Data Protection Policy
Fairfax Multi-Academy Trust

Document Owner:	**Robert Fitzgerald**
Ratified By:	**Audit and Risk Committee (Sub-committee of Trust Board)**
Date Ratified:	**June 2025**
Review Date:	**September 2026**

Contents

Appendices

1 Policy statement

1.1 Everyone has rights with regard to the way in which their **personal data** is handled. During the course of our activities as a Trust we will collect, store and **process personal data** about our pupils, **workforce**, parents and others. This makes us a **data controller** in relation to that **personal data**.

1.2 We are committed to the protection of all **personal data** and **special category personal data** for which we are the **data controller**.

1.3 The law imposes significant fines for failing to lawfully **process** and safeguard **personal data** and failure to comply with this policy may result in those fines being applied.

1.4 All members of our **workforce** must comply with this policy when **processing personal data** on our behalf. Any breach of this policy may result in disciplinary or other action.

2 About this policy

2.1 The types of **personal data** that we may be required to handle include information about pupils, parents, our **workforce**, and others that we deal with. The **personal data** which we hold is subject to certain legal safeguards specified in the U K General Data Protection Regulation ('**UK GDPR**'), the Data Protection Act 2018, and other regulations (together '**Data Protection Legislation**').

2.2 This policy and any other documents referred to in it set out the basis on which we will **process** any **personal data** we collect from **data subjects**, or that is provided to us by **data subjects** or other sources.

2.3 This policy does not form part of any employee's contract of employment and may be amended at any time.

2.4 This policy sets out rules on data protection and the legal conditions that must be satisfied when we process **personal data**.

3 Definition of data protection terms

3.1 All defined terms in this policy are indicated in **bold** text, and a list of definitions is included in the Annex to this policy.

4 Data Protection Officer

4.1 Fairfax Multi-Academy Trust is required to appoint a Data Protection Officer ("**DPO**"). Our DPO can be contacted at dpo@fmat.co.uk

4.2 The DPO is responsible for ensuring compliance with the Data Protection Legislation and with this policy. Any questions about the

operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO.

4.3 The DPO is also the central point of contact for all to matters of data protection.

5 Data protection principles

5.1 Anyone **processing personal data** must comply with the data protection principles. These provide that **personal data** must be:

5.1.1 **Processed** fairly and lawfully and transparently in relation to the **data subject**;

5.1.2 **Processed** for specified, lawful purposes and in a way which is not incompatible with those purposes;

5.1.3 Adequate, relevant and not excessive for the purpose;

5.1.4 Accurate and up to date;

5.1.5 Not kept for any longer than is necessary for the purpose and securely destroyed, see 13.3.3;

5.1.6 **Processed** securely using appropriate technical and organisational measures.

5.2 **Personal Data** must also:

5.2.1 be **processed** in line with **data subjects'** rights;

5.2.2 not be transferred to people or organisations situated in other countries without adequate protection.

5.3 We will comply with these principles in relation to any **processing** of **personal data** by the Trust.

6 Fair and lawful processing

6.1 Data Protection Legislation is not intended to prevent the **processing** of **personal data**, but to ensure that it is done fairly and without adversely affecting the rights of the **data subject**.

6.2 For **personal data** to be **processed** fairly, **data subjects** must be made aware:

6.2.1 that the **personal data** is being **processed**;

6.2.2 why the **personal data** is being **processed**;

6.2.3 what the lawful basis is for that **processing** (see below);

6.2.4 whether the **personal data** will be shared, and if so with whom;

6.2.5 the period for which the **personal data** will be held;

6.2.6 the existence of the **data subject's** rights in relation to the **processing** of that **personal data**; and

6.2.7 the right of the **data subject** to raise a complaint with the Information Commissioner's Office in relation to any **processing**.

6.3 We will only obtain such **personal data** as is necessary and relevant to the purpose for which it was gathered, and will ensure that we have a lawful basis for any **processing**.

6.4 For **personal data** to be **processed** lawfully, it must be **processed** on the basis of one of the legal grounds set out in the Data Protection Legislation. We will normally **process personal data** under the following legal grounds:

6.4.1 where the **processing** is necessary for the performance of a contract between us and the **data subject**, such as an employment contract;

6.4.2 where the **processing** is necessary to comply with a legal obligation that we are subject to, e.g. the Education Act 2011;

6.4.3 where the law otherwise allows us to **process** the **personal data** or we are carrying out a task in the public interest; and

6.4.4 where none of the above apply we will seek the consent of the **data subject** to the **processing** of their **personal data.**

6.5 When **special category personal data** is being processed an additional legal ground must apply to that processing. We will normally only **process special category personal data** under following legal grounds:

6.5.1 where the **processing** is necessary for employment law purposes, for example in relation to sickness absence;

6.5.2 where the **processing** is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment;

6.5.3 where the **processing** is necessary for health or social care purposes, for example in relation to pupils with medical conditions or disabilities; and

6.5.4 where none of the above apply we will seek the consent of the **data subject** to the **processing** of their **special category personal data**.

6.6 We will inform **data subjects** of the above matters by way of appropriate privacy notices which shall be provided to them when we collect the data or as soon as possible thereafter, unless we have already provided this information such as at the time when a pupil joins us.

6.7 If any **data user** is in doubt as to whether they can use any **personal data** for any purpose, they must contact the DPO before doing so.

Vital interests

6.8 There may be circumstances where it is considered necessary to **process personal data** or **special category personal data** in order to protect the vital interests of a **data subject**. This might include medical emergencies where the **data subject** is not in a position to give consent to the **processing**. We believe that this will only occur in very specific and limited circumstances. In such circumstances we would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur.

Consent

6.9 Where none of the other bases for **processing** set out above apply, the academy must seek the consent of the **data subject** before **processing** any **personal data** for any purpose.

6.10 There are strict legal requirements in relation to the form of consent that must be obtained from **data subjects**.

6.11 When pupils and/or our **workforce** join the Trust a consent form will be required to be completed in relation to them. This consent form deals with the taking and use of photographs and videos of them, amongst other things. Where appropriate, third parties may also be required to complete a consent form.

6.12 In relation to all pupils under the age of 13 years old we will seek consent from an individual with parental responsibility for that pupil.

6.13 We will generally seek consent directly from a pupil who has reached the age of 13; however, we recognise that this may not be appropriate in certain circumstances and therefore may be required to seek consent from and individual with parental responsibility.

