Excalibur Academies Trust

Data Protection

Policy

Date of approval	April 2024
Approved by	Excalibur Audit Committee
Review date	April 2026 unless Legislation depicts a change

Registered Office: Excalibur Academies Trust, Granham Hill, Marlborough SN8 4AX
Registered in England and Wales
Company number: 8146633

Contents

1. Aims and Purpose

Excalibur Academies Trust aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the UK GDPR

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

The Trust will ensure that all stakeholders, including employees, contractors, agents, consultants, or partners who have access to any personal data held by or on behalf of its schools, are fully informed and compliant with their obligation under the legislation.

The Trust collects and uses personal information to carry out its functions. This includes current, past, and potential students, parents/carers, employees, suppliers, customers, service users and others. We collect and use this information to fulfil our legal obligations and comply with governments regulations. Personal data is handled properly, whether stored on paper or electronically, in accordance with the UK General Data Protection Regulations to ensure data protection safeguards.

The Trust considers the lawful and proper handling of personal information crucial for its operations and maintaining trust with stakeholders. This policy outlines how the Trust ensures compliance with Data Protection legislations, including organisational measures and individual responsibilities to uphold Data Protection principles and respect individuals' rights. This is an overarching policy which establishes measures and a monitoring structure for compliance.

2. Legislation and guidance

This policy meets the following requirements:

UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated in 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 UK GDPR and the DfE guidance for Data Protection in Schools

the Protection of Freedoms Act 2012 when referring to the Trust's use of biometric data.

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

In addition, this policy complies with our funding agreements and articles of association.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data, which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Any action on personal data, whether manual or automated, including collection, recording, storage, use, adaption or alteration, disclosure, restriction, retrieval, and deletion.
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.
Pseudonymisation	The processing of Personal Data so that it can no longer be attributed to a specific person.

4. The data controller

Excalibur Academies Trust processes personal data relating to parents/carers, pupils, staff, governors, visitors and others, and therefore is a data controller.

The Trust is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required. Registration Number ZA106446
ICO Certification can be found here

5. Roles and responsibilities

This policy applies to **all staff** employed by the Trust, all volunteers, and all external organisations or individuals working on the Trust's behalf. It is a criminal offence to access personal data for any other reason than school business. Staff who do not comply with this policy may face disciplinary action.

5.1 Board of Trustees

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

5.2 Data Protection Officer

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

They will provide a regular update of their activities to the Audit Committee, a committee of the Board. Where relevant, they will report to the board their advice and recommendations on data protection issues.

All schools have a local data protection lead. Their contact details can be found on school privacy notices. The Trust DPO is the first point of contact for individuals whose data the school processes, and for the ICO.

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

Our DPO is Andrew Twine and is contactable via dpo@excalibur.org.uk

5.3 CEO and Principals / Head Teachers of Trust Academies

Principals / Head Teachers and the CEO act as the representative of the data controller on a day-to-day basis.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting their local data protection lead or 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 European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The UK GDPR is based on six data protection principles for processing personal data that the Trust must comply with. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject **('lawfulness, fairness and transparency')**
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes **('purpose limitation'**)
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('**data minimisation'**)
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay **('accuracy**')
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject **('storage limitation'**)
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures **('integrity and confidentiality')**

7. Collecting personal data

7.1 Lawfulness, fairness, and transparency

The Trust and its schools will collect and process personal data in order to fulfil operational needs and/or to comply with legal requirements. Personal data will be processed where at least one of 6 'lawful bases' (legal reasons) to do so applies as detailed in Article 6(1) of the UK GDPR:

- The data needs to be processed in order to **fulfil a contract** with the individual, or to take steps that the individual has asked to be taken before entering a contract
- Processing is necessary so that the school can **comply with a legal obligation**
- The data needs to be processed to protect the **vital interests** of the individual e.g., to protect someone's life
- Processing is necessary in order to **perform a task in the public interest,** and carry out official functions

- The data needs to be processed for the **legitimate interests** of the school 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** and fully understands that consent can be withdrawn at any time.

