GDPR Policy
and Privacy Notices

AUTHOR:	Chief Operating Officer
DATE APPROVED:	June 2020 (updated Nov ’20 to include Campton Academy)
APPROVED BY:	Trust Board
NEXT REVIEW DATE:	June 2022

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). 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 provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR.

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, living individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation

Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data Controller	A person or organisation that determines the purposes 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
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. The Data Controller

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, and pays, for this registration annually as 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 its 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.

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise or defence of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes,** and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **archiving purposes,** scientific or historical research purposes, or statistical purposes, and the processing is in the public interest.

For criminal offence data, BEST and its entities will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for or in connection with legal proceeds, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation.

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

Whenever BEST and its entities receive personal data from another transferring school, they will seek confirmation that the data being transferred is compliant with the General Data Protection Regulations. Schools may choose to request that written confirmation is obtained.

For any processing that is likely to result in a high risk to individuals, a **data protection impact assessment (DPIA)** must be completed. DPIA is a process to help identify and minimise the data protection risks of a project. The DPIA must:

- Describe the nature, scope, context and purposes of the processing
- Assess necessity, proportionality and compliance measures
- Identify and assess risks to individuals
- Identify any additional measures to mitigate those risks

The DPL in each school must be consulted when a DPIA is felt necessary.

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 contract with the supplier or contractor 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 we are legally required to do so.

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
- How we use Trustee/Governor 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 may be submitted in any form, but BEST and its entities may be able to respond to requests more quickly if they are made in writing using the Access Request Form included in Appendix B or the request states the specific data required.

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
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- 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
- The safeguards provided if the data is being transferred internationally

BEST and its entities may **not** reveal information in response to subject access requests for a variety of reasons – these could include:

- 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 being or has been abused, or is at risk of abuse, where disclosure ofthat information would not be in the child's best interests
- Information that would include another person's personal data that cannot reasonably be anonymised, and the other person has not given their consent, and it would be unreasonable to proceed without it
- Information that is part of a certain sensitive document, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

Children and subject access requests

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

Primary aged pupils

Children below the age of 12 are generally not regarded as mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents and carers of pupils at the school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Secondary aged students

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students at the school may not be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

Parental requests to see the educational record

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

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it.

The right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced. This may include some safeguarding documentation.

Responding to subject access requests

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

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

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 (or receipt of the additional information needed to confirm identity, where relevant). However, BEST reserves the right to extend this deadline to three months of receipt of the request where a request is complex or numerous. The individual will be informed of this within one month and explain why the extension is necessary.

There is no fee for subject access requests.

If the request is unfounded or excessive, BEST and its entities may refuse to act on it, or charge a reasonable fee to cover the administrative costs. BEST and its entities will take into account whether the request is repetitive in nature when making the decision. 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, or they can seek to enforce their subject access right through the courts.

Other data protection rights of an individual

In addition to the right to make a subject access request (see above), and to receive the information that BEST and its entities are processing, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask that their personal data is rectified, erased or restricted in terms of processing (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making human decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach (in certain circumstances)
- Make a complaint to ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPL or DPO. If staff receive such a request, they must immediately forward it to the DPL for their school.

11. Biometric recognition systems

Biometric data means personal information about an individual's physical or behavioural characteristics that can be used to identify that person; this can be their fingerprint, facial shape, retina and iris patterns, and hand measurements.

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 (this applies to all pupils/students in schools under the age of 18).

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 withdraw consent, at any time, and the school/entity will make

sure that any relevant data already captured is either deleted or undergoes a process of irreversible anonymisation.

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 either delete any relevant data already captured or ensure it undergoes a process of irreversible anonymisation.

BEST and its entities will ensure that biometric data is stored securely to prevent any unauthorised or unlawful use. Biometric data will only be used for the purposes for which it has been obtained.

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. This policy should be read in conjunction with the school's CCTV policy.

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.

If there is a conflict of interests i.e. the child consents but the parent does not consent, if the child is under 18 years of age, the parent's view will take precedent.

Any photographs or videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, BEST request that photos or videos with other pupils/students in are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or students where appropriate) have agreed to this.

Where BEST and its entities take photographs and videos, 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 and 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

BEST and its entities will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. 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 aspossible • 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 deletebetween 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. All trustees/governors must sign a trustee/governor consent form; in which they agree to comply with the GDPR policy. **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 andemails • 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 isunoccupied • 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. If an outside company is used, BEST and its entities will require the third party to provide sufficient guarantees that it complies with the data protection law.

