Data Protection Policy

Version	Author	Dated	Status	Details
1	Compliance Officer	23.05.2018	Approved by Trustees	
2	Compliance Officer	25.05.2021	Approved by Trustees	
3				

Aims

Elevate Multi Academy Trust (Elevate) aims to ensure that all personal data collected about staff, children, parents, Trustees, governors, visitors and other individuals is collected, stored and processed in accordance with the UK data protection law

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

Legislation and Guidance

This policy meets the requirements of the:

UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020

Data Protection Act 2018 (DPA 2018)

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

Schools that use biometric data insert:

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

Schools that use CCTV insert:

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

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

Definitions

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

Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data Subject	The identified or identifiable individual whose personal data is held or processed.
Data Controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data Processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

The Data Controller

Elevate and its Academies processes personal data relating to parents, children, staff, Trustees, governors, visitors and others, and therefore is a data controller.

Elevate is registered with the ICO and will renew this registration annually or as otherwise legally required.

Roles and Responsibilities

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

The Board of Trustees, Local Governing Body

The Trustees have overall responsibility for ensuring that Elevate complies with all relevant data protection obligations. This responsibility may be delegated to the Local Governing Body.

Data Protection Officer

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

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

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

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

Our DPO is: Dianne Mousley and is contactable via d.mousley@elevatemat.org.
Elevate Multi Academy Trust, Inspiration Way, Topcliffe Road, Thirsk, North Yorkshire. YO7 1ST

Head teacher

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

All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy;
- Informing Elevate and its Academies of any changes to their personal data, such as a change of address;

- Contacting the DPO in the following circumstances:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure;
  - If they have any concerns that this policy is not being followed;
  - If they are unsure whether or not they have a lawful basis to use personal data in a particular way;
  - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK;
  - 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.

Data Protection Principles

The UK GDPR is based on data protection principles that Elevate and its Academies must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes;
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed;
- Accurate and, where necessary, kept up to date;
- Kept for no longer than is necessary for the purposes for which it is processed;
- Processed in a way that ensures it is appropriately secure.

This policy sets out how Elevate and its Academies aims to comply with these principles.

Collecting Personal Data

Lawfulness, Fairness and Transparency

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

- The data needs to be processed so that Elevate and its Academies can **fulfil a contract** with the individual, or the individual has asked the Academy to take specific steps before entering into a contract;
- The data needs to be processed so that Elevate and its Academies 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 Elevate and its Academies, 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 Elevate and its Academies or a third party (provided the individual's rights and freedoms are not overridden;)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent.**

For special categories of personal data, Elevate and its Academies will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a child) has given **explicit consent;**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law;**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent;

- The data has already been made **manifestly public** by the individual;
- The data needs to be processed for the establishment, exercise or defence of **legal claims;**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation;
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law;
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law;
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest.

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

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

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

Elevate and its Acadeies will always consider the fairness of our data processing. They will ensure they do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

Limitation, Minimisation and Accuracy

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

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

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

Elevate and its Academies will keep data accurate and, where necessary, up-to-date. Inaccurate data will be rectified or erased when appropriate.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Information and Records Management Society's toolkit for schools.

Sharing Personal Data

Elevate and its Academies will not normally share personal data with anyone else, but may do so where:

- There is an issue with a child or parent/carer that puts the safety of their staff at risk;
- They need to liaise with other agencies – they will seek consent as necessary before doing this;
- Their suppliers or contractors need data to enable Elevate and its Academies to provide services to their staff and children – for example, IT companies. When doing this, they will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law;
    - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data they share;
    - Only share data that the supplier or contractor needs to carry out their service.

Elevate and its Academies will also share personal data with law enforcement and government bodies where we are legally required to do so.

Elevate and its Academies may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of their children or staff.

Where Elevate and its Academies transfer personal data internationally they will do so in accordance with UK data protection law.

Subject Access Requests and other Rights of Individuals

Individuals have a right to make a 'subject access request' to gain access to personal information that their Academy 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;
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing;
- The right to lodge a complaint with the ICO or another supervisory authority;
- The source of the data, if not the individual;
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual;
- The safeguards provided if the data is being transferred internationally.

Subject access requests must be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and 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.

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 children at Elevate's Academies may be granted without the express permission of the child. This is not a rule and a child's ability to understand their rights will always be judged on a case-by-case basis.

Responding to Subject Access Requests

When responding to requests Elevate and its Academies:

- 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(or receipt of the additional information needed to confirm identity, where relevant);
- Will provide the information free of charge;
- May tell the individual they will comply within 3 months of receipt of the request, where a request is complex or numerous. They will inform the individual of this within 1 month, and explain why the extension is necessary.

