General Data Protection Regulation Policy

Policy approval date	October 2020
Policy review date	October 2022
Policy Lead	Data Protection Officer
Trustee approval	Trustee Approval
Committee responsible for policy	Trust Resource Committee

Contents

1. Aims

Our Trust aims to ensure that all personal data collected about staff, pupils, parents, Trustees, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

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

This policy sets out the Trusts commitment to GDPR and the implementation of a data protection by design approach.

The Trust will refer to documents and guidance from the Information Commissioner's Office and the Department for Education in relation to GDPR and data processing.

This includes ensuring the following:

- The creation and maintenance of a data protection working group
- Assigning responsibility to an individual within The Trust
- Assigning a Data Protection Officer
- Development and maintenance of a GDPR project
- Ensuring that all staff are trained in data protection and take responsibility for the collection, processing, storage and destruction of data
- A lawful basis for processing is documented for all processing activity
- Principles relating to processing of personal data are adhered to
- The rights of data subjects are respected
- Risks to the rights of data subjects are assessed and mitigated for all large-scale and new processing
- Regular independent reviews of processing activity and processing documentation are carried out
- Trust and technical measures are implemented to protect data

Data breaches impacting on the rights and freedoms of data subjects will be reported to the Information Commissioner's Office (ICO)

2. Legislation and guidance

This policy meets the requirements of the GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions

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

4. The data controller

Our Trust determines the purpose and the means of personal data processing and therefore is a data controller.

The Trust is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

The Trust as the Data Controller will comply with its obligations under the GDPR and the Data Protection Act 2018. The Trust is committed to being concise, clear and transparent about how it obtains and uses personal information and will ensure data subjects are aware of their rights under the legislation. This policy sets out how the Trust will do this.

All Trust staff and Trust workforce must have a general understanding of the law and understand how it may affect their decisions in order to make an informed judgement about how information is gathered, used and ultimately deleted. All staff must read, understand and comply with this policy in order to comply with its obligations under GDPR and the Data Protections Act 2018.

The Information Commissioner as the Regulator can impose substantial fines for breaches of GDPR and the Data Protection Act 2018 and other Data Protection Legislation. Therefore, it is imperative that the Trust, all staff and the workforce comply with the legislation. The Data Protection Officer will be the principal point of contact with the ICO.

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

5.1 Board of Trustees

The Board of Trustees has overall responsibility for ensuring that our Trust complies with all relevant data protection obligations.

5.2 Data protection officer

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

The DPO will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on Trust data protection issues.

The DPO is also the first point of contact for individuals whose data the Trust processes, and for the ICO.
Full details of the DPO's responsibilities are set out in their job description.

The Trust shall ensure that the Data Protection Officer is involved properly and in a timely manner, in all issues which relate to the protection of personal data

The Trust shall support the Data Protection Officer in performing the responsibilities outlined below by providing resources necessary to carry out those tasks and access to personal data and processing operations. The Data Protection Officer shall maintain his or her expert knowledge.

Data subjects may contact the Data Protection Officer with regard to all issues related to processing of their personal data and to the exercise of their rights under the regulations.

The Data Protection Officer and the Data Protection Lead will be bound by confidentiality and must maintain data security by protecting the confidentiality**,** integrity and availability of all personal data, defined as follows:

1. **Confidentiality** means that only people who have a need to know and are authorised to use the personal data can access it.
2. **Integrity** means that personal data is accurate and suitable for the purpose for which it is processed.
3. **Availability** means that only authorised users can access the personal data when they need it for authorised purposes.

The Data Protection Officer shall have the following responsibilities:

- Review of all data processing activities (inventory / mapping)
- Conduct of regular health checks/audits and issue recommendations
- Assist with data protection impact assessments and monitoring performance
- Monitoring and advice relating to subject access requests and data breaches
- Assist the Trust with maintenance of records
- Monitoring and advice relating to FOI and other information requests
- Cooperation with, and acting as the contact point for the Information Commissioner's Office, who are the supervisory authority in respect of all data protection matters
- Act as the contact point for data subjects to deal with requests and complaints
- Training of Trust staff and workforce

Our DPO is Data Protection Education Limited and is contactable via email DPO@dataprotection.education

5.3 Head teacher

The head teacher or head of school acts as the representative of the data controller on a day-to-day basis.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this and related policy and procedures
- Informing the Trust of any changes to their personal data, such as a change of address

Contacting the DPO in the following circumstances:

- With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure

- If they have any concerns that this policy is not being followed
- If they are unsure whether or not they have a lawful basis to use personal data in a particular way
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data to a third country or to an international organisation
- 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 and data subject rights

6.1. Data protection principles

Anyone processing personal data must comply with the data protection principles. The Trust will comply and is committed to these principles in relation to any processing of personal data. The Data Protection principles provide that personal data must be:

- **Processed lawfully, fairly and in a transparent manner** in relation to the data subject and their rights;
- **Collected for specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes;
- **Adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed;
- **Accurate and, where necessary, kept up to date;**
- **Kept in a form which permits identification of data subjects for no longer than is necessary**;
- **Processed in a manner that ensures appropriate security of the personal data**
- **Must NOT be transferred to people or Trusts situated in other countries without adequate protection.**

6.2. Data subject rights

The Trust supports the rights of data subjects (or the parents/carers of data subjects where data subjects are not able to demonstrate the capacity to understand their rights) in relation to data that is processed or stored about them, as follows:

- Right to fair and transparent processing
- Right of access
- Right of rectification
- Right to erasure (the "right to be forgotten")
- The right to restrict processing
- Right to be notified of erasure, rectification or restriction
- Right of data portability
- Right to object to processing
- Right to object to processing for the purposes of direct marketing
- Right to object to processing for scientific, historical or statistical purposes
- Right to not be evaluated on the basis of automated processing
- Right to withdraw consent at any time
- Right to be notified about a data breach
- Right to an effective judicial remedy against a supervisory authority
- Right to lodge a complaint with supervisory authority
- Right to an effective judicial remedy against a controller or processor
  Right to compensation

This policy sets out how the Trust aims to comply with these principles and rights and the Trust shall maintain procedures, policies and notices to ensure that data subjects are informed of their rights.

7. Collecting personal data

Lawfulness, fairness and transparency

7.1. For personal data to be processed lawfully it must be processed on the basis on one of the legal grounds set out in the DATA Protection Legislation. The Trust will only process personal data where a lawful basis for processing exists. Specifically, where:

- 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 (e.g the Education Act 2011)
- 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

7.2. For personal data to be processed fairly, data subjects must and will be made aware of the following in our privacy notices or requests to process data:

- That the personal data is being processed
- Why the personal data is being processed
- What the lawful basis is for that processing (see below)
- Whether the personal data will be shared, and if so with whom
- The period for which the personal data will be held
- The existence of the data subject's rights in relation to the processing of that personal data; and
- The right of the data subject to raise a complaint with the Information Commissioner's Office in relation to any processing

The Trust will only process data that is **necessary and relevant to the purpose for which it was gathered, and will ensure that we have a lawful basis for any processing.**

Data collected for the purposes of public health (including visitor contact data for COVID-19) will be kept as long as required. Contact data for visitors will be kept for 21 days after the most recent visit, with information on visitors kept as per standard retention requirements. Public Health data may be shared with third-parties as required including, but not limited to:

- National Health Service (including NHS Test and Trace)
- Public Health England
- Other local health authorities

Data collected and processed for public health purposes is done so under GDPR Article 9(2)(i) which states: (in part) "processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health..." and Recital 54 which includes: "The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject."

Collection and processing of visitor data will be documented in the privacy notices and in a statement available to visitors at the time of data collection to include the following information:

"We collect the following visitor information for the purposes of security, safety and public health:

- Name
- Organisation
- Date and time of visit
- Contact details

These are kept for six years in case of any claims by students, staff or visitors under the Limitations Act (1980). Contact details will be deleted after 21 days.
Should a positive test for COVID-19 be identified, relevant visitor data will be shared with the required public health authorities. A COVID Secure Notice confirming we have an active risk assessment for visitors is on display at reception.

7.3. For personal data to be processed lawfully it must be processed on the basis on one of the legal grounds set out in the DATA Protection Legislation. The organisation will only process personal data where a lawful basis for processing exists. Specifically, where:

- 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 (e.g the Education Act 2011);
- 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.

7.4. Special category data

This is data relating to **health; race; sexuality; religion; criminal offences; political opinions and union memberships**.

