# THE EDUCATION VILLAGE ACADEMY TRUST

# GENERAL DATA PROTECTION REGULATION
# DATA PROTECTION POLICY

# Values and Ethos

Our values and ethos are inclusive and child centred. Our Trust is founded on the principles of inclusivity, diversity and fairness, and they are fundamental to our delivery of exceptional learning experiences.

EVAT stands for:

- **Excellence** and high standards
  - a can-do culture and no-excuses ethos
- **Values driven** with a deep sense of purpose
  - putting children and young people first
  - behaving ethically
- **Ambition** and aspiration for all
  - irrespective of background or barriers – being truly inclusive
- **Teamwork**
  - we do more, better and faster, together

We are a village. We collaborate, with our learners, their families and our communities, to provide exceptional education so that all the children and young people we serve achieve the best possible outcomes.

## *Our Ethos is to:*

- Create a nurturing and friendly atmosphere and provide an environment where everyone feels valued for who they are
- Bring out the best in every child and young person and meet the full range of their individual needs
- Provide different and unique experiences, challenges and activities
- Show tolerance and respect for each other
- Prepare our children and young people for lifelong learning
- Improve the life chances of every child and young person we serve.

**EVAT Version Control**

| Version: | Date: | Policy Owner: | Amendments made by: | Details of amendments made: | Reviewed by: | Approved by: |
|---|---|---|---|---|---|---|
| V0.1 | 20/10/16 | Mike Butler | Wendy Turpin | Initial draft | C Knights/ Mike Butler | - |
| V1.0 | 09.03.16 | Mike Butler | Wendy Turpin | Final | | Mike Butler |
| V1.1 | 16.05.18 | Mike Butler | Wendy Turpin & Cathy Knights | Amendments to reflect GDPR | | |
| V1.2 | 18.05.18 | Mike Butler | Mike Butler | Final QA buy policy owner | Mike Butler | Board of Directors* (July 2018) |
| V1.3 | 16.04.20 | Mike Butler | Wendy Turpin | Amendment v review v protecting Biometric Information | C Knights | |
| V2.0 | 17.7.20 | Mike Butler | Cathy Knights | Amendment to say passwords must be changed every 60 days. | Board of Trustees | 16.7.20 |
| V2.2 | 01.03.21<br>29.09.21 | Marie Roe | Wendy Turpin | New policy owner. Cross ref Trust policies, comparison with School Bus model, alignment Brexit, changes to procedures following Veritau contract & comments on this policy. | | |
| V2.3 | 07.11.21 | Marie Roe | Wendy Turpin | | | |
| V3.0 | 10.12.21 | Marie Roe | Wendy Turpin | Final version | Board of Trustees | 10.12.21 |

## 1. Monitoring and review

This policy is reviewed every **two years** by the Policy Owner: **Marie Roe**

The scheduled review date for this policy is **July 2023**.

**Contents**



N.B. Where reference is made to an 'Academy' or a 'Academy' the intention is that the policy is universal and applies to both. Any reference to Principal may also include Executive Principal, Head of Academy or another member of ELT or SLT.

## 1. Aims

The Education Village Academy Trust (EVAT or 'the Trust') is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under data protection legislation. The Trust may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly local authorities, other academies and educational bodies.
Through this policy our aims are to ensure all staff, Trustees and Education Standards Committee (ESC) members are aware of their responsibilities, and to outline how we comply with the UK GDPR core principles.

This policy applies to all personal data, regardless of whether they are in paper or electronic form.

## 2. Legislation and guidance

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

- The UK General Data Protection Regulation (GDPR)
- Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- Academy Standards and Framework Act 1998
- Data Protection Act 2018

In addition, this policy complies with our Funding Agreement and Articles of Association.

