, Ofsted
- Suppliers and service providers (including online 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 European Economic Area, we will do so in accordance with data protection law.

Your rights

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 or Data Protection Lead in the school.

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 or Data Protection Lead in your school.

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:

- Craig Smith, Chief Operating Officer, BEST
  Telephone: 01462 413511
  Email: DPO@bestacademies.org.uk

For general school specific queries, please contact the Data Protection Lead for the school:

School	Contact	Telephone Number	Email
Samuel Whitbread Academy	Ian Butler	01462 629900	SWA-DPL@bestacademies.org.uk
Etonbury Academy	Victoria Lockey	01462 730391	ETA-DPL@bestacademies.org.uk
Robert Bloomfield Academy	Vincent Holmes	01462 628800	RBA-DPL@bestacademies.org.uk
St Christophers Academy	Rebecca Tootell	01582 500960	SCA-DPL@bestacademies.org.uk
Gothic Mede Academy	Nicola Davis/ Michael Warlow	01462 732002	GMA-DPL@bestacademies.org.uk
Gravenhurst Academy	Carol Davison	01462 711257	GHA-DPL@bestacademies.org.uk
Langford Village Academy	Sonia Singh	01462 629000	LVA-DPL@bestacademies.org.uk
BEST Nurseries	Mrs H Hudson	01462 815637	Nursery-DPL@bestacademies.org.uk

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.

Appendix B – Access Request Form

Enquirer's surname: ……

Enquirer's forenames: ……....

Enquirer's address: ……

……...

Enquirer's telephone number: ……..

Enquirer's email address: ……

Are you the person who is the subject of the records you are enquiring about (i.e. the 'Data Subject')? YES/NO

If no, do you have parental responsibility for a child who is the 'Data Subject' of the records you are enquiring about? YES/NO

If yes, please provide name(s) of child or children about whose personal data records you are enquiring……

Description of concern/area of concern / area of concern:

……

……

Description of information requested

……

……

Please dispatch reply to: (if different from enquirer's details as stated on this form)
Name: ……..

Address:……

……Postcode: …….

Data Subject Declaration

I request that the academy search its records based on the information supplied above under Section 7 of the Data Protection act 1998 and provide a description of the personal data found from the information described in the details outlined above relating to me (or my child/children) being processed by the academy. I agree that the reply period will commence when I have supplied sufficient information to enable the academy to perform the search. I consent to the reply being disclosed and sent to me at my stated address (or to the dispatch name and address above who I have authorised to receive such information).

Signature of 'Data Subject' (or subject's parent if pupil is under 13 years of age):

……..

Name of 'Data Subject' (or subject's parent): ……PRINTED

Date: ……

Form to be returned to the Data Protection Officer or Lead for the school/entity concerned (see overleaf)

School	Contact	Telephone Number	Email
Samuel Whitbread Academy	Ian Butler	01462 629900	SWA-DPL@bestacademies.org.uk
Etonbury Academy	Victoria Lockey	01462 730391	ETA-DPL@bestacademies.org.uk
Robert Bloomfield Academy	Vincent Holmes	01462 628800	RBA-DPL@bestacademies.org.uk
St Christophers Academy	Rebecca Tootell	01582 500960	SCA-DPL@bestacademies.org.uk
Gothic Mede Academy	Nicola Davis/ Michael Warlow	01462 732002	GMA-DPL@bestacademies.org.uk
Gravenhurst Academy	Carol Davison	01462 711257	GHA-DPL@bestacademies.org.uk
Langford Village Academy	Sonia Singh	01462 629000	LVA-DPL@bestacademies.org.uk
BEST Nurseries	Mrs H Hudson	01462 815637	Nursery-DPL@bestacademies.org.uk

Refer to page 9 of the GDPR and Privacy Notices Policy for further details concerning subject access requests. Please note that two forms of identification will be required.

For office use only

☐ Has the identity of the person making the request been confirmed by telephone

☐ Has the age of pupil been checked (does the pupil need to give consent)

☐ Have two forms of identification been seen

☐ Has the subject access request been granted (request to be met within one month),

If not, give reason ……..

…….