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 after becoming aware of the incident. 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. This may be completed via an online training system.
Data protection will also form part of continuing professional development, where changes to legislation or the school's processes make it necessary.
BEST and its entities provide refresher training annually to all staff including analysis of cross trust trends in terms of data protection incidents.

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

This policy is linked to:

- Freedom of Information Policy and Publication Scheme
- Recruitment and selection Policy
- E-safety Policy
- Safeguarding and child protection
- Staff Code of Conduct (including social media and acceptable use of IT facilities and monitoring)
- Whistleblowing (Confidential Reporting)
- School CCTV 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 – Procedure for processing personal information relating to staff
- Appendix D – Retention Schedule
- Appendix E – Data Breach Procedure

Appendix A – Privacy Notices

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 trust/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 categories of pupil information that we process include:

- Personal identifiers (such as name, unique pupil number, contact details, contact preferences, address date of birth and identification documents)
- Characteristics (such as ethnic background, nationality, language or eligibility for free school meals)
- Assessment and attainment (such as key stage 1 and phonics results, post 16 courses enrolled for and any relevant results)
- Special educational needs (including the needs and ranking)
- Medical and administration (such as doctors information, child health, dental health, allergies, medication and dietary requirements)
- Attendance (such as sessions attended, number of absences, absence reasons and any previous schools attended)
- Safeguarding information (such as court orders and professional involvement)
- Behavioural information (such as exclusions and any relevant alternative provision put in place)
- Photographs
- CCTV images captured in school
- Biometrics (not used 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.

The above is not an exhaustive list, to access the current list of categories of information each school processes, please contact the relevant Data Protection Lead (see 'Contact us' below).

Why we collect and use pupil information

We use this data to:

- Support pupil learning
- Monitor and report on pupil attainment progress
- Provide appropriate pastoral care
- Protect pupil welfare
- Meet the statutory duties placed upon us for DfE data collections
- Assess the quality of our services
- Administer admissions waiting lists

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

- Carry out research
- Enable us to carry out educational trips/visits
- To celebrate achievement
- 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 (where consent is given)

We do not currently process any personal data through automated decision making or profiling. If this changes in the future, we will amend any relevant privacy notices in order to explain the processing to you, including your right to object to it.

Under the General Data Protection Regulation (GDPR), the lawful bases we rely on for processing pupil information are:

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

The following data, which we collect, is classed as special category data:

- racial or ethnic origin
- religious or philosophical beliefs
- biometric data
- data concerning health (both physical and mental)
- special educational needs
- photographs and CCTV images captured in school

Under the General Data Protection Regulation (GDPR), the lawful bases we rely on for processing special category information are:

- the data subject has given explicit consent to the processing of those personal data for one or more specified purposes;
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law;
- processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- processing relates to personal data which are manifestly made public by the data subject;

- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- processing is necessary for reasons of substantial public interest;
- processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

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

We collect pupil information via registration forms, Common Transfer File (CTF) and secure file transfer from previous school.

Pupil data is essential for the schools' operational use. Whilst the majority of pupil information you provide to us is mandatory, some of it requested on a voluntary basis. In order to comply with the data protection legislation, we will inform you at the point of collection, whether you are required to provide certain pupil information to us or if you have a choice in this.

How we store this data

We hold pupil data securely for the set amount of time shown in our data retention schedule. For more information on our data retention schedule and how we keep your data safe, please refer to our GDPR policy, which is stored on the BEST website www.bestacademies.org.uk under 'Governance'.

The BEST record retention schedule can be found within the above policy. The schedule is based on the Information and Records Management Society's toolkit for schools.

Who we share pupil information with

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 pupil data, safeguarding concerns and exclusions
- Government departments and agencies
- The pupil's family and representatives
- Educators and examining bodies
- Our regulator, Ofsted
- Suppliers and service providers (including online system suppliers) – to enable them to provide the service we have contracted them for

- 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
- Further education provider/next school (including all entities of BEST)

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.

Youth support services

Once our pupils reach the age of 13, we also pass pupil information to our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- youth support services
- careers advisers

The information shared is limited to the child's name, address and date of birth. However, where a parent or guardian provides their consent, other information relevant to the provision of youth support services will be shared. This right is transferred to the child / pupil once they reach the age 16.