## 3. Definitions

| Term | Definition |
|---|---|
| **Personal data**<br>**The UK GDPR applies to both electronic personal data and to manual filing systems** | Any information relating to a living identified, or identifiable, individual<br>This may include the individual's:<br>• Name (including initials)<br>• Identification number |

| | |
|---|---|
| | • Location data<br>• Online identifier, such as an IP address and/or username<br>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 are more **sensitive** and so needs more protection, including information about an individual's:<br>• Racial or ethnic origin<br>• Political opinions<br>• Religious or philosophical beliefs<br>• Trade union membership<br>• Genetics<br>• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes<br>• Health – physical or mental<br>• 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.<br>Processing can be automated or manual. |
| **Data subject** | The identified or identifiable individual whose personal data are held or processed. |
| **Data controller** | A person or organisation that determines the purposes and the means of processing of personal data. |
| **Data processor** | A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller. |

| | |
|---|---|
| **Personal data breach** | A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. |
| | |

**4. The Data Controller**

The Trust processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The Trust is registered as a Controller with the ICO and will renew this registration annually or as otherwise legally required. Under the UK GDPR, the Data Controller is responsible for compliance with, and demonstrating compliance with, all the data protection principles as well as the other UK GDPR requirements. The Data Controller is also responsible for the compliance of Trust processors.

**5. Roles and responsibilities**

This policy applies to Trust staff, Trustees and ESC members, volunteers and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

**Board of Trustees**

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

**Chief Executive Officer (CEO)**

The CEO acts as the representative of the data controller on a day-to-day basis and is also the Trust's Chief Accounting Officer.

**Senior Information Risk Owner (SIRO)**

The Senior Information Risk Owner is responsible for the Trust's information risk policy, acts as champion for information risk at the Board, and provides advice to the accounting officer on the content of the organisation's statement of internal control in regard to information risk.

**Information Asset Owner**

An Information Asset Owner (IAO) is the individual responsible for an information asset, understands the value of that information and the potential risks associated with it. The Trust will ensure that IAOs are appointed based on sufficient seniority and level of responsibility.

IAOs are responsible for the security and maintenance of their information assets. This includes ensuring that other members of staff are using the information safely and

responsibly. The role also includes determining the retention period for the asset, and when destroyed, ensuring this is done so securely.

**Data Protection Officer (DPO)**

The Trust has appointed Veritau Ltd to be its Data Protection Officer (DPO). The role of the DPO is statutory. Veritau acts in an advisory capacity to ensure the Trust, as Data Controller, is compliant.

However, if you would like to discuss anything in this policy, please contact the Trust's Specific Point of Contact (SPOC) who is the first point of contact for all Data Protection issues -

Alana Mackenzie,
The Education Village Academy Trust,
Salters Lane South
Darlington
DL1 2AN

Email: amackenzie@educationvillage.org.uk
Tel: 01325 248156

Veritau's contact details are:

Veritau Ltd
County Hall
Racecourse Lane
Northallerton
DL7 8AL

**Specific Point of Contact (SPOC)**

The SPOC is the first point of contact for individuals whose data EVAT processes and is responsible for:

- Overseeing the implementation of this policy
- Monitoring the Trust's compliance with the UK GDPR other data protection laws
- Informing and advising the Trust and its employees about their obligations to comply with GDPR and other laws
- Managing internal data protection activities, advising on DPIAs and conducting internal audits
- Developing related policies and guidelines where applicable
- Processing Subject Access Requests.

They will provide an annual report of their activities directly to the Board and, where relevant, report to the Board their advice and recommendations on EVAT data protection issues.

**All staff**

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the Trust of any changes to their personal data, such as a change of address
- Contacting the SPOC 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, or if one is suspected
    - 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 UK GDPR is based on data protection principles that the Trust 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 they are processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which they are processed
- Processed in a way that ensures they are appropriately secure.

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

## 7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear and unambiguous **consent**.

- The data needs to be processed so that the Trust can **fulfil a contract** with the individual, or the individual has asked the Trust or Academy to take specific steps before entering into a contract.
- The data needs to be processed so that the Trust 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 Trust, 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 Trust or a third party (provided the individual's rights and freedoms are not overridden).

The Trust will only process personal data without consent where any of the above purposes cannot reasonably be achieved by other, less intrusive means or by processing fewer data.

the special category conditions for processing which are set out in the UK GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as learning apps, and we intend to rely on consent as a basis for processing, we will obtain 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 through the provision of a privacy notice.

7.2 Limitation, minimisation and accuracy

The Trust has an obligation to ensure that personal data is accurate and complete. This is referred to as the Accuracy Obligation. The aim of the Accuracy Obligation is to ensure that where personal data may be used to make a decision that affects the individual, the data is reasonably correct and complete so as to ensure that 9the decision is is made taking into account all relevant parts of accurate personal data.

