GREENWOOD ACADEMIES TRUST

Data Protection Policy

Version 2.0 Status: Approved

Document Owner:	Corporate Affairs Director

Table of Contents

1. Statement of Intent 3
2. Legislation and Definitions 3
3 The Data Controller 3
4 Roles and Responsibilities 3
5. Data Protection Principles 4
6. Fair and Lawful Processing 5
7 Sharing Personal Data 6
8 Subject Access Requests (SARs) 7
9 Other Data Protection Rights of the Individual 8
10 Biometric Recognition Systems 9
11 CCTV 9
12 Photographs and Videos 9
13 Data Protection by Design and Default 10
14 Data Security and Storage of Records 10
15 Disposal of Records 11
16 Personal Data Breaches 11
17 Training 11
18 Monitoring Arrangements and Complaints 11

Appendix 1 Definitions 12
Appendix 2 CCTV 13
Appendix 3 Data Security Breach Procedure 15

1. Statement of Intent

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**. 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.

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. 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.

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. 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.

2. Legislation and Definitions

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)

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

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data. It also reflects the ICO's guidance for the use of surveillance cameras and personal information.

All defined terms in this policy are indicated in bold text, and a list of definitions is included in Appendix 1 of this policy.

3 The Data Controller

We process personal data relating to parents, pupils, staff, governors, visitors and others and we are therefore a data controller. As one legal entity, the Greenwood Academies Trust is the data controller for each of the academies we operate.

We are registered with the ICO as legally required.

4 Roles and Responsibilities

This policy applies to **all staff** employed by the Trust, and to external organisations or individuals working on our behalf.

4.1 Trust Board

The Board has overall responsibility for reviewing this policy and for ensuring that the Trust complies with all relevant data protection obligations. They delegate the responsibility for detailed scrutiny to the Audit and Risk Committee and executive accountability for our data protection practice to the Chief Executive.

4.2 Data Protection Officer

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

They will provide a regular report of their activities directly to the board and, where relevant, report to the board their advice and recommendations on data protection issues.

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

Our Trust Data Protection Officer is Alison Hope (dataprotection@greenwoodacademies.org)
(Andy Gannon will deputise in Alison's absence)

The DPO is line managed by the Corporate Affairs Director but has the right of direct access to the Chief Executive and the Trust Board if required.

4.3 Principals

The Principal acts as the representative of the data controller on a day-to-day basis and is accountable for ensuring this policy is followed within their academy. They will oversee data protection related activity within their own academy, supported by the DPO.

4.4 All Leaders within our Trust

All leaders and line managers are responsible for ensuring that colleagues who report to them are familiar with this policy, engage in training and development activities around data protection and fulfil their obligations within the policy.

4.5 All Colleagues

Anyone who is covered by this policy is responsible for:

- collecting, storing and processing any personal data in accordance with this policy
- informing us of any changes to their personal data, such as a change of address
- contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

5. Data Protection Principles

Our processing of personal data will always comply with the data protection principles. These provide that personal data must be:

- processed fairly and lawfully and transparently in relation to the **data subject**
- processed for specified, lawful purposes and in ways that are not incompatible with those purposes
- adequate, relevant and not excessive for the purpose
- accurate and up to date
- not kept for any longer than is necessary for the purpose
- processed securely using appropriate technical and organisational measures.

Personal data must also:

- be processed in line with data subjects' rights
- not be transferred to people or organisations situated in other countries without adequate protection.

6. Fair and Lawful Processing

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.

For personal data to be processed fairly, data subjects must be aware of:

- the fact that the personal data is being processed
- why the personal data is being processed
- what the lawful basis is for that processing (see below)
- whether the personal data will be shared, and if so, with whom
- the period for which the personal data will be held
- the existence of the data subject's rights in relation to the processing of that personal data
- the right of the data subject to raise a complaint with the Information Commissioner's Office in relation to any processing.

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.

