GREENWOOD ACADEMIES TRUST

# Data Protection Policy

Version: 1.0 Approval Status: Approved

| | |
|---|---|
| Document Owner: | Graham Feek |
| Classification: | External |
| Review Date: | 21/05/2020 |
| Reviewed: | 21/5/2018 |

# Table of Contents

## Definitions

| | |
|---|---|
| Automated data | Data which is processed by means of equipment operating automatically (e.g. by computer) or which is recorded with the intention that it should be so processed. |
| Biometric data | Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data. |
| Consent | Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. |
| Data | Information which is processed automatically or recorded manually. |
| Data Controller | The natural or legal entity which determines the purposes and means of processing personal data. The Trust Data Controller is the Greenwood Academies Trust. |
| Data Subject Access Request | A request by a Data Subject for details of the personal data held about them. |
| Data Subject | A natural person whose personal data is processed by a controller or processor. |
| Data Protection Officer | A Data Protection Officer (DPO) is a leadership role required by the General Data Protection Regulation (GDPR) and is responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements, acting as an independent advocate. The Trust DPO is Alison Hope, Trust Governance Manager. |
| Data User | Someone who controls the collection, holding, processing or the use of data. |
| Explicit consent | Explicit consent is that which must be affirmed by the individual in an informed, clear and specific statement, preferably in writing, specifying the purposes for which the particular types of sensitive personal data may be used and/or the countries to which they may be disclosed. |
| Personal data | Any information relating to an identified or identifiable natural person ('data subject') that can be used to directly or indirectly identify that person. |
| Personal Data Breach | A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. |
| Privacy Impact Assessment | A PIA is a process to help organisations identify, assess and mitigate or minimise privacy risks with data processing activities – for example, the launch of a new product or the adoption of a new practice or policy or system. |
| Privacy Notice | A statement made to a data subject that describes how the organisation collects, uses, retains and discloses personal information. |
| Process/processing | Any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, including collection, recording, organisation, structuring, storage, erasure or destruction. |
| Sensitive personal data | Information concerning a data subject's racial or ethnic origin, political opinions, religious or philosophical beliefs , trade union activities, physical or mental health or condition, sexual life or orientation, genetic data or biometric data. |

## Introduction

This document sets out the Trust's and it's Academies' responsibilities under the General Data Protection Regulation (GDPR) 2018 ("the Regulation") and provides guidance on the maintenance of and access to data, including employment and educational records in accordance with the provisions of the Regulation.

It is important all staff read and have an understanding of this policy; this will form part of the staff induction programme.

We also have the following suite of data protection policies available on Sharepoint for your reference.

- Biometric Data Policy
- CCTV Policy
- Data Subject Access Request Procedure
- Data Security Breach Procedure (*at the back of this policy*)
- E-Safety Policy Statement
- E-Safety Procedure
- Freedom of Information Policy and Procedure
- Freedom of Information Publication Scheme
- Trust Media Protocol
- Privacy Policy (*Pupils and Parents*)
- Privacy Policy *(Staff)*
- Records Management Policy

## 1. The General Data Protection Regulation (GDPR)

The **GDPR** (Regulation (**EU**) 2016/679) is a binding, legislative regulation by which the **European** Parliament, the Council of the **European** Union and the **European** Commission intend to strengthen and unify data protection for all individuals within the **European** Union (**EU**). The Regulation came into force on 25 May 2018 and replaces the Data Protection Act 1998, with many of the main concepts and principles remaining the same but with new elements and significant enhancements added.

The Regulation provides that:

- anyone who records and uses personal information (data controllers/users) must be open about how the information is used and must follow the six principles of 'good information handling'.
- all individuals (data subjects) have the right to see information that is held about them and the right to rectification if incorrect.
- The Regulation applies to all electronic records that contain information about living and identifiable individuals and extends data protection to manual files where the personal data of a data subject is readily accessible (a structured filing system).
- The main aim of the Regulation is to protect data from unnecessary, unauthorised or harmful use and to provide individuals with some control over the use of their personal data. Individuals have the right to take action for compensation caused by inaccurate, lost or destroyed data or unauthorised disclosure of information. They also have the right to complain to the Information Commissioner who may serve an enforcement notice and, in some circumstances, impose a financial penalty.

### 1.2 Notification

The Greenwood Academies Trust is registered with the Information Commissioner's Office (ICO) as data controller for all Trust and Academy data. The Trust Governance Manager is responsible for maintaining the record with the ICO.

Academy Principals and Central Team staff must advise the Trust Governance Manager if there are any changes to the use of personal data that are not covered by the Trust registration.

## 2. Principles of Data Protection

In collecting, using, storing and disposing of data, the Trust or Academy will comply with the requirements of the Regulation that govern the processing of personal data. Under these requirements, the information will be collected and used fairly, stored safely and not disclosed to any other person where to do so would be in breach of those requirements or would otherwise be unlawful.

The Trust will maintain documentation of the key data it holds, the systems for processing that data and the consents that are required to enable the processing.

All Trust staff who process or use personal information will ensure they comply with the following six data protection principles which are laid out in the GDPR Regulation. Article 5 of the Regulation requires that personal data shall be:

2.1 **Principle 1:** Processed fairly, lawfully and in a transparent manner in relation to the data subject

The collection and disclosure of data is subject to scrutiny and is only 'lawful' if it meets at least one of the following criteria:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes[1];

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

For clarification in point (e), the Trust considers the following to be in the public interest and therefore consent forms are not considered necessary:

- Pupil details – name/DOB/address/SEN needs/allergies/health data etc
- Parent details – names/contact information/address/relationship to pupil etc
- Staff details – names/addresses/contact information/salary/contracts/next of kin
- Behaviour – assessments/census data etc
- General school business – attendance/lesson planning/contact with parents etc
- Pupil images – for use in Academy management systems and for monitoring or educational uses eg, curriculum subjects requiring video and photographs to be submitted to external examiners.