6.14 If consent is required for any other **processing** of **personal data** of any **data subject**, the form of this consent must:

6.14.1 Inform the **data subject** of exactly what we intend to do with their **personal data**;

6.14.2 Require them to positively confirm that they consent – we cannot ask them to opt-out rather than opt-in; and

6.14.3 Inform the **data subject** of how they can withdraw their consent.

6.15 Any consent must be freely given, which means that we cannot make the provision of any goods or services or other matter conditional on a **data subject** giving their consent.

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

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

7 Processing for limited purposes

7.1 In the course of our activities as a Trust, we may collect and **process** the **personal data** set out in our Schedule of Processing Activities. This may include **personal data** we receive directly from a **data subject** (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and **personal data** we receive from other sources (including, for example, local authorities, other schools, parents, other pupils or members of our **workforce**).

7.2 We will only **process personal data** for the specific purposes set out in our Schedule of Processing Activities or for any other purposes specifically permitted by Data Protection Legislation or for which specific consent has been provided by the data subject.

8 Notifying data subjects

8.1 If we collect **personal data** directly from **data subjects**, we will inform them about:

8.1.1 our identity and contact details as **Data Controller** and those of the DPO;

8.1.2 the purpose or purposes and legal basis for which we intend to **process** that **personal data**;

8.1.3 the types of third parties, if any, with which we will share or to which we will disclose that **personal data**;

8.1.4 whether the **personal data** will be transferred outside the European Economic Area ('**EEA**') and if so the safeguards in place;

8.1.5 the period for which their **personal data** will be stored, by reference to our Retention and Destruction Schedule

8.1.6 the existence of any automated decision making in the **processing** of the **personal data** along with the significance and envisaged consequences of the **processing** and the right to object to such decision making; and

8.1.7 the rights of the **data subject** to object to or limit processing, request information, request deletion of information or lodge a complaint with the ICO.

8.2 Unless we have already informed **data subjects** that we will be obtaining information about them from third parties (for example in our privacy notices), if we then receive **personal data** about a **data subject** from other sources, we will provide the **data subject** with the above information as soon as possible thereafter, informing them of where the **personal data** was obtained from.

9 Adequate, relevant and non-excessive processing

9.1 We will only collect **personal data** to the extent that it is required for the specific purpose notified to the **data subject**, unless otherwise permitted by Data Protection Legislation.

10 Accurate data

10.1 We will ensure that **personal data** we hold is accurate and kept up to date.

10.2 We will take reasonable steps to destroy or amend inaccurate or out-of-date data.

10.3 **Data subjects** have a right to have any inaccurate **personal data** rectified. See further below in relation to the exercise of this right.

11 Timely processing

11.1 We will not keep **personal data** longer than is necessary for the purpose or purposes for which it was collected. We will take all reasonable steps to destroy, or erase from our systems, all **personal data** which is no longer required.

12 Processing in line with data subject's rights

12.1 We will **process** all **personal data** in line with **data subjects'** rights, in particular their right to:

12.1.1 request access to any **personal data** we hold about them;

12.1.2 object to the **processing** of their **personal data**, including the right to object to direct marketing;

12.1.3 have inaccurate or incomplete **personal data** about them rectified;

12.1.4 restrict **processing** of their **personal data**;

12.1.5 have **personal data** we hold about them erased

12.1.6 have their **personal data** transferred; and

12.1.7 object to the making of decisions about them by automated means.

The right of access to personal data

12.2 **Data subjects** may request access to all **personal data** we hold about them. Such requests will be considered in line with the Trust's Subject Access Request Procedure.

The right to object

12.3 In certain circumstances **data subjects** may object to us **processing** their **personal data**. This right may be exercised in relation to **processing** that we are undertaking on the basis of a legitimate interest or in pursuit of a statutory function or task carried out in the public interest.

12.4 An objection to **processing** can be raised verbally or in writing. If the Trust/academy receives a request verbally, they should ask for the objection to be raised in writing.

12.5 An objection to **processing** does not have to be complied with where the academy can demonstrate compelling legitimate grounds which override the rights of the **data subject**.

12.6 Such considerations are complex and must always be referred to the DPO upon receipt of the request to exercise this right.

12.7 In respect of direct marketing any objection to **processing** must be complied with.

12.8 The Trust is not obliged to comply with a request where the **personal data** is required in relation to any claim or legal proceedings.

The right to rectification

12.8 If a **data subject** informs the Trust that **personal data** held about them by the Trust is inaccurate or incomplete, we will consider that request and provide a response within one month.

12.9 If we consider the issue to be too complex to resolve within that period, we may extend the response period by a further two months. If this is necessary, we will inform the **data subject** within one month of their request that this is the case.

12.10 We may determine that any changes proposed by the **data subject** should not be made. If this is the case, we will explain to the **data subject** why this is the case. In those circumstances we will inform the **data subject** of their right to complain to the Information Commissioner's Office at the time that we inform them of our decision in relation to their request.

The right to restrict processing

12.11 **Data subjects** have a right to "block" or suppress the **processing** of **personal data**. This means that the Trust can continue to hold the **personal data** but not do anything else with it.

12.12 The Trust must restrict the **processing** of **personal data**:

12.12.1 Where it is in the process of considering a request for **personal data** to be rectified (see above);

12.12.2 Where the Trust is in the process of considering an objection to processing by a **data subject**;

12.12.3 Where the **processing** is unlawful but the **data subject** has asked the Trust not to delete the **personal data**; and

12.12.4 Where the Trust no longer needs the **personal data** but the **data subject** has asked the Trust not to delete the **personal data** because they need it in relation to a legal claim, including any potential claim against the Trust.

12.13 If the Trust has shared the relevant **personal data** with any other organisation, we will contact those organisations to inform them of any restriction, unless this proves impossible or involves a disproportionate effort.

12.14 The DPO must be consulted in relation to requests under this right.

The right to Be forgotten

12.15 **Data subjects** have a right to have **personal data** about them held by the Trust erased only in the following circumstances:

12.15.1 Where the **personal data** is no longer necessary for the purpose for which it was originally collected;

12.15.2 When a **data subject** withdraws consent – which will apply only where the Trust is relying on the individuals consent to the **processing** in the first place;

12.15.3 When a **data subject** objects to the **processing** and there is no overriding legitimate interest to continue that **processing** – see above in relation to the right to object; or

12.15.4 Where the **processing** of the **personal data** is otherwise unlawful;

12.15.5 When it is necessary to erase the **personal data** to comply with a legal obligation;

12.16 The Trust is not required to comply with a request by a **data subject** to erase their **personal data** if the **processing** is taking place:

12.16.1 To exercise the right of freedom of expression or information;

12.16.2 To comply with a legal obligation for the performance of a task in the public interest or in accordance with the law;

12.16.3 For public health purposes in the public interest;

12.16.4 For archiving purposes in the public interest, research or statistical purposes; or

12.16.5 In relation to a legal claim.

12.17 If the Trust has shared the relevant personal data with any other organisation, we will contact those organisations to inform them of any erasure, unless this proves impossible or involves a disproportionate effort.

