Data protection policy and procedures

September 2020

Published date:	Next review deadline:	Statutory	Executive Lead at ATT:
September 2020	September 2023		Andy Gannon Head of Corporate Affairs

Associated documents:	
Links to:	
• Freedom of Information policy • Privacy notices	

Approved by the Trust Board, July 2020

Our Vision

We have one core purpose:
To have the biggest positive impact in the varied communities we serve through ensuring top drawer education for our learners. #TransformingLives

How do we ensure this across our trust?
In all we do we are:

1. Ethical to the core, ensuring that education is always front and centre
2. Futures focused system leaders – never simply followers
3. Collaborative in every endeavour
4. Resolutely learner centred.

What does this look like across our trust?
Education
We are:

1. Ruthlessly ambitious for all who learn and work with us
2. Unwaveringly inclusive – determined on eradicating barriers to educational success
3. Committed to excellent teaching
4. Determined upon academic excellence for all in our communities
5. Compassionate, ethical and caring advocates for all in our communities
6. Outwardly facing and globally conscious

Operations
We are:

1. Committed to the very best people development and empowerment
2. Determined to shout loudly and share proudly our successes
3. The best professional and technical experts (supporting education) in the sector
4. Committed to the very best understanding and management of risk

Financial
We are:

1. Providing the best possible public service for the best possible value
2. Determined to supplement our public income with shrewd income generation
3. Building financially sustainable models of educational improvement in our communities
4. Demonstrably efficient in all we do

Our values

- We will work inclusively within our communities, embracing the varied localities we serve while sharing our common vision and values.
- We will develop the very best leaders of the future, working to improve education and transform lives.
- We will adhere unwaveringly to the 'Nolan Principles' of Public Service, which is made clear in our commitment to Ethical Leadership.

Contents

Our Trust Data Protection Officer is Andy Gannon, Head of Corporate Affairs (DPO@academytransformation.co.uk)

The Data Protection Lead (DPL) for Mildenhall College Academy is Chris Leach.

1 Statement of intent

1.1 Everyone has rights with regard to the way in which their **personal data** is handled. During the course of our activities 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 take our responsibilities in the realm of data protection very seriously. We are committed to the protection of all personal data and special category personal data for which we are the data controller.

1.3 We expect all our people to treat the data entrusted to us as if it were their own, and to apply to its storage and processing the same standards that they would expect to be applied to their own data.

1.4 In accordance with the principles set out in our statement of ethical leadership, we are committed to openness, honesty and transparency. We apply these principles most strictly to our work in regard to data protection. We will ensure that information and data is openly available where possible and ensure that access to personal data is easy for all those who request it.

1.5 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.

1.6 All our people must comply with this policy when processing personal data on our behalf. This includes staff, volunteers, contractors and those involved in our governance. Any breach of this policy may result in disciplinary or other action.

We will

- ensure that there is a single point of contact with the overall responsibility for data protection (the Data Protection Officer)
- ensure each academy has a named Data Protection Lead
- provide training and development for all members of staff who handle personal information
- provide clear lines of report and supervision for compliance with data protection
- carry out regular checks to monitor compliance with this policy across all our academies

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 General Data Protection Regulation ('**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

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

4 Data Protection Officer

4.1 We are required to appoint a Data Protection Officer ("DPO"). Our DPO is Andy Gannon, and they can be contacted at DPO@academytransformation.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 **data subjects** and others in relation to matters of data protection. Our network of academy-based DPLs (data protection leads) works closely with the DPO and individual academy queries should first be raised with the appropriate DPL.

5 Data protection principles

5.1 Our **processing of personal data** will always 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

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.

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 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**

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** on the following legal basis:

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.

Where none of the above apply then 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 then an additional legal ground must apply to that processing. We will normally only **process special category personal dat**a on the following legal basis:

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.

Where none of the above apply then 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, for example 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 then 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 then we will 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** then the form of this consent will

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

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 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, 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 procedures (see Appendix 4).