We will only process personal data where we have one of six 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that we can **fulfil a contract** with the individual, or the individual has asked us to take specific steps before entering into a contract
- The data needs to be processed so that we can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual or another person i.e. to protect someone's life
- The data needs to be processed so that we, as a public authority, can **perform a task in the public interest or exercise its official authority**
- The data needs to be processed for our **legitimate interests** (where the processing is not for any tasks we perform as a public authority) or a third party, provided the individual's rights and freedoms are not overridden
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent.**

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

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise or defence of **legal claims**

- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest.

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

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

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law in the form of a privacy notice.

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

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

7 Sharing Personal Data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- there is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- we need to liaise with other agencies – we will seek consent as necessary before doing this
- our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies, payroll, catering or training providers. When doing this, we will:
    - only appoint suppliers or contractors which can provide sufficient guarantees that they comply with UK data protection law
    - establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
    - only share data that the supplier or contractor needs to carry out their service.

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

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

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

8 Subject Access Requests (SARs) (including requests for access to the educational record)

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

- confirmation that their personal data is being processed
- access to a copy of the data
- the purposes of the data processing
- the categories of personal data concerned
- who the data has been, or will be, shared with
- how long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- the right to lodge a complaint with the ICO or another supervisory authority
- the source of the data, if not the individual
- whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- the safeguards provided if the data is being transferred internationally.

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

- the name of the individual
- a correspondence address
- a contact number and email address
- details of the information requested.

All requests for access to the educational record will not be treated as a SAR and will be responded to within 15 school days.

Staff receiving a SAR must notify the DPO immediately.

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children below the age of 13 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our primary academies may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Children aged 13 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our secondary academies may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

When responding to requests, we:

- may ask the individual to provide two forms of identification
- may contact the individual via phone to confirm the request was made
- will respond without delay and within one (1) month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant) or within fifteen (15) days if the request relates solely to the 'educational record'
- will provide the information free of charge
- may tell the individual we will comply within three (3) months of receipt of the request, where a request is complex or numerous; we will inform the individual of this within one (1) month and explain why the extension is necessary.

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

- might cause serious harm to the physical or mental health of the pupil or another individual
- would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or examination scripts

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

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

We will not disclose personal data to third parties (e.g. solicitors) unless we are certain that the request has been authorized by the data subject themselves.

9 Other Data Protection Rights of the Individual

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

- withdraw their consent to processing at any time
- ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- prevent use of their personal data for direct marketing
- object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- be notified of a data breach (in certain circumstances)
- make a complaint to the ICO
- ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10 Biometric Recognition Systems

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

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

Parents/carers and pupils have the right to choose not to use our biometric system(s). We will provide alternative means of accessing the relevant services for those pupils.

Parents/carers and pupils can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

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

Where staff members or other adults use an Academy's biometric system(s), we will also obtain their consent before they first take part in it and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time and the Academy will delete any relevant data already captured.

The same principles will apply to any other system powered by artificial intelligence (AI) in line with GAT's AI protocol.

11 CCTV

We use CCTV in various locations to ensure safety. We will follow the ICO's guidance for the use of CCTV and comply with data protection principles.

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

See Appendix 2 for further information.

12 Photographs and Videos

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

We will obtain written consent from parents/carers, or pupils aged 13 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

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

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

Where an Academy takes photographs and videos, uses may include:

- within an Academy on notice boards and in school magazines, brochures, newsletters, etc.
- outside of school by external agencies such as the school photographer, newspapers, campaigns
- online on our Academy websites or social media pages.

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

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

13 Data Protection by Design and Default

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

- appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- completing data protection impact assessments where the Trust's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- integrating data protection into internal documents including this policy, any related policies and privacy notices
- regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply
- maintaining records of our processing activities, including:
    - for the benefit of data subjects, making available the name and contact details of our Trust and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - for all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure

14 Data Security and Storage of Records

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

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Secure passwords are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment

- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

15 Disposal of Records

Personal data will only be kept for the length of time permitted by our retention schedule, which is contained within our separate Records Management policy.

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

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

16 Personal Data Breaches

We will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 3.