12.18 The DPO must be consulted in relation to requests under this right.

Right to data portability

12.19 In limited circumstances a **data subject** has a right to receive their **personal data** in a machine-readable format, and to have this transferred to other organisation.

12.20 If such a request is made, the DPO must be consulted.

13 Data security

13.1 We will take appropriate security measures against unlawful or unauthorised processing of **personal data**, and against the accidental loss of, or damage to, **personal data**.

13.2 We will put in place procedures and technologies to maintain the security of all **personal data** from the point of collection to the point of destruction.

13.3 Security procedures include:

13.3.1 Any stranger seen in entry-controlled areas should be reported to Designated Safeguarding Lead ("**DSL**")

13.3.2 **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

13.3.3 **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required. IT assets must be disposed of in accordance with the Information Commissioner's Office guidance on the disposal of IT assets.

13.3.4 **Equipment.** Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

13.3.5 **Working away from the Trust premises – paper documents** so follow best practice and ensure confidential of all documents containing personal data. **Personal data** should be securely stored and retained for only as long as necessary. Documents should be destroyed at an academy-based secure disposal bin.

13.3.6 **Working away from the school premises – electronic working.** Staff are to follow best practice and

ensure the security and confidentiality of all personal data.

13.3.7 **Document printing.** Documents containing **personal data** must be collected immediately from printers and not left on photocopiers.

13.4 Any suspected data breach must be reported to the Trust's Data Protection Officer (DPO), via the Trust's **Data Breach Report Form**.

13.5 Any member of staff found to be in breach of the above security measures may be subject to disciplinary action.

14 Data protection impact assessments

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

14.2 In certain circumstances the law requires us to carry out detailed assessments of proposed **processing**. This includes where we intend to use new technologies which might pose a high risk to the rights of **data subjects** because of the types of data we will be **processing** or the way that we intend to do so.

14.3 The Trust will complete an assessment of any such proposed **processing** and has a template document which ensures that all relevant matters are considered.

14.4 The DPO should always be consulted as to whether a data protection impact assessment is required, and if so how to undertake that assessment.

15 Disclosure and sharing of personal information

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

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

15.3 In some circumstances we will not share safeguarding information. Please refer to our Child Protection Policy.

16 Data processors

16.1 We contract with various organisations who provide services to the Trust including:

16.1.1 Payroll providers

16.1.2 School meal providers

16.1.3 Educational learning platform providers

16.1.4 ICT support provider

16.1.5 Educational learning platform providers

16.1.6 Electronic communication providers

16.2 In order that these services can be provided effectively we are required to transfer **personal data** of **data subjects** to these **data processors**.

16.3 **Personal data** will only be transferred to a **data processor** if they agree to comply with our procedures and policies in relation to data security, or if they put in place adequate measures themselves to the satisfaction of the Trust. The Trust will always undertake due diligence of any **data processor** before transferring the **personal data** of **data subjects** to them.

16.4 Contracts with **data processors** will comply with Data Protection Legislation and contain explicit obligations on the **data processor** to ensure compliance with the Data Protection Legislation, and compliance with the rights of **data subjects**.

17 Images and videos

17.1 Parents and others attending Trust events are allowed to take photographs and videos of those events for domestic purposes. For example, parents can take video recordings of a school performance involving their child. The Trust does not prohibit this as a matter of policy.

17.2 The Trust does not however agree to any such photographs or videos being used for any other purpose, but acknowledges that such matters are, for the most part, outside of the ability of the Trust to prevent.

17.3 The Trust asks that parents and others do not post any images or videos which include any child other than their own child on any social media or otherwise publish those images or videos.

17.4 As a Trust we want to celebrate the achievements of our pupils and therefore may want to use images and videos of our pupils within promotional materials, or for publication in the media such as local, or

even national, newspapers covering Trust events or achievements. We will seek the consent of pupils, and their parents where appropriate, before allowing the use of images or videos of pupils for such purposes.

17.5 Whenever a pupil begins their attendance at the Trust, they, or their parent where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that pupil. We will not use images or videos of pupils for any purpose where we do not have consent.

18 CCTV

18.1 The Trust operates a CCTV system. Please refer to the Trust's CCTV Policy.

19 The use of Artificial Intelligence (AI)

19.1 Staff must **not use** generative Artificial Intelligence (AI) tools such as Large Language Models (LLMs), for example as Chat GPT, Gemini etc., if it involves sharing personal data of our staff, students, parents or visitors.

19.2 Personal Data includes:

19.2.1 Names
19.2.2 Any personal identifiers, such as initials or unique identifiers, such as student admission number, a student's Unique Pupil Number (UPN), a staff member's national insurance number etc.
19.2.3 Email address
19.2.4 Any other information that could be used to reasonably identify someone

19.3 AI tools may share data with other third parties or may make shared data publicly available. An example would be sharing spreadsheet of student's exam results through an AI chat tool to analyse, and that information being stored by the AI tool and subsequently returned if a member of the public asks a specific question.