☐ If request is complex and will take more than one month, has the person making the request been informed

Date information sent: ……..

Information sent by: ……..

Appendix C – Retention Schedule

Governing Body				
Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
Agendas for LGB meetings	If meeting is dealing with confidential issues relating to staff		One copy should be retained with the master set of minutes. All other copies can be disposed of	Secure disposal
Minutes of Governing Body meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to staff			
Principal Set (signed minutes)			PERMANENT	If the school is unable to store these then they should be offered to the County Archives Service
Inspection copies (this may include copies the Clerk wishes to retain for requestors)			Date of meeting + 3 years	If these minutes contain any sensitive, personal information they must be shredded.
Reports presented to the Governing Body	There may be data protection issues if the report deals with confidential issues relating to staff		Reports should be kept for a minimum of 6 years. However, if the minutes refer directly to individual reports then the reports should be kept permanently	SECURE DISPOSAL or retain with the signed set of the minutes
Meeting papers relating to the annual parents' meeting held under section 33 of the	No	Education Act 2002, Section 33	Date of the meeting + a minimum of 6 years	SECURE DISPOSAL

Education Act 2002				
Instruments of Government including Articles of Association	No		PERMANENT	These should be retained in the school whilst the school is open and then offered to County Archives Service when the school closes.
Trusts and Endowments managed by the Governing Body	No		PERMANENT	These should be retained in the school whilst the school is open and then offered to County Archives Service when the school closes.
Action plans created and administered by the Governing Body	No		Life of the action plan + 3 years	SECURE DISPOSAL
Policy documents created and administered by the Governing Body	No		Life of the policy + 3 years	SECURE DISPOSAL
Records relating to complaints dealt with by the Governing Body	Yes		Date of the resolution of the complaint + a minimum of 6 years then review for further retention in case of contentious disputes	SECURE DISPOSAL
Annual Reports created under the requirements of the Education (Governor's Annual Reports) (England) (Amendment) Regulations 2002	No	Education (Governor's Annual Reports) (England) (Amendment) Regulations 2002 SI 2002 No 1171	Date of report + 10 years	SECURE DISPOSAL
Proposals concerning the change of status of a maintained school including Specialist Status Schools and Academies	No		Date proposal accepted or declined + 3 years	SECURE DISPOSAL

Headteacher and Senior Management Team				
Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
Log books of activity in the school maintained by the Head Teacher	There may be data protection issues if the log book refers to individual pupils or members of staff		Date of last entry in the book + a minimum of 6 years then review	These could be of permanent historical value and should be offered to the County Archives Service if appropriate
Minutes of Senior Management Team meetings and the meetings of other internal administrative bodies	There may be data protection issues if the minutes refers to individual pupils or members of staff		Date of the meeting + 3 years then review	SECURE DISPOSAL
Reports created by the Head Teacher or the Management Team	There may be data protection issues if the report refers to individual pupils or members of staff		Date of the report + a minimum of 3 years then review	SECURE DISPOSAL
Records created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	There may be data protection issues if the records refer to individual pupils or members of staff		Current academic year + 6 years then review	SECURE DISPOSAL
Correspondence created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	There may be data protection issues if the correspondence refers to individual pupils or members of staff		Date of correspondence + 3 years then review	SECURE DISPOSAL
Professional Development Plans	Yes		Life of the plan + 6 years	SECURE DISPOSAL
School Development Plans	No		Life of the plan + 3 years	SECURE DISPOSAL

Admissions Process				
Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
All records relating to the creation and implementation of the School Admissions' Policy	No	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Life of the policy + 3 years then review	SECURE DISPOSAL
Admissions – if the admission is successful	Yes	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Date of admission + 1 year	SECURE DISPOSAL
Admissions – if the appeal is unsuccessful	Yes	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities,	Resolution of case + 1 year	SECURE DISPOSAL

		schools adjudicators and admission appeals panels December 2014		
Register of Admissions	Yes	School attendance: Departmental advice for maintained schools, academies, independent schools and local authorities October 2014	Every entry in the admission register must be preserved for a period of three years after the date on which the entry was made.[3]	REVIEW Schools may wish to consider keeping the admission register permanently as often schools receive enquiries from past pupils to confirm the dates they attended the school.
Admissions – Secondary Schools – Casual	Yes		Current year + 1 year	SECURE DISPOSAL
Proofs of address supplied by parents as part of the admissions process	Yes	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Current year + 1 year	SECURE DISPOSAL
Supplementary Information form including additional information such as religion, medical conditions etc	Yes			
For successful admissions			This information should be added to the pupil file	SECURE DISPOSAL
For unsuccessful admissions			Until appeals process completed	SECURE DISPOSAL