When appropriate, we will report the data breach to the ICO within seventy two (72) hours after becoming aware of it.

17 Training

All those who work within the Trust are provided with data protection training as part of their induction process.

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

18 Monitoring Arrangements and Complaints

The DPO is responsible for monitoring and reviewing this policy.

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

Although you are entitled to complain to the ICO about any matter related to our processing of personal data, we would prefer that you raise it first with us using our Complaints Policy and Procedure.

Appendix 1 Definitions

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: › Name (including initials) › Identification number › Location data › Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: › Racial or ethnic origin › Political opinions › Religious or philosophical beliefs › Trade union membership › Genetics › Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes › Health – physical or mental › Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Appendix 2 CCTV

We operate CCTV in many of our academies and sites. The system comprises a number of fixed and dome cameras. All cameras are monitored from in-school site offices/server rooms and are only available to designated staff – members of the Site Team and members of the Senior Leadership Team (SLT).

The purpose of our CCTV system is:

- to increase the personal safety of staff, pupils and visitors and to reduce the fear of crime
- to protect Trust buildings and their assets
- to support the Police in a bid to deter and detect crime
- to assist in identifying, apprehending and prosecuting offenders
- to protect members of the public and private property.

Our establishments will treat their system and all information, documents and recordings obtained and used, as personal data within the terms of this policy.

Staff have been instructed that static cameras are not to focus on private homes, gardens and/or other areas of private property. They will also not record sound.

Unless an immediate response to events is required, staff must not direct cameras at an individual, their property or a specific group of individuals without authorisation being obtained from the Academy Principal and/or the Data Protection Officer (DPO).

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Recordings will only be released to the media for use in the investigation of a specific crime and with the written authority of the Police. Recordings will never be released to the media for purposes of entertainment.

The Data Protection Officer must be informed in the first instance before any recording can be released.

The planning and design of each CCTV Scheme has endeavoured to ensure that they will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

Warning signs, as required by the Code of Practice of the Information Commissioner have been placed at all access routes to areas covered by the Academy CCTV.

The in-school day-to-day management will be the responsibility of the Academy Principal or his/her nominee and/or the Site Manager during the day and out of hours and at weekends. For Sports Villages, the Centre Manager and/or the Academy Principal or his/her nominee will be responsible during the day and out of hours and at weekends.

The Control Room will only be accessed by 'authorised viewers', a list of whom will be maintained by the Principal. 'Authorised viewers' may only include members of the leadership team, IT support and the site team.

The CCTV system will be operated 24 hours each day, every day of the year. Wherever possible, the CCTV Control Room and the Academy's IT Server Room will be one and the same.

The Academy's Site Manager will check and confirm the efficiency of the system daily and in particular that the equipment is properly recording and that cameras are functional.

Visitors and other contractors wishing to enter the Control Room will be subject to particular arrangements as outlined below.

Control Room Operators must satisfy themselves over the identity of any other visitors to the Control Room and the purpose of the visit. Where any doubt exists, access will be refused. Details of all visits and visitors will be recorded in the Control Room log book.

Casual visits will not be permitted. Visitors must first obtain permission from the Academy Principal or his/her nominee and must be accompanied throughout the visit.

Any visit may be immediately curtailed if prevailing operational requirements make this necessary. If out of hours emergency maintenance arises, the Control Room Operators must be satisfied of the identity and purpose of contractors before allowing entry.

A Visitors' book will be maintained at the Academy's main reception. Full details of visitors including time/date of entry and exit will be recorded.

It is permissible for technology to be installed that will allow images to be visible to 'authorised viewers' on other devices. It is the responsibility of individuals to ensure those devices are kept securely and that images are not viewed while others are present.

Emergency procedures will be used in appropriate cases to call the Emergency Services. Camera surveillance may be maintained at all times. A monitor is installed in each Control Room to which pictures will be continuously recorded.