When carrying out data transfers to the youth support service, the data is transferred via secure method and stored as per our policy. For details of the retention period, see retention schedule in our GDPR policy www.bestacademies.org.uk under 'Governance'.

We will also share certain information about pupils aged 16+ with our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers advisers

When carrying out data transfers to the youth support service, the data is transferred via secure method and stored as per our policy. For details of the retention period, see retention schedule in our GDPR policy www.bestacademies.org.uk under 'Governance'.

For more information about services for young people, please visit our local authority website.

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

Department for Education

The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections. We are required to share information about our pupils with the Department for Education (DfE) either directly or via our local authority for the purpose of those data collections, under:

- School census - regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

All data is transferred securely and held by DfE under a combination of software and hardware controls, which meet the current government security policy framework.

For more information, please see 'How Government uses your data' section.

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.

Requesting access to your child's personal data

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your child's personal information, or be given access to your child's educational record, contact the Data Protection Lead (DPL) – see 'Contact us' section for details.

Once your child is able to understand their rights over their own data (generally considered to be over the age of 12, but this has to be considered on a case-by-case basis), we need to obtain consent from your child for you to make a subject access request on their behalf.

Please note it may be necessary for us to apply the GDPR exemption to not supply information relating to the safeguarding of a pupil if we feel that the right of access would be likely to cause serious harm to the physical or mental health of any individual.

You also have the right to:

- object to our use of your child's personal data
- in certain circumstances, have personal data corrected
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have personal data erased or destroyed; and
- a right to seek redress, either through the ICO, or through the courts

If you have a concern or complaint about the way we are collecting or using your child's personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/make-a-complaint/
- 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:

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

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	Dawn Mills	01462 629000	LVA-DPL@bestacademies.org.uk
Lawnside Academy	Cheryl Johnson / Marissa Stoneham	01767 312313	LSA-DPL@bestacademies.org.uk
Pix Brook Academy	Indie King-Mand	01462 416243	PBA-DPL@bestacademies.org.uk
Campton Academy	Sarah Fraher	01462 813359	CMA-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.

How Government uses your child's data

The pupil data that we lawfully share with the DfE through data collections:

- underpins school funding, which is calculated based upon the numbers of children and their characteristics in each school.
- informs 'short term' education policy monitoring and school accountability and intervention (for example, school GCSE results or Pupil Progress measures).
- supports 'longer term' research and monitoring of educational policy (for example how certain subject choices go on to affect education or earnings beyond school)

Data collection requirements

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for- schools

The National Pupil Database (NPD)

Much of the data about pupils in England goes on to be held in the National Pupil Database (NPD).

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department.

It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil- database-user-guide-and-supporting-information.

Sharing by the Department

The law allows the Department to share pupils' personal data with certain third parties, including:

- schools
- local authorities

- researchers
- organisations connected with promoting the education or wellbeing of children in England
- other government departments and agencies
- organisations fighting or identifying crime

For more information about the Department's NPD data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

Organisations fighting or identifying crime may use their legal powers to contact DfE to request access to individual level information relevant to detecting that crime. Whilst numbers fluctuate slightly over time, DfE typically supplies data on around 600 pupils per year to the Home Office and roughly 1 per year to the Police.

For information about which organisations the Department has provided pupil information, (and for which project) or to access a monthly breakdown of data share volumes with Home Office and the Police please visit the following website: https://www.gov.uk/government/publications/dfe-external-data-shares

Under the terms of the Data Protection Act 2018, you are entitled to ask the Department:

- if they are processing your personal data
- for a description of the data they hold about you
- the reasons they're holding it and any recipient it may be disclosed to
- for a copy of your personal data and any details of its source

If you want to see the personal data held about you by the Department, you should make a 'subject access request'. Further information on how to do this can be found within the Department's personal information charter that is published at the address below:

https://www.gov.uk/government/organisations/department-for-education/about/personal-information-charter

To contact DfE: https://www.gov.uk/contact-dfe

Privacy Notice for Pupils (How we use pupil information)

Introduction

You have a legal right to be informed about how our trust/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 characteristics, like your ethnic background, language, nationality, country of birth or any special educational needs
- Your test results
- Any additional needs you may have
- Your attendance and behaviour records
- Any medical conditions you have
- Details of any behaviour issues or exclusions
- Any information required to keep you safe
- Photographs
- CCTV images
- Biometrics (such as fingerprint etc)

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.