Operational Administration				
Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
General file series	No		Current year + 5 years then REVIEW	SECURE DISPOSAL
Records relating to the creation and publication of the school brochure or prospectus	No		Current year + 3 years	STANDARD DISPOSAL
Records relating to the creation and distribution of circulars to staff, parents or pupils	No		Current year + 1 year	STANDARD DISPOSAL
Newsletters and other items with a short operational use	No		Current year + 1 year	STANDARD DISPOSAL
Visitors' Books and Signing in Sheets	Yes		Current year + 6 years then REVIEW	SECURE DISPOSAL
Records relating to the creation and management of Parent Teacher Associations and/or Old Pupils Associations	No		Current year + 6 years then REVIEW	SECURE DISPOSAL

Human Resources				
Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
All records leading up to the appointment of a new Principal	Yes		Date of appointment + 6 years	SECURE DISPOSAL
All records leading up to the appointment of a new member of staff – unsuccessful candidates	Yes		Date of appointment of successful candidate + 6 months	SECURE DISPOSAL
All records leading up to the appointment of a new member of staff – successful candidate	Yes		All the relevant information should be added to the staff personal file (see below) and all other information retained for 6 months	SECURE DISPOSAL
Pre-employment vetting information – DBS Checks	No	DBS Update Service Employer Guide June 2014: Keeping children safe in education. July 2015 (Statutory Guidance from Dept. of Education) Sections 73, 74	The school does not have to keep copies of DBS certificates. If the school does so the copy must NOT be retained for more than 6 months	
Proofs of identity collected as part of the process of checking "portable" enhanced DBS disclosure	Yes		Where possible these should be checked and a note kept of what was seen and what has been checked. If it is felt necessary to keep copy documentation then this should be placed on the member of staff's personal file	

Pre-employment vetting information – Evidence proving the right to work in the United Kingdom[4]	Yes	An employer's guide to right to work checks [Home Office May 2015]	Where possible these documents should be added to the Staff Personal File [see below], but if they are kept separately then the Home Office requires that the documents are kept for termination of Employment plus not less than two years	
Staff Personal File	Yes	Limitation Act 1980 (Section 2)	Termination of Employment + 6 years	SECURE DISPOSAL
Timesheets	Yes		Current year + 6 years	SECURE DISPOSAL
Annual appraisal/ assessment records	Yes		Current year + 5 years	SECURE DISPOSAL
Allegation of a child protection nature against a member of staff including where the allegation is unfounded[5]	Yes	"Keeping children safe in education Statutory guidance for schools and colleges March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	Until the person's normal retirement age or 10 years from the date of the allegation whichever is the longer then REVIEW. Note allegations that are found to be malicious should be removed from personnel files. If found they are to be kept on the file and a copy provided to the person concerned	SECURE DISPOSAL These records must be shredded
Disciplinary Proceedings	Yes			
oral warning			Date of warning[6] + 6 months	SECURE DISPOSAL [If warnings are placed on personal files then they must be weeded from the file]
written warning – level 1			Date of warning + 6 months	
written warning – level 2			Date of warning + 12 months	
final warning			Date of warning + 18 months	
case not found			If the incident is child	SECURE DISPOSAL

			protection related then see above otherwise dispose of at the conclusion of the case	