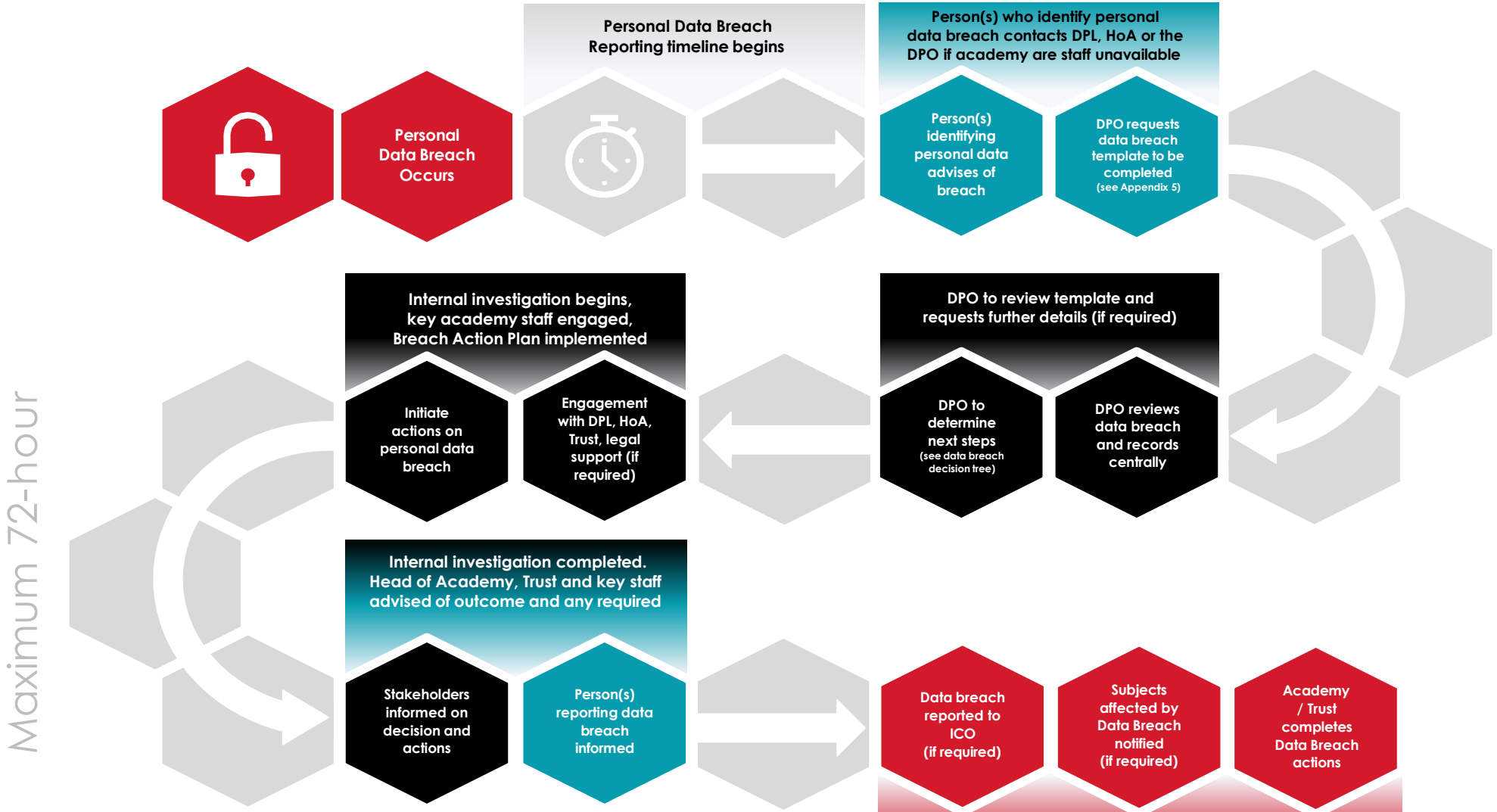
20 Changes to this policy

We may change this policy at any time. Where appropriate, we will notify **data subjects** of those changes.

Appendix 1 - Definitions of terms

Term	Definition
Data	is information which is stored electronically, on a computer, or in certain paper-based filing systems
Data Subjects	for the purpose of this policy this include all living individuals about whom we hold personal data including pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information
Personal Data	means any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Data Controllers	are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used across our Trust
Data Users	are those of our workforce (including Academy Associates and volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times
Data Processors	include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions
Processing	is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties
Special Category Personal Data	includes information about a person's racial or ethnic origin, religious or philosophical beliefs, trade union membership, physical or mental health or condition or biometric data
Workforce	Includes, any individual employed by Trust such as staff and those who volunteer in any capacity including Academy Associates and/or Trustees / Members/ parent/carers/ helpers.

Appendix 2 - Personal Data Breach Notification Timeline



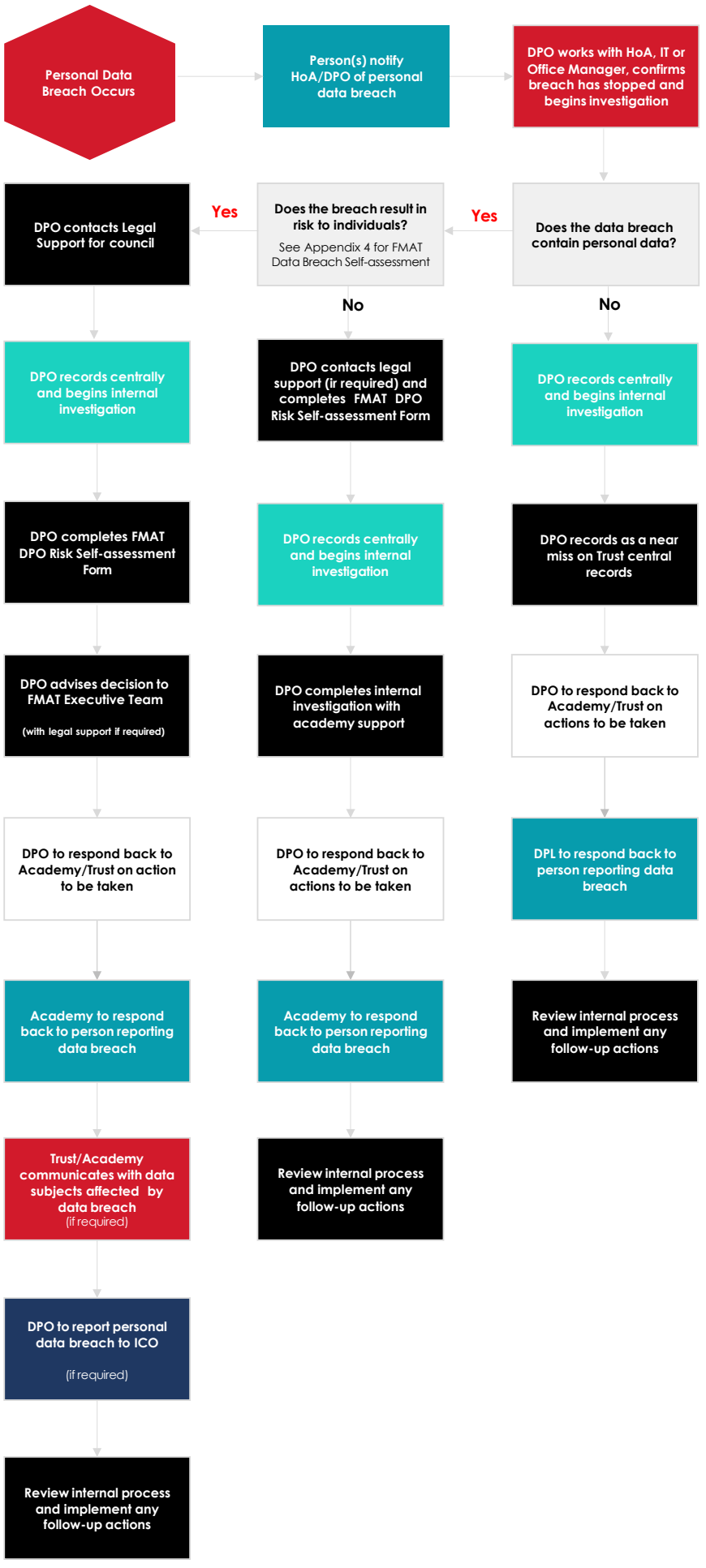
Descriptors

Person(s) identify data breach and complete *FMAT Data Breach Report Form*

DPO

DPO relates to the Data Protection Officer, Robert Fitzgerald, Fairfax Multi-Academy Trust