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law, as detailed in Article 9 of the UK GDPR:

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

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

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for or in connection with **legal 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 we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not expect or use personal data in ways which have unjustified adverse effects on them.

7.2 Limitation, minimisation, and accuracy

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

When personal data is to be used for a new purpose, information will be provided to the individuals concerned before and, if necessary, new consent will be sought.

Staff must only process personal data where it is necessary in order to do their jobs and any data held must be relevant to the stated purpose and not excessive

Information will only be held for as long as is necessary, in line with the Trust's data retention policy. 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 policy for data retention. Redundant personal data will be destroyed in line with the Trust's procedure for disposal of confidential waste.

8. Sharing personal data

The Trust will not normally share personal or sensitive personal data without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff or others at risk
- There is a need to liaise with other agencies – we will seek consent as necessary before doing this
- Suppliers or contractors need data to enable the Trust to provide services to itsstaff and pupils – for example, IT companies. When doing this, the Trust 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 shared
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with the Trust.

The Trust will also share personal data with law enforcement and government bodies where legally required to do so, or to emergency services and local authorities to help them 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 and with approval from the data controller

9. Subject access requests and other rights of individuals

Data subject rights are:

- The right to be informed that processing is being undertaken
- The right of access to one's personal information
- The right to prevent processing in certain circumstances
- The right to rectify, block or erase information which is regarded as wrong information
- The right to have decisions reviewed where they have been made automatically
- The right to object to receiving marketing information

9.1 Subject access requests

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

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

Subject access requests may be submitted in writing or verbally, either to the Principal school Data Protection Lead or Trust DPO. When the SAR is acknowledged, the following information should be obtained, if not clear from in the initial request:

- 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 their Principal / Head teacher or school Data Protection Lead, who will contact the DPO.

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

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school 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, the Trust

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May need to apply an extension of a further 2 months where a request is complex. The Trust will inform the individual of this within 1 month, and explain why the extension is necessary

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or 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 we cannot anonymise, and we do not have the other person's consent and it would be unreasonable to proceed without its 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
- Would reveal that the child is being or has been abused, or 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 we cannot anonymise, and we 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, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will consider whether the request is repetitive in nature when making this decision.

When the Trust refuses a request, they 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.

All Subject Access Requests received will be recorded for monitoring and reporting purposes.

9.4 Other data protection rights of the individual

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

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

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.
The Trust will review requests from individuals to correct, rectify, block, or erase information they deem inaccurate or causing harm or distress, on a case-by-case basis. The individual will be informed of the decision and reasons behind it. Legal advice will be sought for sensitive or complex cases or unsupported requests.

The Trust will promptly honour requests to stop sending marketing or consultation materials.

10. Parental requests to see the educational record

Excalibur schools are all academies, and as such there is no automatic parental right of access to the educational record of students. Schools will endeavour to provide parents/carers with the information they are requesting. Requests should be made to the Principal / Head teacher detailing the information parents/carers would like to review. Providing the provision of information is not onerous, no charge will be made.

11. Biometric recognition systems

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

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

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners using a PIN number

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

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

Where staff members or other adults use the school'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 school will delete any relevant data already captured.

12. CCTV

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

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

Any enquiries about the CCTV system should be directed to the Principal / Head teacher at the location of the school where the CCTV is installed.

13. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

Primary Schools

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

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other

pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

Secondary Schools

We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing, and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we do not need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

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

Where the school takes photographs and videos, uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, reports to Governors or Directors.
- Outside of school such as the school prospectus, or by external agencies such as the school photographer, newspapers, local media, campaigns, and recruitment websites.
- Online on our school or Trust websites, social media pages or blogs.

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

14. Data protection by design and default

The Trust 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 (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant

- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school 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. Taking specific care in respect of services obtained via 'the cloud'

The Trust, as data controller, as far as is reasonably practical will ensure that contractors and subcontractors comply with Data Protection legislation. Contractors cannot subcontract data processing without the Trust's written permission. Staff will monitor third-party data processing for compliance through use of the ROPA. When parties are joint data controllers, responsibilities must be clearly outlined. Contractors must confirm compliance with Data Protection legislation to the same standard as the Trust and any security incidents or concerns must be reported immediately. Breach of Data Protection is considered a breach of contract.