We may also hold information sent to us by other organisations, including other schools, local authorities and the Department for Education.

If you would like any further details about the information we hold on you, please contact the Data Protection Lead for your school (see 'Contact us' below).

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 including health
- To enable use of our biometric food and library systems (not in all our schools)
- For marketing purposes including websites, prospectus and social media (when consent is given)
- To celebrate your achievement
- To comply with the law

We do not currently put your personal information through any automated decision making or profiling process. This means we do not make decisions about you using only computers without any human involvement. If this changes in the future, we will update this notice in order to explain the processing to you, including our right to object to it.

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)
- We have a legitimate interest

For special category data (more sensitive personal information), we only collect and use it when we have both a lawful basis, as set out above, and one of the following conditions for processing as set out in the data protection law:

- We have obtained your explicit consent to use your information in a certain way
- We need to use your information under employment, social security or social protection law
- We need to protect an individual's vital interests (i.e. protection your life or someone else's life), in situations where you're physically or legally incapable of giving consent
- The information has already been made obviously public by you
- We need to use it to make or defend against legal claims
- We need to use it for reasons of substantial public interest as defined in legislation
- We need to use it for health or social care purposes, and it's used by, or under the direction of, a professional obliged to confidentiality under law
- We need it for public health reasons, and it's used by, or under the direction of, a professional obliged to confidentiality under law
- We need to use it for archiving purposes, scientific or historical research purposes, or for statistical purposes, and the use is in the public 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. This policy is available on the Trust website www.bestacademies.org.uk/ under 'Governance'.

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

Who we share your information with

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 such as concerns about pupils' safety and exclusions
- Government departments or agencies
- Your family and representatives
- Youth support services
- Educators and examining bodies
- 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
- 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
- Further education provider / next school (including all entities of BEST)

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.

Youth support services

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 enables them to provide services as follows:

- youth support services
- careers advisers

The information shared is limited to your name, address and date of birth. However, where a parent or guardian provides their consent, other information relevant to the provision of youth support services will be shared. This right is transferred to you once you reach the age 16.

Once you reach the age of 16, we share certain information about you with our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds.

This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers advisers

For details of how long we store this information and how it is disposed of, see the retention schedule in our GDPR policy www.bestacademies.org.uk under 'Governance'.

For more information about services for young people, please visit our local authority website.

Department for Education (DfE)

The Department for Education (a government department) collects information about you from schools and local authorities. We are legally required to share this information. For more information, please see 'How Government uses your data' section.

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.

Requesting access to your personal data

Under data protection legislation, you and your parents have the right to request access to information we hold about you. To make a request or find out more information about what rights you have concerning the information we hold on you, contact the Data Protection Lead (DPL) for your school – see 'Contact us' section for details.

You also have certain rights regarding how your personal information is used and kept safe. For example:

- Say that you don't want your personal information to be used
- Stop it being used to send you marketing materials
- Say that you don't want it to be used for automated decisions (decisions made by a computer or machine, rather than a person)
- In some cases, have it corrected if it's inaccurate
- In some cases, have it deleted or destroyed, or restrict its use
- In some cases, be notified of a data breach

- Make a complaint to the Information Commissioner's Office
- Claim compensation if the data protection rules are broken and this harms you in some way

To exercise any of these rights, please contact us (see 'Contact us' section below).

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 concerns about our data processing, please let us know first.

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

- Report a concern online at https://ico.org.uk/make-a-complaint/
- 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	Dawn Mills	01462 629000	LVA-DPL@bestacademies.org.uk
Lawnside Academy	Cheryl Johnson / Marissa Stoneham	01767 312313	LSA-DPL@bestacademies.org.uk
Pix Brook Academy	Indie King-Mand	01462 416243	PBA-DPL@bestacademies.org.uk
Campton Academy	Sarah Fraher	01462 813359	CMA-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.

How Government uses your data

We are legally required to share information with the Department for Education (government department) through data collections:

- to help them calculate school funding as it is based upon the numbers of children and their characteristics in each school
- to inform education policy monitoring and school accountability and intervention (for example, school GCSE results or Pupil Progress measures)
- to support research and monitoring of educational policy (for example how certain subject choices go on to affect education or earnings beyond school)

Data collection requirements

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses- for-schools

The National Pupil Database (NPD)

Much of the data about pupils in England goes on to be held in the National Pupil Database (NPD).