Health & Safety				
Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
Health and Safety Policy Statements	No		Life of policy + 3 years	SECURE DISPOSAL
Health and Safety Risk Assessments	No		Life of risk assessment + 3 years	SECURE DISPOSAL
Health and Safety Risk Assessments (Pupil or staff specific risk assessment that contain personal data)	Yes	Management of Health Safety at Work regulations 1999	Adult Life of the risk assessment + 3 years DOB of child + 21 years	SECURE DISPOSAL
Records relating to accident/ injury at work	Yes		Date of incident + 12 years In the case of serious accidents a further retention period will need to be applied	SECURE DISPOSAL
Accident Reporting	Yes	Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980		
Adults			Date of the incident + 6 years	SECURE DISPOSAL
Children			DOB of the child + 25 years	SECURE DISPOSAL

Control of Substances Hazardous to Health (COSHH)	No	Control of Substances Hazardous to Health Regulations 2002. SI 2002 No 2677 Regulation 11; Records kept under the 1994 and 1999 Regulations to be kept as if the 2002 Regulations had not been made. Regulation 18(2)	Current year + 40 years	SECURE DISPOSAL
Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos	No	Control of Asbestos at Work Regulations 2012 SI 1012 No 632 Regulation 19	Last action + 40 years	SECURE DISPOSAL
Process of monitoring of areas where employees and persons are likely to have become in contact with radiation	No		Last action + 50 years	SECURE DISPOSAL
Fire Precautions log books	No		Current year + 6 years	SECURE DISPOSAL
Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI1986/1960), revised 1999 (SI1999/567)	Current year + 3 years	SECURE DISPOSAL
Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes		Current year + 6 years	SECURE DISPOSAL

Financial Management				
Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
Employer's Liability Insurance Certificate	No		Closure of the school + 40 years	SECURE DISPOSAL
Asset Management				
Inventories of furniture and equipment	No		Current year + 6 years	SECURE DISPOSAL
Burglary, theft and vandalism report forms	No		Current year + 6 years	SECURE DISPOSAL
Accounts and Statements including Budget Management				
Annual Accounts	No		Current year + 6 years	STANDARD DISPOSAL
Loans and grants managed by the school	No		Date of last payment on the loan + 12 years then REVIEW	SECURE DISPOSAL
Student Grant applications	Yes		Current year + 3 years	SECURE DISPOSAL
All records relating to the creation and management of budgets including the Annual Budget statement and background papers	No		Life of the budget + 3 years	SECURE DISPOSAL
Invoices, receipts, order books and requisitions, delivery notices	No		Current financial year + 6 years	SECURE DISPOSAL
Records relating to the collection and banking of monies	No		Current financial year + 6 years	SECURE DISPOSAL
Records relating to the identification and collection of debt	No		Current financial year + 6 years	SECURE DISPOSAL
Contract Management				
All records relating to the management of contracts under seal	No	Limitation Act 1980	Last payment on the contract + 12 years	SECURE DISPOSAL
All records relating to the	No	Limitation Act 1980	Last payment on the	SECURE DISPOSAL

management of contracts under signature			contract + 6 years	
Records relating to the monitoring of contracts	No		Current year + 2 years	SECURE DISPOSAL
School Fund				
School Fund - Cheque books	No		Current year + 6 years	SECURE DISPOSAL
School Fund - Paying in books	No		Current year + 6 years	SECURE DISPOSAL
School Fund – Ledger	No		Current year + 6 years	SECURE DISPOSAL
School Fund – Invoices	No		Current year + 6 years	SECURE DISPOSAL
School Fund – Receipts	No		Current year + 6 years	SECURE DISPOSAL
School Fund - Bank statements	No		Current year + 6 years	SECURE DISPOSAL
School Fund – Journey Books	No		Current year + 6 years	SECURE DISPOSAL
School Meals Management				
Free School Meals Registers	Yes		Current year + 6 years	SECURE DISPOSAL
School Meals Registers	Yes		Current year + 3 years	SECURE DISPOSAL
School Meals Summary Sheets	No		Current year + 3 years	SECURE DISPOSAL

Property Management				
Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
Title deeds of properties belonging to the school	No		PERMANENT These should follow the property unless the property has been registered with the Land Registry	
Plans of property belong to the school	No		These should be retained whilst the building belongs to the school and should be passed onto any new owners if the building is leased or sold.	
Leases of property leased by or to the school	No		Expiry of lease + 6 years	SECURE DISPOSAL
Records relating to the letting of school premises	No		Current financial year + 6 years	SECURE DISPOSAL
All records relating to the maintenance of the school carried out by contractors	No		Current year + 6 years	SECURE DISPOSAL
All records relating to the maintenance of the school carried out by school employees including maintenance log books	No		Current year + 6 years	SECURE DISPOSAL