15. Data security and storage of records

The Trust will implement appropriate technical and organisational security measures to 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 secure when not in use
- Staff must not use or leave computers, memory devices or papers where there is a significant risk that they may be viewed or taken by unauthorised persons: they should not be viewed in public, and they must never be left in view in a car, where the risk of theft is greatly increased
- The Trust uses a range of measures to protect personal data stored electronically, including cloud-based storage, file encryption, anti-virus and security software, user passwords, audit trails and back-up systems;
- Papers containing 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
- Strong passwords containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Personal data must not be held on any unencrypted devices and appropriate user-profile password controls must be in place
- Staff are instructed not to use memory sticks or unsecure portable devices to store personal data and must not use personal accounts for email and file sharing of personal data.

- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment. (See our acceptable use policy)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

16. 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, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school'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 Trust will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 2. All breaches, however minor, should be reported to the Principal / Head teacher or Data Protection Lead and when appropriate, the breach will be reported to the ICO within 72 hours as per UK GDPR guidelines.

Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being shared with unauthorised individuals or published on the school website
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

18. Training

On joining the Trust, employees are required to undertake training on Data Protection and ICT Security as part of their induction.

The Trust will ensure that:

- All staff understand and fulfil their responsibility for good data protection practices
- Staff handling personal information receive proper training and supervision
- Prompt and courteous assistance is provided for inquiries about handling personal information
- Regular assessment and evaluation of methods and performance in handling personal information are conducted
- Employees are informed of the necessary actions in case of a data breach

The Data Protection Officer maintains the on-going programme of training and awareness to preserve a high level of understanding of Data Protection and security among all staff and to communicate any legal or policy changes that occur.

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

Data Protection audits are regularly carried out by internal audit (external audits may be commissioned if required) in order to monitor compliance with the GDPR and this policy.

This policy will be reviewed **every 2 years** (or sooner if there are changes to the law within that time) and shared with the Audit Committee for approval.

Data Protection Regulation will be dealt with in accordance with this Policy. Complaints will be fully dealt with after a formal review.

Individuals have a right to request that the Information Commissioner make an assessment of compliance of particular circumstances with the General Data Protection Regulation. If individuals are not happy about how we have handled their information, they can contact the ICO via:

Customer Contact

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Alternatively via their website - www.ico.gov.uk or contact them by phone on 0303 123 1113

The Trust will respond promptly and fully to any request for information about data protection compliance made by the Information Commissioner.

The Trust will comply with any Information Commissioner Information Notice (to provide answers and information to the Commissioner) or Enforcement Notice (for failure to provide answers or information or for a breach of the Act) sent to the Trust by the Information Commissioner. The Commissioner can also carry out audits, prosecute individuals and organisations and report concerns to parliament.

20. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- HR Manual – section on Data Protection
- Privacy Notices
- Acceptable Use Policy

Appendix 1

Excalibur Academies Trust Data Security Protocols for All Staff Part of the GDPR Policy

DO:

✓ **Remember that data protection laws DO NOT stop you from reporting safeguarding concerns**

- You must still report to the relevant people where you're concerned about a child or the behaviour of an adult/member of staff. You do not need anyone's consent to do this

✓ **Only collect the information you need**

- When you're requesting information (for example, via consent forms, admissions forms or surveys) ask yourself "Do I really need this? What will I actually use it for?"
- If you don't need it, or only want it "just in case", don't collect it
- If you've already collected personal information that you don't need, delete it

✓ **Keep personal data anonymous, if possible**

- For example, if you're emailing a colleague about accommodating a pupil's religion, or about managing a pupil's medical condition, don't name the child if you don't need to
- This is particularly important with photographs for external use – if you have an image of a child, don't attach their name to it unless you have explicit consent to do so and ensure that you have checked the appropriate consent has been given before sharing the photograph