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information

Sharing by the Department

The law allows the Department to share pupils' personal data with certain third parties, including:

- schools
- local authorities
- researchers
- organisations connected with promoting the education or wellbeing of children in England
- other government departments and agencies
- organisations fighting or identifying crime

For more information about the Department's NPD data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

Organisations fighting or identifying crime may use their legal powers to contact DfE to request access to individual level information relevant to detecting that crime. Whilst numbers fluctuate slightly over time, DfE typically supplies data on around 600 pupils per year to the Home Office and roughly 1 per year to the Police.

For information about which organisations the Department has provided pupil information, (and for which project) or to access a monthly breakdown of data share volumes with Home Office and the Police please visit the following website: https://www.gov.uk/government/publications/dfe-external-data-shares

Under the terms of the Data Protection Act 2018, you are entitled to ask the Department:

- if they are processing your personal data
- for a description of the data they hold about you
- the reasons they're holding it and any recipient it may be disclosed to
- for a copy of your personal data and any details of its source

If you want to see the personal data held about you by the Department, you should make a 'subject access request'. Further information on how to do this can be found within the Department's personal information charter that is published at the address below:

https://www.gov.uk/government/organisations/department-for-education/about/personal-information-charter

To contact DfE: https://www.gov.uk/contact-dfe

Privacy Notice for Staff

(How we use school's workforce information)

Introduction

Under Data Protection law, individuals have a right to be informed about how the trust/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:

- Personal information (such as name, contact details, employee or teacher number)
- Next of kin and emergency contact numbers
- Characteristics information (such as gender, age, ethnic group)
- Contract information (such as start date, hours worked, post, role, salary information)
- 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 (such as number of absences and reasons)
- Copy of driving license
- Photographs
- CCTV footage
- Vehicle details
- Pecuniary interests
- Data about your use of the school's information and communications system

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

- Race, ethnicity, religious beliefs, sexual orientation and political opinions
- Trade union membership
- Health, including any medical conditions, and sickness records
- Biometrics (not used in all our schools)

Privacy Notice for Staff

(How we use school's workforce information)

Why we collect and use workforce information

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 the development of 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

Under the General Data Protection Regulation (GDPR), the lawful bases we rely on for processing personal information for general purposes are:

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Under the General Data Protection Regulation (GDPR), the lawful bases we rely on for processing special category information are:

- the data subject has given explicit consent to the processing of those personal data for one or more specified purposes;
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law;
- processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- processing relates to personal data which are manifestly made public by the data subject;
- processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity;
- processing is necessary for reasons of substantial public interest;

- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
- processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

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 workforce information

We collect personal information during the application and recruitment process.

Workforce data is essential for the school's / local authority's operational use. Whilst the majority of personal information you provide to us is mandatory, some of it is requested on a voluntary basis. In order to comply with GDPR, we will inform you at the point of collection, whether you are required to provide certain information to us or if you have a choice in this.

Storing workforce information

We hold data securely for the set amount of time shown in our data retention schedule. For more information on our data retention schedule and how we keep your data safe, please visit the Trust website https://www.bestacademies.org.uk under 'Governance'.

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

Who we share workforce information with

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

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

- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and workforce census
- Government departments and agencies
- Our regulator, Ofsted – for inspection purposes for meet our legal obligations
- Suppliers and service providers (including online providers) – to enable them to provide the service we have contracted them for, such as payroll, HR, pensions and banking services.

- 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
- All entities of BEST

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.

Department for Education

The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections.

All data is transferred securely and held by DfE under a combination of software and hardware controls which meet the current government security policy framework.

For more information, please see 'How Government uses your data' section.

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact the Data Protection Lead (DPL) for your school – see 'Contact us' section.

You also have the right to:

- ask us for access to information about you that we hold
- have your personal data rectified, if it is inaccurate or incomplete
- request the deletion or removal of personal data where there is no compelling reason for its continued processing
- restrict our processing of your personal data (i.e. permitting its storage but no further processing)
- object to direct marketing (including profiling) and processing for the purposes of scientific/historical research and statistics
- object to decisions being taken by automated means where it produces a legal or similarly significant effect on you
- a right to seek redress, either through the ICO, or through the courts

Privacy Notice for Staff

(How we use school's workforce information)

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/make-a-complaint/
- 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	Dawn Mills	01462 629000	LVA-DPL@bestacademies.org.uk
Lawnside Academy	Cheryl Johnson / Marissa Stoneham	01767 312313	LSA-DPL@bestacademies.org.uk
Pix Brook Academy	Indie King-Mand	01462 416243	PBA-DPL@bestacademies.org.uk
Campton Academy	Sarah Fraher	01462 813359	CMA-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.