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

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), then if we 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

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

We will not keep **personal data** longer than is necessary for the purpose or purposes for which they were 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 subjects' 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

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 our subject access request procedure (see Appendix 3).

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** does not have to be complied with where the school can demonstrate compelling legitimate grounds which override the rights of the **data subject**.

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

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

12.7 We are not, however, 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 then we will consider that request and provide a response within one calendar month.

12.9 If we consider the issue to be too complex to resolve within that period then we may extend the response period by a further two months. If this is necessary then 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 then 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 we can continue to hold the **personal data** but not do anything else with it.

12.12 We must restrict the **processing** of **personal data**

12.12.1 where we are in the process of considering a request for **personal data** to be rectified (see above)

12.12.2 where we are 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 us not to delete the **personal data**

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

12.13 If we have shared the relevant **personal data** with any other organisation then 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 us 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 we are relying on the individual's 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.

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 We are 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

12.16.5 in relation to a legal claim.

12.17 If we have shared the relevant personal data with any other organisation then 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 then 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 **entry controls** – please see our 'Visitors to Site' policy for further details

13.3.2 **secure lockable desks and cupboards** - desks and cupboards will be kept locked if they hold confidential information of any kind – and personal information is always considered confidential

13.3.3 **methods of disposal** - paper documents will be shredded; digital storage devices will be physically destroyed when they are no longer required; IT assets will be disposed of in accordance with the Information Commissioner's Office guidance on the disposal of IT assets

13.3.4 **equipment** - data users will 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 **paper documents** – any paper documents removed from site will be kept securely by the data user – this means they will be kept on the user's person or locked away securely and out of sight of passers-by

13.3.6 **electronic devices** – only authorised devices will be permitted to be used for working offsite where the processing of personal data takes place – in the event that these devices are personal to data users, appropriate safeguards will be put in place to ensure the security of data; material may be transferred between devices by USB stick, but the data must be erased from the stick as soon as it is securely stored on a device

13.3.7 **document printing** - documents containing **personal data** must be collected immediately from printers and not left on photocopiers.

13.4 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 We take 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 We will complete an assessment of any such proposed **processing** and we have 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, Education and Skills Funding Agency (ESFA), Ofsted, health authorities and professionals, local authorities, examination bodies, other schools, and other organisations where we have a lawful basis for doing so.

15.2 We 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 Safeguarding and 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 catering providers

16.1.3 security providers

16.1.4 estates contractors

16.1.5 training 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 our satisfaction. We 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 our 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. We do not prohibit this as a matter of policy.

17.2 We do not however agree to the use of such photographs or videos for any other purpose, but we acknowledge that such matters are, for the most part, outside our ability to prevent.

17.3 We ask 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 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 school 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 with us 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

We operate CCTV systems on many of our sites. Please refer to Appendix 5.

19 Changes to this policy

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

21 Complaints relating to this policy

Any complaints relating to this policy should be made in accordance with our Complaints policy.

Appendix 1 - definitions

Term	Definition
Biometric data	is information about a person's physical or behavioural characteristics or features that can be used to identify them and is obtained or recorded for the purposes of a biometric recognition system and can include fingerprints, hand shapes, features of the eye or information about a person's voice or handwriting
Biometric recognition system	is a system that operates automatically (electronically) and • obtains or records information about a person's physical or behavioural characteristics or features; and • compares or otherwise processes that information with stored information in order to establish or verify the identity of the person or otherwise determine whether they are recognised by the system
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 include all living individuals about whom we hold personal data. This includes 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 in our business for our own commercial purposes
Data users	are those of our workforce (including Governors 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, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or Biometric Data
Workforce	Includes, any individual employed by Trust such as staff and those who volunteer in any capacity including Trustees/Members/Local Academy Committee members/parent helpers

Appendix 2 – data breach procedure

In the event of a suspected or identified breach, we will take steps to minimise the impact of the breach and prevent the breach from continuing or reoccurring. Efficient internal management of any breach is required, to ensure swift and appropriate action is taken and confidentiality is maintained as far as possible. This will be led by the Data Protection Lead for each academy.