Appendix 3 - Data Breach Decision Tree



DPO Action 1:

DPO acknowledges data breach and reviews Data Breach Report Format

DPO Action 2:

The DPO to confirm if the data breach results in a risk to individuals

DPO Action 3:

The DPO will review the breach and advise of the appropriate next steps

DPO Action 4:

Scenario 1:

Data Breach with no personal data disclosed:

- DPO to ensure academy/trust follows the FMAT Data Breach Procedure
- DPO to start data breach investigation
- DPO to present findings back to Academy/Trust
- DPO to update records as near miss
- Academy/Trust to review internal findings and complete any follow-up actions

Scenario 2:

Data Breach will not result in risk to the individual (legal council may be required):

- DPO ensures academy/trust follows the FMAT Data Breach Procedure
- DPO completes FMAT Data Breach Self-Assessment see Appendix 4 of FMAT Data Protection Policy
- DPO completes FMAT Data Breach Risk Self-Assessment Form
- DPO to present findings back to Academy/Trust
- Academy/trust review internal findings and complete any follow-up actions
- DPO to update records and record anyfollow-up actions

Scenario 3:

Data Breach will result in a risk to the individual (legal council may be required):

- DPO to contact legal support to understand how to prioritise data subjects rights and freedoms
- DPO ensures academy/trust follows the FMAT Data Breach Procedure
- DPO completes FMAT Data Breach Risk Self-Assessment Form
- DPO to present findings back to academy/trust
- Academy/trust to communicate with data subjects affected by breach without delay (if required)
- DPO to report data breach to ICO without delay (if required)
- Academy/trust review internal findings and complete any follow-up actions
- DPO to support with Information Commissioners Office (ICO) on any follow up actions (if required).
- DPO to update records and record any follow-up actions

Appendix 4 - Data Breach Risk Self-Assessment Decision Tree

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

If we experience a personal data breach we need to consider whether this poses a risk to people. We need to consider the likelihood and severity of the risk of physical, material or non-material damage to an individual.

If it's likely there will be a risk then we must notify the ICO; if it's unlikely then we don't have to report. We do not need to report every breach to the ICO, however we do need to assess the risk of each data breach.

The Data Protection Officer (DPO) will keep the trust up-to-date with latest guidance on data protection law.

The DPO determines the risk level of breaches and determines whether to the data subjects are required to be advised of a data breach.

The DPO is responsible for reporting data breaches to the Information Commissioners Office (ICO)

Personal Data Breach Occurs

Staff follow the FMAT Data Breach Procedure

DPO begins FMAT DPO Data Breach Risk Self-Assessment

Does the breach contain any of the following;

a) large amounts of data
b) sensitive data
c) financial personal data
d) child protection information
e) data which should be confidential
f) medical
g) data relating to sexual orientation
h) commercially sensitive data
i) reputationally damaging to the data subject
j) location or home address
k) operationally sensitive
m) CCTV or video footage
n) passwords or login information
o) lost or loss of access to data
p) not knowing was data has been accessed/copied

This list is non-exhaustive.

All breaches will be judged case-by case basis by DPO,

Legal support and/or ICO to provide advice on any queries.

Yes

Can we establish that the data was breached to trusted individuals?

A scenario would be whereby the unintended recipient of personal data agrees not to access, and deletes all records.

If we can ascertain that the individuals who were involved in the breach can be trusted, this may limit the risk of the breach.

This information needs to be provided to the DPO to help assess the risk. Each data breach will be reviewed on a case by case basis.

No

Assessing the risk to individuals:

A breach can cause a data subject emotional distress, and physical and material damage.

To help determine the risk of a data breach, we should meet the following conditions;

1) we have corrected the data breach

2) There has been no damage to the data subject

3) We can ensure that there will be no future damage caused by the breached information

The Trust DPO will review the data breach and taking into account the duration of the breach, the amount of data, the types of data, and how the data was breached.

Each data breach must be reviewed on its own individual circumstances.

DPO to complete FMAT DPO Data Breach Risk Self-Assessment. Queries to be raised with legal support and/or support from the ICO (if required). DPO determines whether the breach will result in risk to individual, and if so, what level.

Likely Risk

Assessing Risk:

Likely risk to individual

Is there a high risk?

High Risk

Academy advises data subjects. Trust DPO notifies ICO without delay.

Not High Risk

Trust DPO notifies ICO of the data breach. without delay

Unlikely Risk

Assessing Risk:

Unlikely risk to individuals

Academy/ Trust completes the FMAT Data Breach Procedure following, with the pathway of:

Scenario 2:

'Data Breach will not result in risk to the individual'

Unlikely Risk

Assessing Risk:

Unlikely risk to individuals

Academy/ Trust completes the FMAT Data Breach Procedure following, with the pathway of:

Scenario 2:

'Data Breach will not result in risk to the individual'

DPO Action 3:

If a personal data breach occurs, the DPO will review the breach and advise of the appropriate next steps

DPO Action 4:

Scenario 1:

Data Breach with no personal data disclosed:

- DPO to ensure academy/trust follows the FMAT Data Breach Procedure
- DPO to start data breach investigation
- DPO to present findings back to Academy/Trust
- DPO to update records as near miss
- Academy/Trust to review internal findings and complete any follow-up actions

Scenario 2:

Data Breach will not result in risk to the individual (legal council may be required):

- DPO ensures academy/trust follows the FMAT Data Breach Procedure
- DPO completes FMAT Data Breach Self-assessment see Appendix 4 of FMAT Data Protection Policy
- DPO completes FFMAT Data Breach Risk Self-Assessment Form
- DPO to present findings back to Academy/Trust
- Academy/trust review internal findings and complete any follow-up actions
- DPO to update records and record any follow-up actions

Scenario 3:

Data Breach will result in a risk to the individual (legal council may be required):

- DPO to contact legal support to understand how to prioritise data subjects rights and freedoms
- DPO ensures academy/trust follows the FMAT Data Breach Procedure
- DPO completes FMAT Data Breach Risk Self-Assessment Form
- DPO to present findings back to academy/trust
- Academy/trust to communicate with data subjects affected by breach without delay (if required)
- DPO to report data breach to ICO without delay (if required)
- Academy/trust review internal findings and complete any follow-up actions
- DPO to support with Information Commissioners Office (ICO) on any follow up actions (if required).
- DPO to update records and record any follow-up actions