Pupil / Student Management (inc child protection, SEN & educational visits)				
Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
Pupil's Educational Record required by The Education (Pupil Information) (England) Regulations 2005	Yes	The Education (Pupil Information) (England) Regulations 2005 SI 2005 No. 1437		
Primary			Retain whilst the child remains at the primary school	The file should follow the pupil when he/she leaves the primary school. This will include: • to another primary school • to a secondary school • to a pupil referral unit • If the pupil dies whilst at primary school the file should be returned to the Local Authority to be retained for the statutory retention period. If the pupil transfers to an independent school, transfers to home schooling or leaves the country the file should be returned to the Local Authority to be retained for the statutory retention period. Primary Schools do not ordinarily have sufficient storage space to store records for pupils who have not transferred in the normal way. It makes more sense to transfer the record to the Local Authority as it is more likely that the pupil will request the record from the Local Authority
Secondary		Limitation Act 1980	Date of Birth of the pupil	SECURE DISPOSAL

		(Section 2)	+ 25 years	
Examination Results – Pupil Copies	Yes			
Public			This information should be added to the pupil file	All uncollected certificates should be returned to the examination board.
Internal			This information should be added to the pupil file	
Child protection information held on pupil file	Yes	Keeping Children Safe in Education statutory guidance for schools and colleges Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children	If any records relating to child protection issues are placed on the pupil file, it should be in a sealed envelope and then retained for the same period of time as the pupil file	SECURE DISPOSAL – these records MUST be shredded
Child protection information held in separate files	Yes	Keeping Children Safe in Education statutory guidance for schools and colleges Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children	DOB of the child + 25 years then review This retention period was agreed in consultation with the Safeguarding Children Group on the understanding that the principal copy of this information will be found on the Local Authority Social Services record	SECURE DISPOSAL – these records MUST be shredded
Retention periods relating to allegations made against adults can be found in the Human Resources section of this retention schedule.				
<u>Attendance</u>				
Attendance Registers	Yes	School attendance: Departmental advice for maintained	Every entry in the attendance register must be preserved for a period of three years after the date on which the	SECURE DISPOSAL

		schools, academies, independent schools and local authorities October 2014	entry was made.	
Correspondence relating to authorized absence		Education Act 1996 Section 7	Current academic year + 2 years	SECURE DISPOSAL
Special Educational Need				
Special Educational Needs files, reviews and Individual Education Plans	Yes	Limitation Act 1980 (Section 2)	Date of Birth of the pupil + 25 years	REVIEW NOTE: This retention period is the minimum retention period that any pupil file should be kept. Some authorities choose to keep SEN files for a longer period of time to defend themselves in a "failure to provide a sufficient education" case. There is an element of business risk analysis involved in any decision to keep the records longer than the minimum retention period and this should be documented.
Statement maintained under section 234 of the Education Act 1990 and any amendments made to the statement	Yes	Education Act 1996 Special Educational Needs and Disability Act 2001 Section 1	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold
Advice and information provided to parents regarding educational needs	Yes	Special Educational Needs and Disability Act 2001 Section 2	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold
Accessibility Strategy	Yes	Special Educational Needs and Disability Act 2001 Section 14	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold

Curriculum				
Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
Curriculum returns	No		Current year + 3 years	SECURE DISPOSAL
Examination Results (Schools Copy)	Yes		Current year + 6 years	SECURE DISPOSAL
SATS records –	Yes			
Results			The SATS results should be recorded on the pupil's educational file and will therefore be retained until the pupil reaches the age of 25 years. The school may wish to keep a composite record of all the whole year SATs results. These could be kept for current year + 6 years to allow suitable comparison	SECURE DISPOSAL
Examination Papers			The examination papers should be kept until any appeals/validation process is complete	SECURE DISPOSAL
Published Admission Number (PAN) Reports	Yes		Current year + 6 years	SECURE DISPOSAL
Value Added and Contextual Data	Yes		Current year + 6 years	SECURE DISPOSAL
Self Evaluation Forms	Yes		Current year + 6 years	SECURE DISPOSAL
Schemes of Work	No		Current year + 1 year	