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 them, 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 they are deleted or anonymised. This retention of data is in accordance with the schedule set out in the Information and Records Management Society's toolkit for academies (see pages 37-56).

7.3 Consent

- Must be a positive indication expressly confirmed in words. It cannot be inferred from silence, inactivity, a positive action without words or pre-ticked boxes.
- Will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

- Where it is given, a record will be kept documenting how and when consent was given, and what the data subject was told.
- We will ensure that consent mechanisms meet the standards of the UK GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.
- Consent accepted under the DPA will be reviewed to ensure it meets the standards of the UK GDPR; however, acceptable consent obtained under the DPA will not be reobtained.
- Can be withdrawn by the individual at any time.

**8. Sharing personal data**

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing so
- There is a statutory requirement, for instance to share data with the DfE or LA
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils e.g. IT companies. When doing so, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

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

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

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

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

**9. Subject access requests and other rights of individuals**

9.1 Subject access requests

Individuals, including children, have a right to make a 'subject access request' (SAR) to gain access or a copy of their personal and other supplementary information that the Trust holds about them in order to verify the lawfulness of the processing. This includes:

- Confirmation that their personal data are 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 or email to the SPOC 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 SPOC.

See Appendix 2 for the SAR procedure.

9.2 Children and subject access requests

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

Children 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 aged 12 or over on roll at one of our Trust's academies or academies may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

- When responding to requests, we:
- Will acknowledge within 5 working days.
- ask the individual to provide 2 forms of identification to verify their identify
- May contact the individual via telephone to confirm the request was made.
- Will respond without delay and within 1 month of receipt of the request.
- 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.
- Will provide a copy of the information to the individual free of charge; however, the Trust may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual requests further copies of the same information.
- Where a SAR has been made for information held about a child, we will evaluate whether the child is capable of fully understanding their rights. If the Trust determines the child can understand their rights, it will respond directly to the child.
- 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.Where a SAR has been made electronically, the information will be provided in a commonly used secure electronic format. SARS submitted via other means will be responded to however the applicant requests.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.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request, 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:

- Be informed about how we use their data. Privacy Notices issued to individuals in regard to the processing of their data will be clear and transparent. Withdraw their consent to processing at any time.
- Ask us to erase their personal data, or object to the processing of it (in certain circumstances) where there is no compelling reason for its continued processing. However, this right is not absolute and is dependent on the lawful basis on which the processing was done.
- Ask us to rectify incomplete or inaccurate personal data. Requests for rectification will be responded to within one month but this may be extended to two months. We will take reasonable steps to ensure that data is accurate or is rectified if inaccurate, implementing a proportional response for data that has a significant impact on the individual, e.g. if significant decisions are made using that data. We will restrict processing of the data in question whilst its accuracy is being verified, where possible. Where no action is being taken in response to a request for rectification, or where the request has been investigated and the data has been found to be accurate, the Trust will explain the reason for this to the individual and will inform them of their right to complain. Requests for rectification will be investigated and resolved, where appropriate, free of charge; however, the Trust may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual makes multiple requests at once. The Trust

reserves the right to refuse to process requests for rectification if they are manifestly unfounded or excessive or if exemptions apply.

- Prevent use of their personal data for direct marketing.
- Challenge processing which has been justified on the basis of public interest.
- 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 SPOC. If staff receive such a request, they must immediately forward it to the SPOC.

Requests will be responded to within one month. This may be extended by two months if the request is complex.

Requests for erasure will be handled free of charge; however, the Trust may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual makes multiple requests at once.

## 10. Parental requests to see the educational record

There is no legal right for parents or carers to access to their child's educational record (which includes most information about a pupil), but the Trust will do all it can to assist. Request will be treated as Subject Access Requests. It is important that handling any such requests does not take a disproportionate amount of time for staff. Where records are held electronically a parent or carer may be invited into the academy or academy to view the record and the Trust would appreciate co-operation in managing requests so that they do not have a significant impact on staff time. Any such request should be made to the Principal of the academy or academy the child attends.