How Government uses your data

The workforce data that we lawfully share with the DfE through data collections:

- informs departmental policy on matters related to child and family social workers
- may be used to inform the distribution of school funding
  supports 'longer term' research and monitoring of children's social care policy

Data collection requirements

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/guidance/childrens-social-work-workforce-census-guide-to-submitting-data.

Sharing by the Department

The Department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

To contact the department: https://www.gov.uk/contact-dfe

Privacy Notice – How we use personal information relating to our Trust Board/Local Governing Bodies

Introduction

This Privacy Notice is to let you know how we look after personal information about our governors, trustees and members. This is in relation to information you provide us with and the information you input on Governor Hub.

We, Bedfordshire Schools Trust (BEST), are the 'data controller' for the purposes of data protection law. Our Data Protection Officer is Craig Smith (see 'Contact us' section at the end of this document).

If you have any questions or queries or would like to discuss anything in this Privacy Notice, please contact the Data Protection Lead for your school (see the 'Contact us' section at the end of this document).

A copy of this Privacy Notice is available on our website www.bestacademies.org.uk.

How we collect governor/trustee information

We obtain governor information through the Clerk to the Governors or Board upon appointment to Bedfordshire Schools Trust (BEST). In addition, to comply with our statutory obligations, we hold governor information on our Single Central Record. Updated information will also be collected during the course of the year to enable us to keep our records up to date.

The personal information we collect and hold includes the following:

- Contact details such as name, address, email address and telephone number
- Special category data such as ethnicity, disability and access requirements
- Business and personal pecuniary interests
- Governance details (such as role and start and end dates)
- An enhanced DBS check
- Training record including LGB skills audits
- Photographs and CCTV images captured in school (when consent given)

In order for us to comply with our statutory obligations, we will publish the following information on the Trust or school website.

- Name
- Governor role
- Category of governor
- Date of appointment / term of office
- Attendance at meetings
- Disclosure of pecuniary interests

Why we collect and use this information

The personal data we collect is essential in order for the school to fulfil their official functions and meet legal requirements.

We collect and use governor information, for the following purposes:

- Maintain effective governance
- Conduct the work of the governing board in accordance with the Nolan principles of public life

- Record attendance at meetings
- Identify training needs
- Meet statutory obligations for publishing and sharing governor/trustee information
- Provide access to Governor Hub (which also allows a secure facility to hold our governance information)
- Provide access to local authority training opportunities and governance resources
- Comply with our safeguarding obligations towards our pupils/students
- Ensure that appropriate access arrangements can be provided for those who need them

We do not currently process any personal data through automated decision making or profiling. If this changes in the future, we will amend any relevant privacy notices in order to explain the processing to you, including your right to object to it.

Lawful basis for holding and using this information

We only collect and use personal information about you when the law allows us to. Most commonly, we use it where we need to:

- 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)

Governor data is essential for the trust/school's operational use. Whilst the majority of personal information you provide to us is mandatory, some of it may be requested on a voluntary basis (such as photographs). In order to comply with GDPR, we will inform you at the point of collection, whether you are required to provide certain information to us or if you have a choice in this.

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.

Who we share governor information with

We routinely share governor/trustee information with:

- Other governors/trustees within BEST
- The Local Authority to meet our legal obligations
- Government departments or agencies
- Our regulator, Ofsted
- Other schools in BEST
- Suppliers and service providers, such as Governor Hub, to enable them to provide the service for which they are contracted
- Professional advisers and consultants who are connected with the school to provide school improvement services
- Our auditors
- Security organisations

We obtain a copy of the GDPR policy, Privacy Notice and/or Data Sharing Agreements with any suppliers/providers of services who have access to or process personal information.

Why we share governor information

We do not share information about our governors with anyone without consent unless the legal basis for holding and sharing the data allow us to do so.

We are required under our statutory duties to share information about our governors with our local authority (LA), government departments and our regulator, Ofsted.