Timetable	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a further retention period or SECURE DISPOSAL
Class Record Books	No		Current year + 1 year	
Mark Books	No		Current year + 1 year	
Record of homework set	No		Current year + 1 year	
Pupils' Work	No		Where possible pupils' work should be returned to the pupil at the end of the academic year if this is not the school's policy then current year + 1 year	SECURE DISPOSAL
Extra-curricular Activities				
Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Primary Schools	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 - "Legal Framework and Employer Systems" and Section 4 - "Good Practice".	Date of visit + 14 years	SECURE DISPOSAL
Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Secondary Schools	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 - "Legal Framework and Employer Systems" and Section 4 - "Good Practice".	Date of visit + 10 years	SECURE DISPOSAL
Parental consent forms for school trips where there has been no major incident	Yes		Conclusion of the trip	Although the consent forms could be retained for DOB + 22 years, the requirement for them being needed is low and most schools do not have the storage capacity to retain every single consent form issued by the school for this period of time.

Parental permission slips for school trips – where there has been a major incident	Yes	Limitation Act 1980 (Section 2)	DOB of the pupil involved in the incident + 25 years The permission slips for all the pupils on the trip need to be retained to show that the rules had been followed for all pupils	
Walking Bus Registers	Yes		Date of register + 3 years This takes into account the fact that if there is an incident requiring an accident report the register will be submitted with the accident report and kept for the period of time required for accident reporting	SECURE DISPOSAL [If these records are retained electronically any back up copies should be destroyed at the same time]
Family Liaison Officers and Home School Liaison Assistants				
Day Books	Yes		Current year + 2 years then review	
Reports for outside agencies - where the report has been included on the case file created by the outside agency	Yes		Whilst child is attending school and then destroy	
Referral forms	Yes		While the referral is current	
Contact data sheets	Yes		Current year then review, if contact is no longer active then destroy	
Contact database entries	Yes		Current year then review, if contact is no longer active then destroy	
Group Registers	Yes		Current year + 2 years	

Central Government & Local Authority				
Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
Local Authority				
Secondary Transfer Sheets (Primary)	Yes		Current year + 2 years	SECURE DISPOSAL
Attendance Returns	Yes		Current year + 1 year	SECURE DISPOSAL
School Census Returns	No		Current year + 5 years	SECURE DISPOSAL
Circulars and other information sent from the Local Authority	No		Operational use	SECURE DISPOSAL
Central Government				
OFSTED reports and papers	No		Life of the report then REVIEW	SECURE DISPOSAL
Returns made to central government	No		Current year + 6 years	SECURE DISPOSAL
Circulars and other information sent from central government	No		Operational use	SECURE DISPOSAL

This retention schedule is based on the recommendations outlined in the Information Management Toolkit for Schools (February 2016)

Appendix D – Data Breach Procedure

Staff member reports potential breach immediately to Data Protection Lead (DPL)

DPL to 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

If the DPL is unsure, they should seek advice from the Data Protection Officer (DPO)

Not a reportable breach

If appropriate, record as 'near miss' – if recurring incident or individual, DPL to assess risk and consider follow up action (disciplinary procedure may be followed at this point – DPO to be informed)

Reportable breach

DPL to report incident to DPO and Principal – **Principal** to report to Chair of Governors.

DPO to assess whether the breach must be reported to ICO (breaches must be reported within 72 hours).

DPO to consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damaged (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

Is breach reportable?

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

Not reportable

DPO will document the decision and store this for future reference – DPO to feedback to DPL and Principal

DPO to report the breach 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 of the above details are not known, the DPO will report as much as they can within 72 hours. The DPO will explain the reasons for the delay and submit the remaining information as soon as possible.

DPO to 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

DPO to also notify any relevant third parties who can help mitigate the loss to individuals – such as policy, insurers, banks etc.

DPO to document the breach, this record will include facts and cause, effects and action taken.

DPO and Principal to meet to review what happened and to prevent future recurrence.