## 11. Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use fingerprints to receive academy dinners instead of paying with cash), we will comply with the requirements of the DfE (2018) Protection of Biometric Information of Children in Academies and Colleges and 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 obtain 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 are 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.

## 12. CCTV

The Trust understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

We do not need to ask individuals'' permission to use CCTV and it is used in various locations around the Trust's sites to ensure they remain safe. We will adhere to the ICO's code of practice for the use of CCTV.

A copy of our CCTV Privacy Notice can be found on our website.

Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose. All CCTV footage will be kept for three months for security purposes; the Health and Safety Manager is responsible for keeping the records secure and allowing access.

Any enquiries about the CCTV system should be directed to the SPOC.

## 13. Photographs and videos

As with CCTV, the Trust understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles. Please see the Trust's Photography Policy at Appendix 3.

## 14. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a DPO, SIRO and SPOC, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that are 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

- 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 contact details for our Academies/Academies 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.

## 15. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops, that contain personal data are kept under lock and key when not in use.
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access.
- Where, exceptionally, personal information needs to be taken off site, staff must sign it in and out from the relevant academy/academy office (e.g. list of pupils and their contact details when going on an academy trip). They must also commit to keeping information secure in line with documented procedures and risk assessments whilst outside Trust premisses.
- All computers and work devices containing personal or photographic information must be password protected.
- Passwords that are at least 8 characters long containing letters and numbers are used to access academy/Trust computers. Staff are required to change their passwords every 60 days.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure they are stored securely and protected adequately (see section 8).

## 16. Disposal of records

Personal data that are 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. All disposals will be in accordance with the Trust's Records Management Policy and Procedure

For example, we will shred 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.

## 17. Personal data breaches

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The Trust will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, the DPO, with support from the SIRO/SPOC, will coordinate an effort to establish whether a personal data breach has occurred, assess the significance of any breach, and take prompt and appropriate steps to address it. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed. All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the Trust becoming aware of it. The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis. In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the Trust will notify those concerned directly and quickly.

The SPOC will follow the full procedure as set out in Appendix 1.

## 18. Training

All staff, Trustees and ESC Members are provided with data protection training as part of their induction process, staff are asked to complete an on-in line training package annually and responsibilities are set out in the Trust's Code of Conduct. The Trust will ensure that all staff, Trustees and ESC members are made aware of, and understand, what constitutes a data breach as part of their ongoing development.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Trust's processes make it necessary.

## 19. Monitoring arrangements

This policy will be reviewed, updated and approved by the Board of Trustees every 2 years or whenever changes in legislation may affect our working practices.

## 20. Links with other Trust policies

This policy is linked to our:

- Freedom of information Policy
- E-Safety Policy
- Safeguarding and Child Protection Policy
- Records Management Policy & Retention Schedule
- CCTV Policy
- Educational Visits Policy

## 21. Public Sector Equality Duty (Equality Act 2010)

In preparing or amending this policy, the author has given due regard to the Public Sector Equality Duty; that is they have considered any potential impact on people who share certain protected characteristics. These protected characteristics are defined as: race, disability, sex, age, religion or belief, sexual orientation, pregnancy and maternity and gender reassignment.

## 21. 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 SPOC.
- The SPOC will investigate the discovery and report the incident to the DPO and in agreement they will determine the consequences, level of risk and whether a breach has occurred. To decide, they 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 SPOC will alert the SIRO, CEO, Principal/s and the Chair of the Board of Trustees as appropriate.
- The DPO and SPOC 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 and SPOC will work out whether the breach must be reported to the ICO, which must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to affect people's rights and freedoms negatively, 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 is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO, The ICI report will be agreed between the DPO and the SIRO.

The SPOC 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 or potential breach. Documented decisions are stored on the Trust's secure IT network by the SPOC, in a drive where access is limited to specific staff members.

- Where the ICO must be notified, the DPO will do so 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 not all the above details are 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 SPOC 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's secure IT network, in a drive where access is limited to specific staff members.