We will also comply with our legal and contractual requirements to notify other organisations including the Information Commissioners Office ("the ICO") and where appropriate **data subjects** whose **personal data** has been affected by the breach. This includes any communications with the press.

Identifying a data breach

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

This could be the result of a breach of cyber security, such as a hack or virus, or it could be the result of a breach of physical security such as loss or theft of a mobile device or paper records. A data breach includes loss of data and so does not have to be the result of a conscious effort of a third party to access the data. Some examples of potential data breaches include leaving a mobile device on a train, theft of a bag containing paper documents, destruction of the only copy of a document, sending an email or attachment to the wrong recipient, using an unauthorised email address to access personal data or leaving paper documents containing personal data in a place accessible to other people.

Reporting a data breach upon discovery

If any member of our **workforce** suspects, or becomes aware, that a data breach may have occurred (either by them, another member of our **workforce**, a **data processor**, or any other individual) then they must contact the Data Protection Lead (DPL) for their academy immediately. The DPL will in turn immediately contact the Data Protection Officer ("the DPO").

The data breach may need to be reported to the ICO, and notified to **data subjects**. This will depend on the risk to **data subjects**. The DPO must always be consulted in making a decision as to whether to report a data breach to the ICO. Initial investigations will inform as to whether the data breach should be reported.

Investigating a suspected data breach

In relation to any suspected data breach the following steps will be taken by the DPL as soon as possible.

- Actions to minimise the impact of a breach
- An investigation into the breach
- An analysis of what caused the breach and how lessons will be learned.

Appendix 3 – subject access request (SAR) procedure

As we process personal data concerning data subjects, those data subjects have the right to access that personal data under data protection law. A request to access this personal data is known as a subject access request or SAR. A data subject is generally only entitled to access their own personal data, and not to information relating to other people.

Any request by a data subject for access to their personal data is a SAR. This includes requests received in writing, by email, and verbally. In order that we are properly able to understand the nature of any SAR and to verify the identity of the requester, any requester making a request verbally will be asked to put their request in writing.

A SAR will be considered and responded to in accordance with data protection law. The DPL will oversee the response to all SARs.

Verifying the identity of a requester

We are entitled to request additional information from a requester in order to verify whether the requester is in fact who they say they are.

Where we have reasonable doubts as to the identity of the individual making the request, evidence of identity may be established by production of two or more of the following:

- Current passport
- Current driving licence
- Recent utility bill with current address
- Birth/marriage certificate
- P45/P60
- Recent credit card or mortgage statement.

If we are not satisfied as to the identity of the requester then the request will not be complied with, so as to avoid the potential for an inadvertent disclosure of personal data resulting to a data breach.

Fee for responding to requests

We will usually deal with a SAR free of charge. Where a request is considered to be manifestly unfounded or excessive a fee may be requested. Alternatively, we may refuse to respond to the request. If a request is considered to be manifestly unfounded or unreasonable we will inform the requester, why this is considered to be the case.

A fee may also be requested in relation to repeat requests for copies of the same information. In these circumstances a reasonable fee will be charged taking into account the administrative costs of providing the information.

Time period for responding to SAR

We will respond to a SAR within one calendar month. This period will run from the later of

- the date of the request
- the date when any additional identification (or other) information requested is received
- payment of any required fee.

In circumstances where we are in any reasonable doubt as to the identity of the requester, this period will not commence unless and until sufficient information has been provided by the requester as to their identity, and in the case of a third party requester the written authorisation of the data subject has been received (see below in relation to sharing information with third parties).

The period for response may be extended by a further two calendar months in relation to complex requests. What constitutes a complex request will depend on the particular nature of the request.

Where a request is considered to be sufficiently complex as to require an extension of the period for response, we will notify the requester within one calendar month of receiving the request, together with reasons as to why this is considered necessary.

Sharing information with third parties

Data subjects can ask that we share their personal data with another person such as an appointed representative (in such cases you should request written authorisation signed by the data subject confirming which of their personal data they would like you to share with the other person).