In order to maintain and preserve the integrity of the disc used to record events from the hard drive and the facility to use them in any future proceedings, the following procedures for their use and retention must be strictly adhered to:

- Each disc must be identified by a unique mark.
- Before using, each disc must be cleaned of any previous recording.
- The Control Room Operator shall register the date and time of disc insert, including tape reference.
- A disc required for evidential purposes must be sealed, witnessed, signed by the Control Room Operator, dated and stored in a separate, secure evidence disk store. If a disc is not copied for the Police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed, signed by the controller, dated and returned to the evidence disk store.
- If the disc is archived the reference must be noted.

Applications received from outside bodies (e.g. Police, Solicitors) to view or release discs must be referred to the DPO in the first instance. In these circumstances, discs will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a Subject Access Request or in response to a Court Order.

Discs may be viewed by the Police for the prevention and detection of crime, authorised officers of the Local Authority for supervisory purposes and/or authorised demonstration and training.

A record will be maintained of the release of discs to the Police or other authorised applicants. Viewing of discs by the Police must be recorded in writing and in the log book.

Should a disc be required as evidence, a copy may be released to the Police under the procedures described in paragraph 8.1 (iv) of this Policy. Discs will only be released to the Police on the clear understanding that the disc remains the property of the Academy and both the disc and information contained on it are to be treated in accordance with this Policy. The Academy also retains the right to refuse permission for the Police to pass to any other person the disc or any part of the information contained thereon. On occasions when a Court requires the release of an original disc, this will be produced from the secure evidence disc store, complete in its sealed bag.

The Police may require the Academy to retain the stored discs for possible use as evidence in the future. Such discs will be properly indexed and properly and securely stored until they are needed by the Police.

Appendix 3 Data Security Breach Procedure

In the event of a breach, it is vital that appropriate action is taken to minimise associated risks.

A data breach is an incident in which any of the types of data specified above is compromised, disclosed, copied, transmitted, accessed, stolen or used by unauthorised individuals, whether accidentally or on purpose. Some examples are:

- Accidental loss or theft of equipment on which data is stored
- Unauthorised access to data
- Human error such as emailing data by mistake
- Failure of equipment and hence data held on it
- Loss of data or equipment through fire or flood, for example
- Hacking attack
- Where information is obtained by deceiving a member of staff.

A personal data breach is a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means a breach is more than just losing personal data.

Any person who realises that a breach may have taken place should first seek to mitigate the breach if possible – for example, by recalling an email sent accidentally or by contacting individuals and asking them to delete inappropriately shared data.

They must also report to the day-to-day lead for data protection (usually the Academy Principal or senior manager in the area of work) and seek advice about any further mitigation measures that may be employed.

They must also report the breach immediately to the Data Protection Officer (DPO) as the primary point of contact. The report should include full and accurate details of the incident, including who is reporting the incident, what type of data is involved, if the data relates to people, how many people are involved. The DPO will keep a log of this information. If a breach occurs out of Academy hours, you must notify the DPO as soon as is reasonably practicable.

The DPO will use the ICO guidance to assess the likely risk of harm from any reported breach. The DPO may suggest further mitigation measures in the case of low risk breaches and will record these in or records.

In the case of a more serious breach with a greater risk of personal harm:

- The DPO may then coordinate a broader team to establish the nature of the breach and any further mitigations to be implemented.
- The DPO will inform the Information Commissioner's Office within seventy-two (72) hours of notification of the breach.
- Notice of the breach will be made to affected individuals to enable them to take steps to protect themselves. This notice will include a description of the breach and the steps taken to mitigate the risks and will be undertaken by the Team.
- The Chief Executive and Deputy Chief Executive will be notified by the DPO following a critical data breach involving large amounts of data or a significant number of people whose personal data has been breached. They, along with the DPO, will make a decision to notify the Trust Board or to inform any external organisation such as the police or other appropriate regulatory body.

Once the breach is contained, a thorough review of the event will be undertaken by a team led by the DPO to establish the cause of the breach, the effectiveness of the response and to identify areas that require improvement.

Recommended changes to systems, policies and procedures will be documented and implemented as soon as possible thereafter.