- The SPOC and CE and/or Principal(s) 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 SPOC as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the SPOC will ask the IT department to recall it
- In any cases where the recall is unsuccessful, the SPOC 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 SPOC will take all reasonable steps to ensure the Trust receives 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, they or the IT team will contact the publisher/website/social media application owner or administrator to request that the information is removed from their publication/website/ social media application and deleted

**Information or images shared via the Trust's website or social media channels**

- If special category data (sensitive information) is accidentally made available via the website or social media channels (i.e. without the data subject's consent), the information or image must be removed as soon as possible after the error is found.
- The SPOC will carry out an internet search to check that the information has not been shared more widely; if it has, they or the IT team will contact the publisher/website/social media application owner or administrator to request that the information is removed from their publication/website/ social media application and deleted.

## 22. Appendix 2 – Subject Access Request Procedure

### Subject Access Requests and Educational Records Requests Procedure

**Role of the SPOC**

1. **Receives, Reads, make a note of the request**
   Reads the request or make a note of the request if made verbally (confirm that the note you have made is accurate if verbal).

2. **Records request on Trust log**

3. **Validates the request**
   Confirms that the requester is who they say they are and that they have a right to access the information (e.g. whether they have parental responsibility).

4. **Retrieves**
   Locates all the relevant information for consideration, keeping a record of systems checked and the search criteria used.

5. **Refers to others**
   Consults any individuals or departments who may have a view or may be affected by the release of information (e.g. safeguarding team or third parties who are referred to in the information).

6. **Redacts**
   Removes any information that is either not relevant to the request or which is not authorised for disclosure (e.g. information about another pupil). The 'redacted' copy is what will be sent to the applicant.

7. **Reviews**
   Once the response has been prepared (see letter template)
   sends to the SIRO or CEO for final decisions as to whether the information should be disclosed or not.

8. **Replies**
   Sends approved response to the applicant in writing. This should be filed along with an exact copy of the disclosed information.

9. **Updates Trust log**
   Retains copies of information and, if the information is not disclosed the reason why. This will enable the Trust to effectively review its response in the event of a complaint.

## 23. Appendix 3

## Photography Policy

### 1 Responsibilities

1.1 Trust Principals are responsible for:

- Submitting consent forms to parents, and pupils where appropriate, at the beginning of the academic year with regards to photographs and videos being taken whilst at a Trust academy.
- Ensuring that all photos and videos are stored and disposed of correctly, in line with the GDPR and the DPA 2018.
- Deciding whether parents are permitted to take photographs and videos during Trust/ academy events.
- Communicating this policy to all the relevant staff members and the wider academy community, such as parents.

1,2 Designated Safeguarding Leads (DSLs) are responsible for:

- Liaising with social workers to gain consent for the use of photographs and videos of LAC pupils.
- Liaising with the DPO to ensure there are no data protection breaches.
- Informing the principal or head of academy of any known changes to a pupil's security, e.g. child protection concerns, which would mean that participating in photography and video recordings would put them at significant risk.

1.1 Parents, and pupils where appropriate, are responsible for:

- Completing the Consent Form on an annual basis.
- Informing the academy in writing if they wish to make any changes to their consent.
- Acting in accordance with this policy.

1.2 In accordance with the Trust's requirements to have a DPO, the SPOC supported by the DPO is responsible for:

- Informing and advising the Trust and its employees about their obligations to comply with the GDPR and the DPA 2018 in relation to photographs and videos at academy.
- Monitoring the Trust's compliance with the GDPR and the DPA 2018 in regards to processing photographs and videos.
- Advising on data protection impact assessments in relation to photographs and videos at academy
- Conducting internal audits regarding the Trust's procedures for obtaining, processing and using photographs and videos.
- Providing the required training to staff members in relation to how the GDPR and the DPA 2018 impacts photographs and videos at academy.

1.3 Overall responsibility for the appropriate use of photography within the Trust and in connection with academy events rests with the Chief Executive Officer (CEO).

## 2 Consent

2.1 All photographs and video content are classified as personal data under the GDPR and the DPA 2018; images or video content may be used for publicity or other purposes only once informed consent has been provided, and it has not been withdrawn.

2.2 [Primary academies only] Parents are responsible for providing consent on their child's behalf, except where the processing is related to preventative or counselling services offered directly to children.