Equally if a request is made by a person seeking the personal data of a data subject, and which purports to be made on behalf of that data subject, then a response must not be provided unless and until written authorisation has been provided by the data subject. We will not approach the data subject directly but will inform the requester that we cannot respond without the written authorisation of the data subject.

If we are in any doubt or have any concerns as to providing the personal data of the data subject to the third party, then we will provide the information requested directly to the data subject. It is then a matter for the data subject to decide whether to share this information with any third party.

Personal data belongs to the data subject, and in the case of the personal data of a child regardless of their age the rights in relation to that personal data are theirs and not those of their parents. Parents, in most cases, do not have automatic rights to the personal data of their child.

However, there are circumstances where a parent can request the personal data of their child without requiring the consent of the child. This will depend on the maturity of the child and whether we are confident that the child can understand their rights. Generally, where a child is under 12 years of age they are deemed not to be sufficiently mature as to understand their rights of access and a parent can request access to their personal data on their behalf.

In relation to a child who is 12 years of age or older, then provided that we are confident that they understand their rights, and there is no reason to believe that the child does not have the capacity to make a request on their own behalf, we will require the written authorisation of the child before responding to the requester or provide the personal data directly to the child in accordance with the process above.

In all cases we will consider the particular circumstances of the case, and the above are guidelines only.

Withholding information

There are circumstances where information can be withheld pursuant to a SAR. These are specific exemptions and requests should be considered on a case by case basis.

Where the information sought contains the personal data of third party data subjects then we will consider whether it is possible to redact information so that this does not identify those third parties, taking into account that it may be possible to identify third parties from remaining information.

If this is not possible, we will consider whether the consent of those third parties can be obtained. If consent is refused, or it is not considered appropriate to seek that consent, then we will consider whether it would be reasonable in the circumstances to disclose the information relating to those third parties. If it is not, then the information may be withheld.

So far as possible, we will inform the requester of the reasons why any information has been withheld.

Where providing a copy of the information requested would involve disproportionate effort we will inform the requester, advising whether it would be possible for them to view the documents in

person or seeking further detail from the requester as to what they are seeking, for example key word searches that could be conducted, to identify the information that is sought.

In certain circumstances information can be withheld from the requester, including a data subject, on the basis that it would cause serious harm to the data subject or another individual. If there are any concerns in this regard, then the DPO should be consulted.

Appendix 4 – retention and destruction of data

Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities we will collect, store and process personal data about our pupils, parents, workforce and others. The DPL in each academy is responsible for ensuring that retention and destruction protocols are adhered to.

Retention periods

In line with Article 5(1)(e) of the GDPR the Trust will not retain data for any longer than necessary.

The standard default period for retaining various types of personal data we hold are set out in the Retention Schedule within the Information Management Toolkit for Schools produced by the Information and Records Management Society. This can be found at https://irms.org.uk/general/custom.asp?page=SchoolsToolkit

Destruction procedures

Data will not be kept for any longer than is necessary for the purpose for which it has been collected.

The Retention Schedule within the Information Management Toolkit for Schools also contains direction regarding how data should be disposed of. We will adhere to these recommendations.

Exceptions to destruction procedures

There may be circumstances which prevent us from adhering to the recommendations for data destruction. These include where

- the data is subject to a current Subject Access Request
- there is an ongoing legal action which may require access to relevant data
- there is an ongoing investigation which may require access to relevant data
- the data subject has exercised their right to restrict the processing of the data in accordance with Article 18 of the GDPR
- the data is processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes and we have put in place appropriate technical and organisational measures.

Appendix 5 – CCTV procedures for individual academies

Our academies may use Close Circuit Television ("CCTV") within the premises.

The principles set out below apply to all members of our Workforce, visitors to the Academy premises and all other persons whose images may be captured by the CCTV system.

Purpose of CCTV

Our academies may use CCTV

- to provide a safe and secure environment for pupils, staff and visitors
- to prevent the loss of or damage to buildings and/or assets
- to assist in the prevention of crime and assist law enforcement agencies in apprehending offenders.

