

Fylde Coast Academy Trust

# Data Protection Policy

including Personal Data Breach Response and Employee Responsibilities

**Policy Owner:** Pete Montgomery, FCAT Lead in Data & IT and Data Protection Officer

**Reviewed in:** April 2022

**Next Review date:** August 2023

## Aims

Our Multi Academy Trust (FCAT) and member academies aim to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with 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.

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

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

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

## Definitions

Term	Definition
<b>Personal Data</b>	<p>Any information relating to an identified, or identifiable, individual.</p> <p>This may include the individual's:</p> <ul style="list-style-type: none"><li>• Name (including initials)</li><li>• Identification number</li><li>• Location data</li><li>• Online identifier, such as a username</li></ul>

	It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
<b>Special categories of personal data</b>	<p>Personal data which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none"> <li>● Racial or ethnic origin</li> <li>● Political opinions</li> <li>● Religious or philosophical beliefs</li> <li>● Trade union membership</li> <li>● Genetics</li> <li>● Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes</li> <li>● Health – physical or mental</li> <li>● Sex life or sexual orientation</li> </ul>
<b>Processing</b>	<p>Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.</p> <p>Processing can be automated or manual.</p>
<b>Data subject</b>	The identified or identifiable individual whose personal data is held or processed.
<b>Data controller</b>	A person or organisation that determines the purposes and the means of processing of personal data.
<b>Data processor</b>	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.

<b>Personal data breach</b>	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
<b>“The Trust”; or “Trust”</b>	This includes Fylde Coast Academy Trust, Central Services and all member academies

## 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 data controller 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 the Trust, and to external organisations or individuals working on our behalf. All employees have a contractual responsibility and legal obligation to ensure that personal data and information is processed for students and staff in line with this policy and the UK GDPR. Failure to do so or to follow the employee responsibilities outlined in this policy may result in disciplinary action being taken in accordance with the Trust's Disciplinary Policy.

## Board of Trustees

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

## 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 board of Trustees and, where relevant, report to the board their advice and recommendations on data protection issues.

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

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

Our DPO is Mr. P Montgomery and is contactable via [dpo@fcat.org.uk](mailto:dpo@fcat.org.uk)

## Headteacher

In each FCAT academy, the Headteacher 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, they should ensure that they read through and adhere to the staff responsibilities set out in appendix 2
- Informing the Trust of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  - If they have any concerns that this policy is not being followed
  - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
  - If they need to rely on or capture consent, draft or update 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 potential 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

## Staff Leavers

When a member of staff leaves their employment with the Trust we will remove their access permissions to systems containing personal information by suspending or deleting their user accounts.

# Data Protection Principles

The 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 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 the Trust aims to comply with these principles.

## Collecting Personal Data

### 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 data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual or another person i.e. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can **perform a task in the public interest or exercise its official authority**
- The data needs to be processed for the **legitimate interests** of the school (where the processing is not for any tasks the school performs as a public authority) 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, we 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 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 reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

We provide more detailed information for individuals about how the Trust uses any personal data that we hold about them in our Privacy Notices which are available on our websites.

Some of the Schedule 1 conditions for processing special category and criminal offence data require us to have an Appropriate Policy Document in place, setting out and explaining our procedures for securing compliance with the principles in Article 5 and policies regarding the retention and erasure of such personal data. A copy is available upon request.

## Limitation, minimisation and accuracy

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

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

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

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

In addition, 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 school's record retention schedule.

## 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 this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, 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.

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 internationally, we will do so in accordance with UK data protection law.

## Subject Access Requests and Rights of Individuals

### Subject Access Requests

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

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

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing, either by letter or email, 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 who will advise the academy on how to respond appropriately to the request in accordance with the legislation.

### 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 in the Trust 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 in the Trust 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.

## Responding to subject access requests

When responding to requests, we:

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

We 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 can't reasonably anonymise, and we don't 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

Guidance from the Information Commissioner's Office advises that we should make reasonable efforts to find and retrieve the requested information. This guidance also states that we are not required to conduct searches that would be unreasonable or disproportionate to the importance of providing access to the information. This means that we may refuse to use or we may change search criteria if we determine searches would be unreasonable.

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 take into account whether the request is repetitive in nature when making this decision.

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

## 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 Collecting Personal Data), 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 (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.

## Parental Requests to see the Educational Record

Parents, or those with parental responsibility, can make a request to access their child's educational record (which includes most information about a pupil). We will aim to provide access to within 15 school days of receipt of a written request.

Individuals with parental responsibility do not have an automatic right of access to the personal data belonging to a child. Decisions about sharing the personal data of children without consent will be assessed on a case by case basis. Please note that there is no parent/carer independent right of access to a pupils' school records; as this right contained within the Education Act 2005 applies to maintained schools and does not apply to academies or free schools

## Biometric Recognition Systems

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

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

Parents/carers and pupils have the right to choose not to use an academy'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 academy'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 academy'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.

## CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will follow the ICO's guidance for the use of CCTV, and comply with data protection principles.

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 initially be directed to [dpo@fcat.org.uk](mailto:dpo@fcat.org.uk)

## Photographs and Videos

As part of the Trust's activities, we may take photographs and record images of individuals within the Trust.

We will obtain written consent from parents/carers, or students considered old enough (at least aged 13), 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 don't 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 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.

Uses may include:

- Within the Trust on notice boards and in FCAT magazines, brochures, newsletters, etc.
- Outside of the Trust by external agencies such as the school photographer, newspapers, campaigns
- Online on the Trust's websites or social media pages

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

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

See our Safeguarding and Child Protection Policy for more information on our use of photographs and videos.

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

## 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. Employee responsibilities to protect personal data are outlined at appendix 2.

## 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 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.

## 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 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches may include, but are not limited to:

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

## Training and Resources

All staff and governors are provided with data protection training as part of their induction process.

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

The Trust will make available to its academies, any resources or information that may be helpful and assist with their responsibilities in implementing this policy.

## Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and approved by the Board of Trustees.

## Linked Policies

The document creates a policy environment in which all other policies operate.

# Appendix 1: Personal data breach procedure

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

- 1) On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO.
- 2) 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:
  - a) Lost
  - b) Stolen
  - c) Destroyed
  - d) Altered
  - e) Disclosed or made available where it should not have been
  - f) Made available to unauthorised people
- 3) The DPO will, as necessary, alert the Head Teacher.
- 4) The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure).
- 5) The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- 6) 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:
  - a) Loss of control over their data
  - b) Discrimination
  - c) Identify theft or fraud
  - d) Financial loss
  - e) Unauthorised reversal of pseudonymisation (for example, key-coding)
  - f) Damage to reputation
  - g) Loss of confidentiality
  - h) Any other significant economic or social disadvantage to the individual(s) concerned
- 7) If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- 8) The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the Trust's computer system.



- 9) 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) A description of the nature of the personal data breach including, where possible:
    - i) The categories and approximate number of individuals concerned
    - ii) The categories and approximate number of personal data records concerned
  - b) The name and contact details of the DPO
  - c) A description of the likely consequences of the personal data breach
  - d) 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
- 10) 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
- 11) 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:
  - a) The name and contact details of the DPO
  - b) A description of the likely consequences of the personal data breach
  - c) 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
- 12) 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
- 13) The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - a) Facts and cause
  - b) Effects
  - c) Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- 14) Records of all breaches will be stored on the Trust's computer system.
- 15) The DPO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.
- 16) The DPO and Trust senior leadership team 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

We set out the staff responsibilities in appendix 2 to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive

information. We will review the effectiveness of these responsibilities and amend them as necessary after any data breach

# Appendix 2: Employee Responsibilities

## Data Protection: Safeguarding Personal Data

Data Protection laws introduced and updated in 2018 emphasise safeguarding personal and sensitive data. These include greater accountability and enhanced rules for aspects of how personal data is collected, stored, shared, used and disposed of.

Individuals also now have greater rights on what and how their personal data is processed.

Personal data is any information that can identify an individual e.g. name, NI number, student number, address, date of birth

Special categories of data are personal data which the GDPR says is more sensitive, and therefore requires a higher level of protection. This includes information about an individual's race, ethnicity, medical condition/information, their membership of a trade union amongst others.

FCAT DPO – Pete Montgomery – [DPO@fcats.org.uk](mailto:DPO@fcats.org.uk)

## Employee Responsibilities

All staff are responsible for safeguarding personal information and must ensure that personal data is processed for specific and justified purposes. Sometimes this means individuals must give their consent before personal data can be processed.

You must always be careful and thoughtful when working with information that could be used to identify or be linked to a pupil, parent or member of staff

You must consider whether you, or the person requesting it, need(s) personal data to achieve your/their objective or task

You must only process the minimum amount of personal data required and have a justified reason, as outlined in the privacy notice to perform a task

You must take all reasonable steps to safeguard the personal data that you access and use.