Appendix 5 - Data Breach Report Form

If you discover a potential personal data security breach, please immediately contact the Trust's Data Protection Officer (DPO). After which you will be requested to complete an electronic form accessible here, alternatively you can email it to: dpo@fmat.co.uk

NOTIFICATION OF PERSONAL DATA BREACH FORM	
Date(s) and time of breach:	
Date and time data breach was discovered:	
Academy the data breach relates to:	
Name and initials of person who identified the incident:	
Name and initials of person reporting the incident:	
Brief description of personal data breach:	
Number of data subjects affected – if known:	
Brief description of any actions taken since the breach was discovered:	
DATA PROTECTION OFFICER USE ONLY	
Data breach DPO notification date and Trust case number:	
Data breach reported to ICO:	
Communicated to data subjects (include communication):	

Frequently Asked Questions:

What is personal data?

As an academy you will hold data on our pupils, on parents/carers and our staff members.

Personal data relates to any information you can identify someone with, most commonly, their name. This data can be stored in a paper file, an email, a spreadsheet, a word document or even a photograph/video. As you can identify a person, you may also be able tell more information about the person, such as their ethnicity, something relating to their health (e.g. SEN or allergies) or their personal circumstances (e.g. Free School Meals).

What is a personal data breach?

A personal data breach means that, accidently or deliberately, personal data has been shared, amended, accessed, destroyed or lost when it should not have been.

The below incidents could be a personal data breach:

- **Emailing a parent/carer information on another pupil**
- **A lost or stolen laptop/memory stick (encrypted or unencrypted)**
- **A lost or stolen markbook/pupil list**
- **Unauthorised access to a school system (SIMs, Show My Homework, PS Connect etc.)**
- **Accidently or deliberately deleting data which should be retained**
- **Altering data without permission**
- **Posting personal data to an incorrect recipient**
- **Losing personal data in the post**
- **Verballing providing information to someone who should not receive it, i.e. phone scam**
- **Not securely destroying sensitive information i.e. not using secure disposal bins or not wiping electronic equipment**
- **Inability to access information i.e. ransomware, prolonged system outage**
- **Failure to redact some personal data if supporting with a Subject Access Request (SAR)**

(This list is not exhaustive.)

If you are unsure whether a data breach has occurred:

Please contact your Head of Academy or member of leadership responsible for data protection. If they are unavailable contact FMAT Data Protection Officer (DPO) at **dpo@fmat.co.uk**

What should I do if a personal data breach has occurred?

If you believe there has been a data breach, you should immediately contact your Head of Academy or member of leadership responsible for data protection, they will contact the DPO.

The DPO will begin an internal investigation and work with you and your academy to understand the cause and any follow up actions.

For more information;

Please refer to the **FMAT Data Breach Timeline** and the **FMAT Data Breach Decision Tree**.

You can also find more information on the ICO website https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

Appendix 6 - Subject Access Request Decision Tree

FAIRFAX MULTI-ACADEMY TRUST

Subject Access Request (SAR) raised by data subject.

SAR processed following internal FMAT Subject Access Request (SAR) Procedure

SAR completed without undue delay and within a maximum of one month

Day 1

SAR Timeline Day 1:

One Month Max timeline starts

SAR relates to staff

SAR relates to pupils

SAR relates to parents

SAR Timeline Day 1:

Academy (unless trust related) reviews request template and determines actions

HoA/DPL advised of Subject Access Request (SAR). DPO records centrally

HoA/DPL advised of Subject Access Request (SAR). DPO records centrally

HoA/DPL advised of Subject Access Request (SAR). DPO records centrally

SAR Timeline Day 1 to 2:

Academy processes (unless trust related), acknowledges request to requester and begins data collation

Academy validates and completes Subject Access Request

Academy validates and completes Subject Access Request

Academy validates and completes Subject Access Request

Day 1 to 15

SAR Timeline: Day 1 to15

Academy processes (unless trust related) and begins data collation

Is Legal Support Required before completing Subject Access Request?

SAR Timeline Day 2 to15

Academy to liaise with DPO on current status of the SAR

YES

NO

DPO contacts legal support (if required) for support with SAR

Minimum 5 Day Turnaround

Day 2 to 20

SAR Timeline Day 2 to 20:

DPO to liaise with legal support (if required)

DPO confirms legal status or necessary actions to complete SAR

Day 2 to 25

SAR Timeline Day 2 to 25:

DPO to advise academy of legal advice and/or necessary actions

Academy completes SAR without undue delay and sends electronically unless requester states a preferred method

Academy completes SAR without undue delay and sends electronically unless requester states a preferred method

Day 2 to 31 MAX

SAR Timeline Day 2 to One Month:

Academy to send SAR to data subject via preferred method

DPO records SAR is completed on central Trust records

DPO records SAR is completed on central Trust records

SAR Timeline Day 2 to One Month:

DPO centrally records SAR completed

Academy/DPO responds to any queries or SAR process starts again if new request

Academy /DPO responds to any queries or SAR process starts again if new request

Restart Process

After closure of SAR:

Any additional queries recorded or SAR process restarts

Appendix 7- Subject Access Request (SAR) Request Form

You can use this form to request access to the personal information held on you by the academy/trust. Please send a signed copy of this form and proof of your identity (see Section 3) to the relevant academy.

If your request relates to a pupil at the age of 13 or above, we will require their consent. Please refer the authority on Section 4 of this form.

Section 1 – your details:

Legal Surname:	
Legal First name(s):	
Address:	
Postcode:	
Telephone/Mobile:	
Email:	
Name of the person you are requesting personal data for: If the information relates to a pupil at the academy, please provide the name and age of the pupil(s):	
If your request relates to a pupil, do you have parental responsibility? If the answer is no, please provide justification for your request.	

Please ensure you enclose proof of your identity when sending this request. Please see **FMAT Subject Access Request Verification**, Section 3 of this form.

Section 2 – Personal Data Requested:

Please provide a description of the data you are requesting in the box below. You may continue overleaf if needed. You should describe the information you need as clearly as possible: it is not sufficient to ask for "everything about me". If your request is too broad or unclear, we may need to ask you to be more specific.

Section three – declaration

I am the enquirer named in **Section One** of this form and request that…….. (insert name of the academy to which this relates) provide me with a copy of the personal data held for the Data Subject.

Signed: ……..

Date: ……..