2.3 [Secondary academies only] Where the academy opts to provide an online service directly to a child, the child is aged 13 or over, and the child understands what they will be consenting to, the academy will obtain consent directly from the child; otherwise, consent will be obtained from whoever holds parental responsibility for the child, except where the processing is related to preventative or counselling services offered directly to children.

2.4 [Secondary academies only] In all other instances with regards to obtaining consent, an appropriate age of consent will be considered by the academy on a case-by-case basis, taking into account whether the child understands what they will be consenting to.

**2.5** Parents and pupils are required to be aware that their child/they may be photographed at academy and they have the right to withdraw consent for:

- Photographs or video taken by members of staff for academy-based publicity and promotional purposes (academy newsletters/prospectus) or for anonymous use on the academy website.
- Photographs or video taken by parents and other family members of children at the academy during academy concerts, performances, sports events and other similar events organised by the academy.
- Photographs or video taken by members of the press who are on the academy premises by invitation in order to celebrate individual, group or academy success.

2.6 The Trust understands that consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

2.7 Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

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

2.9 Parents and pupils, as applicable, will be asked to complete the Consent Form on an annual basis, which will determine whether or not they allow their child/themselves to participate in photographs and videos.

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

2.11 If there is a disagreement over consent, or if a parent/pupil does not respond to a consent request, it will be treated as if consent has not been given and photographs and videos will not be taken or published of the pupil without consent.

- All parents and pupils are entitled to withdraw or change their consent at any time during the academy year.
- Parents or pupils withdrawing their consent must notify the academy in writing.

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

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

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

## 3 General procedures

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

3.2 Principal's, as Educational Visits Coordinators (EVCs), will oversee the planning of any events and will seek advice from the SPOC where photographs and videos will be taken.

3.3 Where photographs and videos will involve LAC pupils, adopted pupils, or pupils for whom there are security concerns, principles will liaise with the DSL to determine the steps involved.

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

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

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

3.6 The staff members involved, alongside principals will liaise with the DSL if any LAC pupil, adopted pupil, or a pupil for whom there are security concerns is involved.

3.7 A Trust/ academy-owned digital camera will be used to take photographs and videos of pupils.

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

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

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

3.11 The Trust will not use photographs of:

- Children who have left a Trust academy without the consent of their parents or, where appropriate, the children themselves.
- Staff members who have left the Trust without their consent.

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

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

4 Additional safeguarding procedures

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

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

4.3 Any measures required will be determined between the DSL, social worker, carers and adoptive parents with a view to minimising any impact on the pupil's day-to-day life. The measures implemented will be one of the following:

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

## 5 General use of digital cameras

5.1 Members of staff may be provided with a camera to record and maintain pictorial evidence of the lessons, behaviour, activities and events related to their pupils.

5.2 Photos may only be taken for educational purposes and in "Trust or educational provision settings" as mentioned above.

5.3 The use of personal cameras, mobile phone cameras or other recording equipment is prohibited on Trust premises at all times.

5.4 The Trust-owned cameras are located in cabinets. Members of staff are responsible for making sure that the camera is locked away after use in the filing cabinet at the end of the day.

5.5 Each camera will be clearly numbered/labelled or identified as belonging to the academy/member of staff.

5.6 Members of staff are not allowed to bring in personal cameras without prior permission. If personal cameras are allowed to be brought in due to a specialist requirement or defective equipment, the memory card should be shown to be empty, and images downloaded to the Trust's server.

5.7 Members of staff are not allowed to take Trust cameras or memory cards home.

5.8 Cameras are not permitted to be taken into the toilet/or swimming pool/changing area. If necessary (e.g. photographs of pupils washing their hands), then prior permission needs to be sought from principals. Staff members are required to be supervised while carrying out this activity.

5.9 Staff or other adults are not permitted to take photographs of pupils in vulnerable circumstances, such as when they are upset or inappropriately dressed.

5.10 Members of staff and the Trust community are required to report inappropriate use of digital cameras and images to principles. If it is found that any incidents raise child protection concerns, immediate action will be taken in consultation with the DSL.

## 6 Other Trust-owned devices

6.1 Where Trust-owned devices other than digital cameras are used, images and videos will be provided to the academy at the earliest opportunity and then removed from the devices.