✓ **Think before you put information up on the wall**

- If your display is an essential part of teaching and learning, or helps to keep pupils safe, it's fine. This might include medical information, or a list of parents' evening appointments. But only have information up for as long as you need it, not indefinitely, and be mindful of where the information is being put – e.g. avoid medical information being able to be read through an outside window.
- If your display is non-essential, promotional, or there might be a safeguarding risk, either ask the pupil or parents for consent first or just don't display it

✓ **Take care if you're taking personal information home with you**

- Sign documents containing personal data out and in from the school office
- Keep physical documents in a secure, closed folder along with your contact details in case the folder is lost
- Store the documents in a safe place at home – don't leave them in your car or at a friend's house

✓ **Practice good ICT security (Information & Communications Technology) (Information & Communications Technology) security**

- Passwords should be at least 7 characters, with upper and lower-case letters and special characters

- Password-protect documents and email attachments that include personal data and try to avoid including personal data in the main body of an email.
- Always double-check that you're emailing personal data to the correct person, who is authorised to see it
- Use 'bcc' when you're emailing a group of people who don't have email addresses for everyone else in the group, e.g. parents or volunteers

DON'T:

✘ **Leave personal data out on your desk**

- Keep your desk clear, so people cannot see information about others accidentally. The same goes for personal data written on post-it notes, on top of the printer, or on an unattended computer screen

✘ **Leave your PC 'logged-in' whilst unattended**

✘ **Take any sensitive personal information home with you**

- If the information is confidential, sensitive or risky, it's best to leave it on the school site or computer system, where there are security measures and processes in place

✘ **Store school data on personal device**

✘ **Use memory sticks**

- If you really need to use one, make sure it is encrypted (speak to the IT Team)

If something doesn't seem right, talk to the schools GDPR Data Lead or a member of the Trust central Data Team for advice (dpo@excalibur.org.uk).

Report to the school GDPR Data Lead immediately if you think personal data has been lost, stolen, or wrongly disclosed.

This is so we can quickly take steps to mitigate the impact of the breach.

You should also speak to the Trust Central Data Team if:

- You have any concerns at all about keeping personal data safe
- You're introducing a new software, process or policy that involves using personal data
- Anyone asks you to see the data that we have about them. This is called a 'subject access request', and the person will be entitled to this information

Appendix 2: 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 their Data Protection Lead or Principal / Head teacher who will immediately inform the Trust Data Protection Officer (DPO)
- The Trust DPO will investigate the report and if necessary, refer to the ICO 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 assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g., emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of Pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- If deemed to be a reportable breach the DPO will alert the CEO and relevant Directors. If the breach relates to a school, The DPO will inform the principal, who will inform the Chair of the Academy Committee.
- 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.
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- 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 by the DPO on the Trust's OneDrive.

- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks, or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- The DPO and Principal will meet to review what happened and how it can be stopped from happening again.

The Trust will take actions to prevent similar data breaches recurring.

The DPO reports regularly to the Audit Committee including details of breaches and mitigation actions taken.

Appendix 3: Subject Access Request Template

Individuals requesting details of information held are requested to use the format below and send to the Principal / Head Teacher, GDPR Data Lead or DPO.

All requests will be dealt with promptly and we will comply with the requirements of the GDPR to respond within one month. However not all email addresses are monitored during school holidays. If the request is urgent and made during the school holidays, we recommend you try alternative contact if no acknowledgement is received within 3 days.

Dear Sir

Re: Subject Access Request

Please provide me with the information about me that I am entitled to under the UK General Data Protection Regulation. This is so I can be aware of the information you are processing about me and verify the lawfulness of the processing.

Here is the necessary information:

Name	
Relationship with the school	Please select: Pupil / parent / employee / governor / volunteer Other (please specify):
Correspondence address	
Contact number	
Email address	
Details of the information requested	Please provide me with: *Insert details of the information you want that will help us to locate the specific information. Please be as precise as possible, for example:* • *Your personnel file* • *Your child's medical records* • *Your child's behavior record, held by [insert class teacher]* • *Emails between 'A' and 'B' between [date]*

If you need any more information from me, please let me know as soon as possible.

Yours sincerely,