Department for Education

The Department for Education (DfE) collects personal data from educational settings and local authorities. We are required to share information about our governors with the (DfE) under the requirements set out in the Academies Financial Handbook

All data is entered manually on the GIAS system and held by DfE under a combination of software and hardware controls which meet the current government security policy framework.

For more information, please see 'How Government uses your data' section.

How we store trustee/governor information

We hold data securely for the set amount of time shown in our data retention schedule. For more information on our data retention schedule and how we keep your data safe, please see our GDPR policy, which is available on our website www.bestacademies.org.uk under 'Governance'.

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact the Data Protection Lead for your school (see Contact Us section).

You also have the right to:

- ask us for access to information about you that we hold
- have your personal data rectified, if it is inaccurate or incomplete
- request the deletion or removal of personal data where there is no compelling reason for its continued processing
- restrict our processing of your personal data (i.e. permitting its storage but no further processing)
- object to direct marketing (including profiling) and processing for the purposes of scientific/historical research and statistics
- not to be subject to decisions based purely on automated processing where it produces a legal or similarly significant effect on you

If you have a concern or complaint about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/make-a-complaint/
- Call 0303 123 1113

- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

For further information on how to request access to personal information held centrally by DfE, please see the 'How Government uses your data' section of this notice.

Withdrawal of consent and the right to lodge a complaint

Where we are processing your personal data with your consent, you have the right to withdraw that consent. If you change your mind, or you are unhappy with our use of your personal data, please let us know by contacting the DPL for your school (see 'Contact us' section below).

Privacy Notice updates

We may need to update this privacy notice periodically – the revised version will be uploaded to the BEST website (www.bestacademies.org.uk). This version was last updated June 2020.

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	Dawn Mills	01462 629000	LVA-DPL@bestacademies.org.uk
Lawnside Academy	Cheryl Johnson / Marissa Stoneham	01767 312313	LSA-DPL@bestacademies.org.uk
Pix Brook Academy	Indie King-Mand	01462 416243	PBA-DPL@bestacademies.org.uk
Campton Academy	Sarah Fraher	01462 813359	CMA-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.

Privacy Notice – How we use personal information relating to our Trust Board/Local Governing Bodies

How Government uses your data

The governance data that we lawfully share with the DfE via GIAS:

- will increase the transparency of governance arrangements
- will enable schools and the department to identify more quickly and accurately individuals who are involved in governance and who govern in more than one context
- allows the department to be able to uniquely identify an individual and in a small number of cases conduct checks to confirm their suitability for this important and influential role

Data collection requirements:

To find out more about the requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/government/news/national-database-of-governors.

Note: Some of these personal data items are not publicly available and are encrypted within the GIAS system. Access is restricted to a small number of DfE staff who need to see it in order to fulfil their official duties. The information is for internal purposes only and not shared beyond the department, unless the law allows it.

How to find out what personal information DfE hold about you

Under the terms of the Data Protection Act 2018, you're entitled to ask the Department:

- if they are processing your personal data
- for a description of the data they hold about you
- the reasons they're holding it and any recipient it may be disclosed to
- for a copy of your personal data and any details of its sources

If you want to see the personal data held about you by the Department, you should make a 'subject access request'. Further information on how to do this can be found within the Department's personal information charter that is published at the address below.

https://www.gov.uk/government/organisations/department-for-education/about/personal-information-charter

To contact DfE: https://www.gov.uk/contact-dfe

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 school search its records based on the information supplied above 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 school. I agree that the reply period will commence when I have supplied sufficient information to enable the school 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	Dawn Mills	01462 629000	LVA-DPL@bestacademies.org.uk
Lawnside Academy	Cheryl Johnson / Marissa Stoneham	01767 312313	LSA-DPL@bestacademies.org.uk
Pix Brook Academy	Indie King-Mand	01462 416243	PBA-DPL@bestacademies.org.uk
Campton Academy	Sarah Fraher	01462 813359	CMA-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

Procedure for processing personal information relating to staff

BEST require each school to ensure that adequate controls are in place with regard to access to personal information - giving access only to people (staff and governors) who need particular information to do their jobs and only when they need it. The guidelines below should be followed for access to personal information relating to staff.

Information relating to staff must be processed in accordance with the BEST GDPR Policy.

Viewing or removal of personal information relating to staff

Personal information relating to staff should not be removed from school premises, electronically or in paper format, unless there is an exceptional circumstance, and express permission should be sort from the Principal.