FMAT Subject Access Request Verification - Section 3

Under the Data Protection Act 2018 and General Data Protection Regulation (GDPR), in order to process your Subject Access Request (SAR) we need to be verify that the data subject making the request for personal data (information) is the data subject the information belongs to, or has the authority to act on their behalf. To help us do this, we need to view some identity documents to confirm your identity or authority.

Please use the Sections below and the Lists overleaf to help you decide which documents you need to include with your application. Please be aware that we only require copies of the documents. **Please send copies electronically, do not send originals.**

If you are requesting your own personal data you will need to provide:

- Two documents from List A;
- If you have changed your name since the records were created, a document from List B also

If you are applying on behalf of a child under 13 years you will need to provide:

- Two documents from List A for yourself as the Applicant;
- A document from List C for the child as the Data subject;
- If the child has changed their name since the records were created, a document from List B also

You are applying on behalf of another person (including children aged 13 years or over) you will need to provide:

- Two documents from List A for yourself as the Applicant;
- A letter of consent from the Data Subject;
- If the Data Subject has changed their name since the records were created, a document from List B also

List A

- ☐ Current Passport
- ☐ Current Full Driving Licence
- ☐ Birth/Marriage Certificate
- ☐ P45/P60
- ☐ Credit Card/Mortgage Statement
- ☐ Recent Utility Bills with Current Address

List B

- ☐ Marriage Certificate
- ☐ Civil Partnership Certificate
- ☐ Deed Poll
- ☐ Decree Absolute Certificate
- ☐ Adoption Certificate

List C

- ☐ Full birth certificate including name(s) of parent(s)
- ☐ Court document granting Parental Responsibility
- ☐ A letter from a Solicitor on headed paper confirming Parental Responsibility

List D

- ☐ Utility Bill dated within the last 6 months
- ☐ Fixed Line (Land Line) Telephone Bill dated within the last 6 months
- ☐ Valid TV Licence
- ☐ Bank or Building Society Statement dated within the last 6 months
- ☐ Local Authority Council Tax Bill for the current council tax year
- ☐ Mortgage statement issued for the last full year
- ☐ Addressed Pay slip dated within the last 6 months
- ☐ Letter from the Department of Work and Pensions (DWP) confirming receipt of benefits

Applications from Solicitors

For applications from a Solicitor for a child under the age of 13 you will need to provide:

- A covering letter on letter headed paper;
- Consent from the parent / legal guardian for you to act on their behalf;
- Confirmation that the parent / legal guardian has Parental Responsibility

For applications from a Solicitor for an adult (including children aged 13 years or over) you will need to provide:

- A covering letter on letter headed paper;
- Consent from the Data Subject authorising you to act on their behalf; **OR**
- Consent from the Data Subject authorising their Personal Representative to act on their behalf **AND** consent from that Personal Representative authorising you to act; **OR**
- Consent from the Personal Representative of the Data Subject **AND** confirmation that the Personal Representative has a registered Power of Attorney (Health and Welfare)

For applications from a Solicitor involving a Litigation Friend you will need to provide:

- A covering letter on letter headed paper;
- Certificate of Suitability of Litigation Friend

FMAT Subject reference request – Section 4 - consent by pupils

Pupil Legal Surname:	
Pupil Legal First name(s):	
Academy:	
Year Group:	
Registration Group:	
Date of Birth:	
Home Address:	
Post Code:	

Pupil consent for release of personal data:

I hereby give my consent for……(insert name) to access my personal data through a Subject Access Request.

Name: ……

Signature: ……

Requesters relationship to you: ……

Date: ……

Please send the completed form to the relevant academy or:

email this form to dpo@fmat.co.uk

or post to:

FAO Data Protection Officer, Fairfax Multi-Academy Trust, Fairfax Road, Sutton Coldfield, Birmingham, B75 7JT

Information Security Procedure

Fairfax Multi-Academy Trust

Appendix 8

1 PROCEDURE OVERVIEW

1.1 Fairfax Multi-Academy Trust is committed to the highest standards of information security and takes it extremely seriously.

1.2 In relation to personal data, the Data Protection Act 2018 requires the Trust to:

1.2.1 use technical and organisational measures to ensure personal information is kept secure, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage;

1.2.2 implement appropriate technical and organisational measures to demonstrate that it has considered and integrated data compliance measures into the Trust's data processing activities; and

1.2.3 be able to demonstrate that it has used or implemented such measures.

1.3 This aim of this procedure is to:

1.3.1 protect against potential breaches of confidentiality and personal data breaches;

1.3.2 ensure the Trust's information assets are protected against damage, loss or misuse;

1.3.3 support the Trust's **Data Protection Policy** in ensuring that all staff are aware of and comply with their legal obligations and the Trust's procedures applying to the processing of personal data; and

1.3.4 increase awareness and understanding of the requirements of information security and the responsibility of staff to protect the confidentiality and integrity of the information that they themselves handle.

1.4 This procedure uses the following definitions:

Term	Meaning
Cloud based systems	is a collective term which means the cloud based software providers engaged by the Trust for organisational purposes;
Confidential information	means trade secrets or other confidential information (either belonging to the Trust or to third parties) that is processed by the Trust;
Criminal offence data	means personal data relating to criminal convictions and offences or related security measures. This includes any personal data linked to criminal offences, or which is specifically used to learn something about an individual's criminal record or behaviour.

Term	Meaning
Organisational information	means all information related to the Trust other than personal data;
Personal data	means any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other available information;
Pseudonymised	means the technique by which personal data is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to additional security measures;
Special category personal data	means personal data afforded special protection by the UK GDPR. This includes, information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetic information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

2 ROLES AND RESPONSIBILITIES

2.1 The Trust's Data Protection Officer (DPO) has overall responsibility for this procedure. They are responsible for ensuring it is adhered to by all staff. They may be contacted using the following details:

Data Protection Officer (DPO)

Fairfax Multi-Academy Trust

Fairfax Road

Sutton Coldfield

West Midlands

B75 7JT

dpo@fmat.co.uk

3 SCOPE OF PROCEDURE

3.1 The information covered by this procedure includes all written, spoken and electronic information held, used or transmitted by or on behalf of the Trust, in whatever media. This includes information held on computer systems, hand-held devices, phones, paper records, and information transmitted orally.

3.2 This procedure applies to all staff, including employees, directors, trainees, agency workers and casual workers.

3.3 All staff must be familiar with this procedure and comply with its terms.

3.4 Where this procedure applies, staff should be aware that other policies and protocols, such as those listed below, are also likely to also apply and staff should comply with those as well as this policy:

3.4.1 Data Protection Policy;

3.4.2 Records Retention Schedule

3.4.3 ICT Acceptable Use Policy

3.4.4 CCTV Policy

3.4.5 Data Breach Procedure;

3.5 This procedure does not form part of any employee's contract of employment and the Trust may amend or remove it, at any time.