For special categories of personal data, will not be processed unless a specific lawful basis as listed in Article 9 of the GDPR applies. When this special category data is being processed we will normally only do so under the following legal grounds:

- Where the processing is **necessary for employment law** purposes, for example in relation to sickness absence
- Where the processing is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment
- Where the processing is necessary for **health or social care purposes**, for example in relation to pupils with medical conditions or disabilities; and
- **Where none of the above apply then we will seek the consent of the data subject to the processing of their special category personal data**

7.5. Consent

When pupils, staff or our Workforce join the Trust a consent form will be required to be completed in relation to them. This consent form(s) deals with:

- Biometric data – information from fingerprints for school dinner payment
- School/Classroom displays
- School newsletters
- School prospectus
- Trust/School website
- School social media accounts
- Newspapers
- Participation in trips & fixtures

Where appropriate third parties may also be required to complete a consent form.

In relation to all pupils under the age of 12 years old we will seek consent from an individual with parental responsibility for that pupil.

We will generally only seek consent directly from a pupil if they are legally able to give such consent. The legal age for consent under Data Protection legislation is 12. However we recognise that this may not be appropriate in certain circumstances and therefore the Trust may be required to seek consent from an individual with parental responsibility. If consent is required for the processing of personal data of any data subject then the form of this consent must:

- Inform the data subject of exactly what we intend to do with their personal data;
- Require them to positively confirm that they consent (we cannot ask them to opt-out rather than opt-in); and
- Inform the data subject of how they can withdraw their consent
- Any **consent must be freely given**, which means that we cannot make the provision of any goods or services or other matter conditional on a data subject giving their consent.

  The DPO must always be consulted in relation to any consent form before consent is obtained.

  A record must always be kept of any consent, including how it was obtained and when.

There may be circumstances where it is considered necessary to process personal data or special category personal data in order to protect the vital interests of a data subject. This might include safeguarding, child protection and medical emergencies where the data subject is not in a position to give consent to the processing. We believe that this will only occur in very specific and limited circumstances. In such circumstances we would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur. Please refer to the Trust Safeguarding Policy, Child Protection Policy and Trust Medical Policy for further information.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.6 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Trust's record retention schedule, which is available on the GDPR Audit.

8. Sharing personal data

We may share personal data that we hold about data subjects, with other organisations, without consent, where we have a lawful basis for doing so. Such organisations include the Department for Education and Education and Skills Funding Agency "ESFA", Ofsted, health authorities and professionals, the Local Authority, examination bodies, other organisations, and other organisations where we have a lawful basis for doing so.:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils. When doing this, we will:

    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law. Data processors who we may contract with include: Payroll providers; parent payment systems; pupil assessment systems; communication systems; photographers and HR systems.
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

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

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

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

Personal data will only be transferred to a data processor if they agree to comply with our procedures and policies in relation to data security, or if they put in place adequate measures themselves to the satisfaction of the organisation and in accordance with data protection law.

The Trust will inform data subjects of any sharing of their personal data unless we are not legally required to do so, for example where personal data is shared with the police in the investigation of a criminal offence.

9. DBS data

All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

Data provided by the DBS will never be duplicated.

Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

Data Subjects have the right to appeal against any automated decision making, such as a DBS check

10. Subject access requests and other rights of individuals

10.1 Subject access requests

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

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

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

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

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

10.2 Children and subject access requests

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

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

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

10.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

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

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

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

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

10.4 Other data protection rights of the individual

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

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- The Data subject can request a copy of agreements detailing the appropriate safeguards where personal data are transferred to a third country or to an international organisation
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

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

11. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request. A reasonable fee that takes into account admin costs may be charged.

12. Biometric recognition systems

Note: That in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18.

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

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The Trust will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

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

Parents/carers and pupils can object to participation in the Trust's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

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

13. CCTV

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

CCTV may be used for the purpose of protecting the safety of staff, students and visitors and to help secure the physical premises. Please refer to the Trust's CCTV Policy.
Notices of recording including details of the Data Controller and where a copy of Trust CCTV policy can be obtained will be included on clearly visible signs posted at all entrances to the Trust site(s).
All CCTV footage is securely stored and can only be accessed by appropriate members of staff. All images recorded by CCTV will be deleted as defined in the retention schedule.
Where the Trust installs new CCTV cameras, a data privacy impact assessment will be carried out prior to installation.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use. Any enquiries about the CCTV system should be directed in the first instance to the Facilities Manager.

14. Photographs and videos

As part of our Trust activities, we may take photographs and record images of individuals within our schools.
We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Photographs and videos will normally only be taken and used where they are deemed essential for performing the public task of the Trust or relative to providing education. However there may be occasions that arise where the Trust would like to celebrate the achievements of our pupils and therefore we may want to use images and videos of our pupils within promotional materials, or for publication in the media such as local, or even national, newspapers covering Trust events or achievements. If this is the case we will seek the consent of the pupils, and their parents where appropriate, before allowing the use of images or videos of pupils for such purposes.
Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

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

The retention period for photographs and videos taken by the Trust, Trust staff and workforce will be documented in the Trust retention schedule. At the end of the retention period photographs will either be destroyed or they may be retained as photos for archiving purposes in the public interest.