Elevate and its Academies will not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the child 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;
- Would include another person's personal data that Elevate and its Academies cannot reasonably anonymise, and they do not have the other person's consent and it would be unreasonable to proceed without it;
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts.

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

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

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 Elevate and its Academies are collecting their data about how they use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time;
- Ask Elevate and its Academies 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;
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests;
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement);
- Be notified of a data breach (in certain circumstances);
- Make a complaint to 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.

CCTV

Some of Elevate's Academies use CCTV in various locations around their Academy site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

Elevate and its Academies do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to The Head Teacher.

Photographs and Videos

As part of Elevate's and its Academies activities, they may take photographs and record images of individuals within their Academies.

Elevate and its Academies will obtain written consent from staff and parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. They will clearly explain how the photograph and/or video will be used to staff, the parent/carer and child.

Any photographs and videos taken by parents/carers at Academy events for their own personal use are not covered by data protection legislation. However, The Academy will ask that photos or videos with other children are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

When the Academy takes photographs and videos uses may include:

- Within Academies on notice boards and in newsletters, brochures, reports, prospectus, etc.
- Outside of Elevate and its Academies by external agencies such as the school photographer, newspapers, campaigns;
- Online on Elevate and its Academy's websites or social media pages.

Consent can be refused or withdrawn at any time. If consent is withdrawn, the Academies will delete the photograph or video and not distribute it further.

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

Data Protection by Design and Default

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

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge;
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law:
- Completing privacy impact assessments where Elevate and their Academies 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; Elevate and its Academies will also keep a record of attendance;

- Regularly conducting reviews and audits to test our privacy measures and make sure Elevate and its Academies are compliant;
- Maintaining records of Elevate and its Academies processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of the DPO and all information they are required to share about how they use and process their personal data (via our privacy notices);
    - For all personal data that they hold, maintaining an internal record of the type of data, data subject, how and why they are using the data, any third-party recipients, how and why they are storing the data, retention periods and how they are keeping the data secure.

Data Security and Storage of Records

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

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use;
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access;
- Where personal information needs to be taken off site, staff must ensure it is kept safe and secure at all times;
- Passwords that are at least 10 characters long containing letters and numbers are used to access Academy computers, laptops and other electronic devices. Staff and children are reminded should not reuse passwords from other sites;
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices;
- Staff, children, Trustees or governors who store personal information on their personal devices are expected to follow the same security procedures as for Academy-owned equipment. See online safety policy/ICT policy/acceptable use agreement/policy on acceptable use;
- Where Elevate and its Academies need to share personal data with a third party, they carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

Disposal of Records

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

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

Personal Data Breaches

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

In the unlikely event of a suspected data breach, Elevate and its Academies will follow the procedure set out in appendix 1.

When appropriate, Elevate and its Academies will report the data breach to the ICO within 72 hours. Such breaches in an Academy context may include, but are not limited to:

- A non-anonymised dataset being published on the Academy's websites which shows the exam results of children eligible for the pupil premium;
- Safeguarding information being made available to an unauthorised person;
- The theft of an Academy laptop containing non-encrypted personal data about children.

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 Elevate or its Academies processes make it necessary.

Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually.

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 head teacher, the Chair of Trustees and the appropriate chair of governors;
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary and the DPO should take external advice when required (eg from IT providers). (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 and the individuals affected using the ICOs self-assessment tool;
- 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 Elevate's computer system;
- 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;
- Where the Academy is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
    - A description, in clear and plain language, of the nature of the personal data breach;
    - The name and contact details of the DPO;
    - A description of the likely consequences of the personal 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 consider, in light of the investigation and any engagement with affected individuals, whether to 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 Elevate's computer system.

- The DPO and head teacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.
- The DPO and head teacher will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches.

Actions to Minimise the Impact of Data Breaches

Elevate and its Academies 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. They 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 support to attempt to recall it from external recipients and remove it from the Academy's email system(retaining a copy of it if required as evidence);
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to 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 endeavor to obtain 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;
- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the Academy should inform any, or all, of its 3 local safeguarding partners.

Other types of breach could include:

- Details of pupil premium interventions for named children being published on the Academy website;
- Non-anonymised pupil exam results or staff pay information being shared with governors;
- An Academy laptop containing non-encrypted sensitive personal data being stolen or hacked;
- The Academy's cashless payment provider being hacked and parents' financial details stolen;
- Hardcopy reports sent to the wrong children or families.