Each BEST school holds a log of who has requested and accessed personal information relating to staff. This log records the following information:

- Date of request
- Name of person requesting the information
- Name of who approved the request and date
- Date the information was viewed
- If a personnel file has been requested, the name and date of who logged this file back in should be recorded

HR Assistants in each school are not required to log any activity that occurs during their day to day duties. However, if a personnel file is removed from storage, this activity should be logged.

If HR Assistants require information from another BEST school, the authorisation process below should be followed.

Payroll information is managed by the Finance Team. Access to the payroll information by the Finance Team during their day to day activities does not need to be logged. However, if payroll information is removed from site, the authorisation process below should be followed.

The CEO, COO and Operations Support Officer have authority to view files from all BEST schools. However, the School Principal should be informed if these files are to be removed from site.

Access to files locally (in each BEST school) is restricted to the HR Assistant, Principal and Senior Leadership Team. However, a justifiable reason for access should be logged.

Hierarchy of approval:

Personal information relating to	Authorisation to be sought from
BEST staff	School Principal, CEO or COO
School Principals	CEO or COO
Executive Leaders	Chair or Vice Chair of BEST Board of Directors, CEO or COO as appropriate dependent on request

Trustees of BEST can request personal information relating to staff via the School Principal, CEO or COO but this must be for a specific reason. This activity must be logged.

In the event that personal information relating to the CEO is required, this can only be viewed by the Chair or Vice Chair of BEST Board of Directors. This activity must be logged.

Any Governor that feels they have sufficient reason to view or remove any personal information relating to staff must make a request for access to the file(s) via the Trustees of BEST. In this circumstance there must be a specific reason, the School Principal must be notified and the request/access must be logged as per the above procedure.

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 caseof 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	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, deputyhead 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	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	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		
Register of Admissions	Yes	School attendance: Departmental advice for maintained schools, academies, independent schools and local authorities	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	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 allother informationretained for 6 months	SECURE DISPOSAL
Pre-employment vetting information – DBS Checks	No	DBS Update Service Employer Guide: Keeping children safe in education. (Statutory Guidance from Dept. of Education)	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	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"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children"	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 protection related then see above otherwise dispose of at the conclusion of the case	SECURE DISPOSAL

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	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). Social Security Administration Act Limitation Act		
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; 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	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	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		
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 secondaryschool • to apupil referral unit • If the pupil dies whilst at primary school the file should be returnedto the Local Authority to be retained for the statutory retentionperiod. 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 LocalAuthority
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	entry was made.	
Correspondence relating to authorized absence		Education Act	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 Special Educational Needs and Disability Act	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	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	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 yearSATsresults. 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 + 1year	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 Guidancewebsite 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 Guidancewebsite 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 andother 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 E – 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 – Princpal and 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 of becoming aware of the incident).

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 or the breach report line (0303 123 1113) within 72 hours. As required, the DPO will set out:

- A description of the nature of the personaldata 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 thebreach 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:

- A description, in clear and plain language, of the nature of the personal data breach
- The name and contact details of the DPO
- A description of the likely consequences of the personal databreach
- 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.

Follow up actions by DPO:

- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts relating to the breach
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored centrally on the Trust's computer system.

- The DPO, Principal and DPL will review what has happened and how it can be stopped from happening again. This review will take place as soon as reasonably possible.

- DPO will consider the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. The Trust will review the effectiveness of these actions and amend them as necessary after any data breach.

  Special category data (sensitive information) being disclosed via email (including safeguarding records:
    - If special category data is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
    - Members of staff who receive personal data sent in error must alert the sender and the DPL or DPO as soon as they become aware of the error
    - If the sender is unavailable or cannot recall the email for any reason, the DPO or DPL will ask the ICT department to attempt to recall it
    - In any cases where the recall is unsuccessful, the DPL or DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
    - The DPO or DPL will ensure that a written response is received from individuals who received the data, confirming that they have complied with this request
    - The DPO or DPL will carry out an internet search to check that the information has not been made public; if it has, the DPO or DPL will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

  Other types of breach might include:
    - Details of pupil premium interventions for named children being published on school website
    - Non-anonymised pupil exam results or staff pay information being shared with governors
    - A school laptop containing non-encrypted sensitive personal data being stolen or hacked
    - The school's cashless payment provider being hacked and parents' financial details stolen