- Especially when handling special categories of personal data such as pupil premium status, medical conditions or identification (as this can reveal race and ethnicity), extra precautions to safeguard must be taken with this data.
- Consider who needs to know this information to perform their role/task before sharing, limit the data available to them to be only the essential information to carry out the task/role
- Consider where you hold any conversations and if you can be overheard by others

- Consider how you store and keep the data protected, who has access and how readily available this is to others

You must only disclose or share personal data when you have an individuals' consent or where there is a legal basis for doing so (as outlined in our privacy notices)

Before disclosing or sharing personal data, you must ensure that you have completed the following, otherwise the may be considered a data breach:

- verified the identity and contact details of the individual making the request; and
- confirmed that they are entitled to access the information as outlined in one of our privacy notices; or gained the appropriate consent from the individual who is the subject of the disclosure

You must only process data that you have a legal basis for doing so (or have an individuals consent where applicable within our privacy notice), you should seek advice from the DPO if you need advice or clarity on the legal basis

If you are unsure whether to disclose or the legal basis for processing any personal data you should seek advice from the DPO before taking any action

You must report a suspected data breach to the Head Teacher and DPO within 48 hours

## Personal data via Emails

Wherever possible, emailing of personal or special categories of data should be avoided, consider if this could be done via Google Drive instead

If sharing or emailing, ensure you are sending the personal data to the intended individuals by double checking the recipient list before sending

If emailing any special categories of personal data, extra precautions must be taken:

- attachments must be password protected
- the password must not be included in the original email but should be sent separately or use a password that is already known to the recipients (Microsoft Office programs such as Word & Excel provide an easy to use "encrypt with password" feature)
- you should be stringent with who this information is sent to, ensure that only those that require to see the special categories of data have a right in order to carry out their role/a task

Do not forward email chains without checking the entire content for personal or sensitive information, if the recipients do not need to see the information for their role then the chain emails should be removed before forwarding or a new email issued

Personal email addresses must not be used for any work-related correspondence

You should not email any personal data (or work data) to any personal email addresses under any circumstances, all email correspondence should be via the Trust/academy email accounts

Steps should be taken to protect the individual when emailing personal data or attachments containing it:

- You must protect the information as far as reasonably possible when choosing an email subject i.e. 'JS – statement' NOT 'John Smith Allegation'
- You must ensure when emailing personal data attachments, the file names attached to emails should not contain more than is necessary in terms of personal data such as: 'Letter – JS – Date' NOT 'JohnSmithExclusionfor....'

## IT use and storing data electronically (Shared drives, folders and files)

You must always lock your computer or laptop if left unattended for any period of time ('Windows key' and 'L' quickly locks your computer)

Ensure that access / Login ID's (usernames and password details) for secure systems are kept secure and not shared

Before saving or copying any documents containing personal data to a shared folder or area of the school network, such as a staff shared drive, you must ensure that all users who could access the files have a legitimate reason to access the information. Access permissions must be approved and any changes to these reviewed by the Headteacher who will then instruct the Network Engineer or Senior IT Technician to facilitate access.

If personal data is included in any part of a Google Drive file or folder which is shared, access must only be granted to Trust domain email addresses. Access to and the content of shared drives are the responsibility of, and must be controlled by, the owner of the file or folder

If you intend to add a document containing personal and/or special categories or data to a shared location, you are responsible for checking that no unauthorised user will have access to the information once it is shared

Personal or special categories of personal data must not be uploaded or shared on social media, online forums or any other online platform unless you have obtained proper consent to do so.

Personal data must not be stored electronically on any device other than a Trust laptop, tablet or computer under any circumstances. This includes storing any data on the following:

- An unencrypted device e.g. hard drives of personal computers

- USB pen drives and other unencrypted removable media

## Trust/Academy equipment and software

Any personal IT equipment used e.g. mobile phones, tablets, home laptops, must have access restrictions enabled such as passcode and fingerprint recognition to unlock devices.

Before using any service, app or software that requires sharing personal data (i.e. pupil names etc) you must:

- check with the Trust Network Manager or the DPO that it has appropriate data protection security measures in place and are to safe use
- ensure a completed third-party processor approval form, available from IT Technicians and the Trust Network Manager, giving details of the service has been completed and approved by the Trust Network Manager (or FCAT Lead in Data & IT their absence)

## Other general responsibilities

Personal data should be stored electronically as much as is reasonably possible:

- Once uploaded or no longer needed, paper documents containing personal data must be shredded or placed in the confidential waste bin provided within the academy
- Paper records that are required and retained must be kept in a locked filing cabinet and the key locked away

You should maintain a clear desk area by removing any confidential or personal data information from your workspace and locking this away securely if you leave the immediate desk area for any period of time

You should ensure that your screen and any personal data cannot be overlooked by others, speak to your line manager in the first instance to address this

Personal data in electronic or paper form, should not be taken off site (personal files should not be taken or accessed from home under any circumstances). In some roles, e.g., teachers, we know this cannot be avoided. If the Head Teacher does determine that as part of your role this is required, the following must be undertaken:

- the data must not be left in an environment where access cannot be controlled
- you must take necessary steps to ensure that the information is kept safe, secure and hidden at all times
- any files (staff or student) which are taken off site and contain personal data, must be signed in and out using the academy personal records register.



## Version Control

Version	Author	Date	Changes
0.1	P Montgomery	2018	First Draft
2.0	P Montgomery	13 April 2022	Reviewed and updated. Added details about Appropriate Policy Document. Added reference to Privacy Notices. Updated some wording for clarity.