4 GENERAL PRINCIPLES

4.1 Personal data, and special category personal data, must be protected against unauthorised and/or unlawful processing and against accidental loss, destruction or damage, by the use of appropriate technical and organisational measures.

4.2 Organisational information (other than personal data) is owned by the Trust and not by any individual. Organisational information must only be used only in connection with work being carried out for the Trust and not for other commercial or personal purposes.

4.3 Personal data must be used only for the specified, explicit and legitimate purposes for which it is collected.

5 INFORMATION MANAGEMENT

5.1 Personal data must be processed in accordance with:

5.1.1 the data protection principles, set out in Article 5 of the Data Protection Act 2018;

5.1.2 The Trust's Data Protection Policy generally; and

5.1.3 all other relevant policies.

5.2 In addition, all personal data collected, used and stored by the Trust must be:

5.2.1 adequate, relevant and limited to what is necessary for the relevant purposes;

5.2.2 kept accurate and up to date;

5.3 The Trust will put in place appropriate technical and organisational measures to ensure that personal data is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage, including:

5.3.1 anonymisation and /or pseudonymisation of personal data;

5.3.2 encryption of personal information;

5.3.3 processes for regularly testing, assessing and evaluating the effectiveness of security measures;

5.3.4 Encryption of personal devices

5.4 Personal data and confidential information will be kept for no longer than is necessary and stored and destroyed securely in accordance with the Trust's Records Retention Schedule.

6 STAFF INFORMATION

6.1 Any individual in a management or supervisory role or involved in recruitment must keep staff information strictly confidential.

6.2 Staff may ask to see their personnel files and any other personal information in accordance with their right of access set out in Article 15 Data Protection Act 2018. For further information on how staff may exercise this right, please refer to the Trust's Data Protection Policy.

7 COMPUTERS AND IT

7.1 The Trust uses a number of software-based processors who supply the Trust with a range of services. Together, the software-based processors are referred to as "cloud-based systems". These include, but are not limited to:

7.1.1 Cloud-based Email and Document holding system

7.1.2 Cloud-based Management Information System

7.1.3 Cloud-based HR systems

7.2 Computers and other electronic devices used for work purposes must be password protected. Passwords must not be written down or given to others.

7.3 Computers and other electronic devices used for work purposes must be locked when not in use and/or unattended, to minimise the risk of accidental loss or disclosure.

7.4 Staff must log out from the Trust's cloud-based systems when not in use.

7.5 Staff must not access the Trust's cloud-based systems using unsecured WiFi networks (e.g. in a hotel or café).

7.6 Personal data and confidential information must not be copied onto external storage (e.g. USB memory sticks, external hard drives) without the express permission of the Trust's Data Protection Officer (DPO) and must be password protected and encrypted. Information held on any of these devices should be transferred to cloud-based systems as soon as possible in order for it to be backed up and then deleted from the external storage device.

8 COMMUNICATIONS AND TRANSFER OF INFORMATION

8.1 Staff must be careful about maintaining confidentiality when speaking in public places, e.g. when speaking on a mobile telephone.

8.2 Confidential information must be circulated only to those who need to know the information in the course of their work for the Trust.

8.3 Staff must ensure that particularly sensitive personal data (including special category personal data and criminal offence data) and confidential information is:

8.3.1 stored on an encrypted device with strong password protection, which is kept locked when not in use;

8.3.2 If being transferred electronically (e.g. by email), either through secure cloud-based sharing or password protecting the document via email;

8.3.3 when in paper copy, not transported in see-through or other unsecured bags or cases;

8.3.4 not read in public places (e.g. waiting rooms, cafes, trains); and

8.3.5 not left unattended or in any place where it is at risk (e.g. in conference rooms, in cars, cafés).

8.4 Postal and e-mail addresses and numbers should be checked and verified before information is sent to them. Particular care should be taken with e-mail addresses where auto-complete features may have inserted incorrect addresses.

8.5 WhatsApp or other chat platforms may be used by staff to communicate urgent, non-sensitive matters. WhatsApp or other chat platforms must never be used to communicate personal data relating to students, parents or other staff members, confidential information, or sensitive organisational information.

9 PERSONAL EMAIL AND CLOUD STORAGE ACCOUNTS

9.1 Staff must not use a personal email account or cloud storage accounts for work purposes in any circumstances.

9.2 Staff must not send or forward personal data, organisational information or confidential information to their personal email account.

9.3 All work undertaken for the Trust should be completed using Trust user accounts and e-mail addresses.

9.4 Staff must not share log-in information for any of their Trust user accounts with anyone or use another person's account credentials to access these accounts.

10 HOME WORKING

10.1 To the extent that staff undertake work for the Trust at home, staff must ensure that appropriate technical and practical measures are in place within the home to maintain the continued security and confidentiality of that information. In particular:

10.1.1 personal data and confidential information must be kept in a secure and locked environment where it cannot be accessed by family members or visitors; and

10.1.2 all personal and confidential information must be retained and disposed of in accordance with the Records Retention Schedule.

10.2 Where staff use personal devices, they must comply with the additional obligations set out in the ICT Acceptable Use Policy.

11 TRAVELLING ABROAD

11.1 Staff must not travel with hard-copy information containing personal data or confidential information without taking appropriate sets to ensure that the information is held securely when travelling, and is disposed of securely upon return.

11.2 Any hard copies of data lost or stolen must be reported to the Trust's Data Protection Officer (DPO) immediately.

11.3 In the event that staff travel with devices (including personal devices used for Trust-related work) for any reason, staff must ensure that no personal data, organisational information or confidential information is saved locally, and all information is saved securely using the relevant cloud-based systems.

12 REPORTING DATA BREACHES

12.1 All members of staff have an obligation to report actual or suspected personal data breaches to Trust's Data Protection Officer (DPO) immediately upon discovery.

12.2 The Trust's Data Protection Policy details the Trust's data protection procedure, how to report a data breach and the next steps taken. Any data breaches must be reported to the Trust's Data Protection Officer (DPO) by completing this form or by emailing the Trust's Data Protection Officer (DPO) at dpo@fmat.co.uk.

12.3 The Trus's Data Breach Procedure can be accessed through the Trust's intranet.

13 CONSEQUENCES OF FAILING TO COMPLY WITH THIS PROCEDURE

13.1 The Trust takes compliance with this procedure very seriously. Failure to comply with it puts both staff and the Trust at significant risk. The importance of this procedure means that failure to comply with any requirement of it may lead to disciplinary action