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

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

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

## 7 Storage and retention

7.1 As per the GDPR and the DPA 2018, images obtained by the Trust/academies will not be kept for longer than necessary; retention periods for the different types of personal data are outlined in the Trust's Record Management Policy.

7.2 Hard copies of photos and video recordings held by the Trust/academies will be annotated with the date on which they were taken and will be stored in the academy offices. They will not be used other than for their original purpose, unless permission is sought from principles and parents of the pupils involved and the SPOC has been consulted.

7.3 Where a parent or pupil has withdrawn their consent, any related imagery and videos involving their child/the pupil will be removed from the Trust/academies drive immediately.

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

7.5 Where a pupil's security risk has changed, DSLs will inform principles immediately. If required, any related imagery and videos involving the pupil will be removed from the Trust/academy's drive immediately. Hard copies will be removed by returning them to the parent/pupil or by shredding, as appropriate.

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

7.7 Images taken on the camera must be downloaded as soon as possible on to an academy computer/laptop, ideally once a week.

7.8 Members of staff are responsible for ensuring that images are safely stored, particularly on memory sticks and hard drives. They must take reasonable measures to ensure that they do not come into the possession of unauthorised persons.

7.9 No digital image will be altered or enhanced in any way by any member of staff, unless given prior permission by their principle to do so.

7.10 Staff members are responsible for ensuring that edited images do not mislead or misrepresent. They must not edit images which result in their subject being vulnerable to embarrassment, teasing, bullying or abuse.

7.11 If the memory card for individual academy cameras needs to be replaced, then the replaced memory card will be destroyed to ensure that no images can be recovered.

7.12 Members of staff must remember that, even when images are physically deleted from a camera or memory card, the camera or the memory card must be appropriately disposed of to ensure that no imprint remains.

## 8 Appropriate use of images under the GDPR and the DPA 2018

8.1 Photographs are used by the Trust/academies for many reasons and the different uses for the same image should be considered separately, as each photograph and use will potentially have different conditions for processing.

Photographs used for marketing purposes

8.2 Photographs will not be used for marketing purposes unless the Trust/academy has specific informed consent for the images and the images are only used in line with the consent provided.

Photographs in the Trust environment relating to education

8.3 These photographs may be essential for performing the public task of the Trust/academy, but once the pupil has left an academy this argument is insufficient. If the Trust/academy wishes to display the image beyond the

pupil's time at a Trust academy, we will obtain the pupil's permission. If permission is not granted, the image will be removed.

8.4 When gaining consent, including when initially taking the photograph or when the purpose of the image has changed, the pupil, or where appropriate their parents, will be informed of the retention period pertaining to the use of the image. If the image is still on display after the retention period stated in the privacy notice used to gain consent, the academy will be in breach of data protection sharing of images.

8.5 All images taken by Trust members of staff or volunteers remain the property of the Trust.

8.6 Images must not be shared with anyone outside the Trust or held for private use.

8.7 No digital image will be uploaded onto any internet/intranet system without the express permission of the child's parent/carer.

8.8 Images may under no circumstances be emailed or shared via private e-mail accounts unless a parent has asked for a photo of their child to be sent to them.

8.9 Unless specific prior consent has been obtained, members of staff and volunteers must not post academy images on personal pages of social networking sites or other websites.

## 9 Use of a professional photographer

9.1 If the Trust decides to use a professional photographer for official Trust photos and events, the principal or head of school will:

- Provide a clear brief for the photographer about what is considered appropriate, in terms of both content and behaviour.
- Issue the photographer with identification, which must be worn at all times.
- Let pupils and parents know that a photographer will be in attendance at an event and ensure they have previously provided consent to both the taking and publication of videos and/or photographs.
- Not allow unsupervised access to pupils or one-to-one photo sessions at events.
- Communicate to the photographer that the material may only be used for the Trust/academy's own purposes and that permission has not been given to use the photographs for any other purpose.
- Ensure that the photographer will comply with the requirements set out in the GDPR and the DPA 2018.

- Ensure that if another individual, such as a parent or governor, is nominated to be the photographer, they are clear that the images and/or videos are not used for anything other than the purpose indicated by the Trust/academy.

## 10 Permissible photography and videos during Trust/academy events

10.1 If the Trust permits parents to take photographs or videos during a Trust/academy event, parents will:

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