Parents and others attending Trust events are allowed to take photographs and videos of those events for domestic purposes. For example, parents can take video recordings of a Trust performance involving their child. The Trust does not prohibit this as a matter of policy. The Trust does not however agree to any such photographs or videos being used for any other purpose, but acknowledges that such matters are, for the most part, outside of the ability of the Trust to control or prevent.
The Trust asks that parents and others do not post any images or videos which include any child other than their own child on any social media or otherwise publish those images or videos.

Whenever a pupil begins their attendance at the Trust they, or their parent where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that pupil. We will not use images or videos of pupils for any purpose where we do not have consent.
Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

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

15. Data protection by design and default and data protection impact assessments

The Trust takes data protection very seriously, and will consider and comply with the requirements of Data Protection Legislation in relation to all of its activities whenever these involve the use of personal data, in accordance with the principles of data protection by design and default by:

- Consulting with the Trusts DPO when a data protection impact assessment is required
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the Trust's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant

Maintaining records of our processing activities, including:

- For the benefit of data subjects, making available the name and contact details of our Trust and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
- For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

16. Data security and storage of records

The Trust will implement appropriate data security measures using policies, procedures and technologies to ensure and maintain the security of all personal data from the point of collection to the point of destruction. These security measures will be appropriate to the risks in processing personal data and will be consistent with the rights of the data subjects. We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Measures and data access controls to ensure that the Personal Data can only be accessed by authorised personnel for the purposes agreed in the record of processing activity and outlined in the organisation privacy notice, for example:

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

17. Data retention and disposal of records

The Trust will not keep personal data longer than necessary and will maintain a retention schedule outlining the retention requirements of electronic and paper records. The Trust will retain the minimum amount of information that it requires to carry out its statutory functions and the provision of services.
In circumstances where a retention period of a specific document has expired, checks will be made to confirm disposal and consideration given to the method of disposal to be used based on the data to be disposed of. These checks will include the following questions being addressed:

- Have the documents been checked to ensure they are appropriate for destruction?
- Is retention required to fulfil statutory obligations or other regulatory obligations, including child protection?
- Is retention required for evidence?
- Is retention required to meet the operational needs of the service?
- Is retention required because the document or record is of historic interest or intrinsic value?

  Retention data will be documented in the Record of Processing or taken as published in the IRMS school toolkit.

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

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

18. Personal data breaches

In the case of a personal data breach, The Trust shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Information Commissioner's Office, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Where the notification to the Information Commissioner's Office is not made within 72 hours, it shall be accompanied by reasons for the delay.

In order to evaluate the personal data breach The Trust shall without undue delay immediately inform and involve the Data Protection Officer in the assessment of the breach and in the execution of the data breach procedure to contain and manage the breach.

The notification to the Information Commissioner's Office shall at least:

- describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- describe the likely consequences of the personal data breach;

- describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects;
- Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

The Trust shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken in a data breach log. The log shall enable the Information Commissioner's Officer to verify compliance with the data breach rules and raise awareness of minor breaches that may assist in the identification of new data handling processes and training requirements.

For examples of data breaches please see Appendix 1

19. Training

All staff, Trustees and governors are provided with data protection training as part of their induction process.
Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Trust's processes make it necessary.

20. Monitoring arrangements

We may change this policy at any time. Where appropriate, we will notify data subject**s** of those changes.
This Policy was approved by the board of Governors on ADD DATE . It will be reviewed annually.

21. Links with other policies

This data protection policy is linked to our:

- Freedom of information policy
- Child protection Policy
- E-Safety Policy
- Acceptable User Agreement
- CCTV Policy

Appendix 1: Personal data breach procedure

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

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the CEO and the chair of trustees
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the Trust network in the GDPR file.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach

    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored on the Trust network in the GDPR file.

- The DPO and head teacher/head of school will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

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

Sensitive information being disclosed via email (including safeguarding records)

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

Trust laptops

- All Trust laptops are encrypted
- If a laptop is lost or stolen the Trust will notify the DPO and record this on the data breach log. An internet search to check that the information has not been made public will be completed; if it has, we will liaise with our DPO and contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.