Siting of cameras

All CCTV cameras will be sited in such a way as to meet the purpose for which the CCTV is operated. Cameras will be sited in prominent positions where they are clearly visible to staff, pupils and visitors.

Cameras will not be sited, so far as possible, in such a way as to record areas that are not intended to be the subject of surveillance. We will make all reasonable efforts to ensure that areas outside of the academy premises are not recorded.

Signs will be erected to inform individuals that they are in an area within which CCTV is in operation.

Cameras will not be sited in areas where individual have a heightened expectation of privacy, such as changing rooms or toilets.

Privacy Impact Assessment

Prior to the installation of any CCTV camera, or system, a privacy impact assessment will be conducted by academy leaders to ensure that the proposed installation is compliant with legislation and ICO guidance.

We will adopt a privacy by design approach when installing new cameras and systems, taking into account the purpose of each camera so as to avoid recording and storing excessive amounts of personal data.

Management and access

The CCTV system will be managed by a member of the academy leadership team, although it may be operated by other staff on a day-to-day basis. Live and recorded CCTV images will only be viewable by designated individuals and a clear justification established for the accessing of images by any other individuals.

No other individual will have the right to view or access any CCTV images unless in accordance with the guidance below regarding disclosure of images.

The CCTV system will be checked regularly to ensure that it is operating effectively.

Storage and retention of images

Any images recorded by the CCTV system will be retained only for as long as necessary for the purpose for which they were originally recorded, and usually not for more than 28 days.

We will ensure that appropriate security measures are in place to prevent the unlawful or inadvertent disclosure of any recorded images. The measures in place include

- CCTV recording systems being located in restricted access areas
- the CCTV system's being encrypted/password protected
- restriction of the ability to make copies to specified members of staff.

A log of any access to the CCTV images, including time and dates of access, and a record of the individual accessing the images, will be maintained by the Academy.

Disclosure of images to data subjects

Any individual recorded in any CCTV image is a data subject for the purposes of data protection legislation, and has a right to request access to those images.

Any individual who requests access to images of themselves will be considered to have made a subject access request and this will be dealt with as such.

When such a request is made an academy leader will review the CCTV footage, in respect of relevant time periods where appropriate, in accordance with the request.

If the footage contains only the individual making the request then the individual may be permitted to view the footage. This must be strictly limited to that footage which contains only images of the individual making the request. The academy leader must take appropriate measures to ensure that the footage is restricted in this way. A permanent copy of such images may be provided if requested.

If the footage contains images of other individuals then we will consider whether

- the request requires the disclosure of the images of individuals other than the requester, for example whether the images can be distorted so as not to identify other individuals
- the other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained
- it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.

A record will be kept, and held securely, of all disclosures which sets out

- when the request was made
- the process followed in determining whether the images contained third parties
- the considerations as to whether to allow access to those images
- the individuals that were permitted to view the images and when
- whether a copy of the images was provided, and if so to whom, when and in what format.

Disclosure of images to third parties

We will only disclose recorded CCTV images to third parties where it is permitted to do so in accordance with data protection legislation.

CCTV images will only be disclosed to law enforcement agencies in line with the purposes for which the CCTV system is in place.

If a request is received form a law enforcement agency for disclosure of CCTV images then academy leaders will follow the same process as above in relation to subject access requests. Detail will be obtained from the law enforcement agency as to exactly what they want the CCTV images for, and any particular individuals of concern. This will then enable proper consideration to be given to what should be disclosed, and the potential disclosure of any third party images.

The information above must be recorded in relation to any disclosure.

If an order is granted by a Court for disclosure of CCTV images then this must be complied with. However very careful consideration must be given to exactly what the Court order requires. If there are any concerns as to disclosure then the Data Protection Officer should be contacted in the first instance and appropriate legal advice may be required.

Review of these guidelines and CCTV system

These guidelines will be reviewed in line with the review schedule for the Data Protection policy.

The CCTV system and the privacy impact assessment relating to it will be reviewed annually.