*[1] Where point (a) of Principle 1 applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.*

The Trust also has a Data Sharing Agreement with relevant Local Authorities through an automated and secure data exchange process. This is central to the success of integrated working across Trust Academies and the LA MIS systems, thus maintaining reliable and accurate pupil and school records.

Point (f) shall not apply to processing carried out by public authorities in the performance of their tasks.

- When personal data is collected then a Privacy Notice will be prepared and published on the Trust website that states:
  - the identity of the organisation in control of the processing
  - the purpose, or purposes, for which the information will be processed
  - any further information necessary, in the specific circumstances, to enable the processing in respect of the individual to be fair

In addition to the requirements outlined above, Sensitive Personal Data may only be processed if the processing also meets at least one of the following criteria:

- The data subject has given explicit written or electronic consent
- It is necessary to meet requirements of employment and social protection law
- It is necessary to protect the vital interests of the data subject or another natural person where the data subject is physically or legally incapable of giving consent
- The data subject has already made the information public
- It is necessary for the exercise or defence of legal claims or whenever courts are acting in their judicial capacity
- It is necessary for reasons of public interest in the area of public health
- It is necessary for medical purposes
- It is necessary for archiving purposes in the public interest
- It is necessary in order to comply with legislation from the Secretary of State

2.2 **Principle 2:** Collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

- Personal data will be obtained only for one or more specified and lawful purpose.
- Data will not be further processed in any manner incompatible with the initial specified purpose or those purposes for which it was obtained as specified in the Privacy Notice.

2.3 **Principle 3:** Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

- Data must be adequate, relevant and not excessive.
- Personal information which is not necessary for the intended processing must not be acquired i.e. personal information cannot be collected just because ‘it may be useful’. Only the minimum information required for the purposes for which it is obtained should be held.

2.4 **Principle 4:** Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

The Trust or Academy must ensure that there is a system in place to review data for accuracy and to ensure it is up to date. Procedures must be in place to make any amendments requested by a data subject or a record kept if the amendment is not considered appropriate.

2.5 **Principle 5:** Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals

Data must not be kept for longer than required for the purpose for which it was obtained. The Trust or Academy must regularly review data held in order to assess whether information is still required in accordance with the Trust Record Management Policy.

Before disposing of any data (physical or electronic), the data user must ensure he/she has consulted the Record Management Policy to ensure the data is disposed of in the correct manner.

2.6 **Principle 6:** Processed in a manner that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

A data subject (including a member of staff) has the right to object to data processing relating to them which is likely to cause substantial and unwarranted damage or distress to that data subject or another person. There are a number of provisos to this right. Data subjects must make such a request in writing and, where their request is refused, can apply to the Court for an order. All requests and Court orders must be managed by the Trust Governance Manager and, where applicable, the respective individual at the Academy.

The Trust and the Academy must guard against unauthorised and unlawful processing (e.g. access, alteration, disclosure or disposal). Appropriate security records must be kept in order to provide an audit trail of any disposal of personal data. Personal information will, so far as possible, be:

- kept in a locked filing cabinet, or
- in a locked drawer; or
- if it is computerised, be password protected, or
- kept only on disk or other media which is encrypted.

When personal data is to be destroyed, paper or microfilm records will be disposed of by shredding or incineration. Data on computer hard disks or other magnetic media will be destroyed using a recognised supplier and destruction certificates obtained and retained. Optical media is to be shredded. Please refer to the Trust's Record Management Policy.

The Data Controller shall be responsible for, and shall be able to demonstrate, compliance with the above principles.

## 3. Transfer of Information outside the European Economic Area (EEA)

Personal data shall not be transferred outside of the EEA unless that country or territory ensures an adequate level of protection. Certain countries/territories have been certified as providing an adequate level of protection. Where it is proposed to transfer to a country/territory that has not been certified, the Data Controller must satisfy itself that the country/territory affords an adequate level of protection.

If the data is to be transferred to a country or territory that does not have adequate protection, then the Trust Governance Manager must approve the transfer and this approval will only be granted if it can be demonstrated that there is a legal basis for the processing (as described in section 2.1 of this document).

## 4. Individuals' Rights

The GDPR provides the following rights for individuals:

4.1. The right to be informed

This right encompasses the Trust's obligation to provide 'fair processing information', typically through a privacy notice. Each Academy will publish a Privacy Notice on their website and have a copy available at the Academy reception.

4.2. The right of access

Under the GDPR, individuals have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information (largely provided in a privacy notice)

Subject Access Requests are covered in Section 5 of this policy and all such requests should be directed to the Trust Governance Manager.

4.3. The right to rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete and to block future processing in cases of unlawful/unfair processing. Data subjects must make such a request in writing and, where their request is refused, can apply to the Court for an order for rectification/erasure. All requests will be managed by the Trust Governance Manager.

4.4. The right to erasure

Also known as the 'right to be forgotten'. This is to enable an individual to request the deletion or removal of personal data in specific circumstances where there is no compelling reason for its continued processing. All requests must be made in writing to the Trust Governance Manager.

4.5. The right to restrict processing

Individuals have the right to block or suppress processing of personal data. The Trust is permitted to store the personal data when processing is restricted but not further process it.

4.6. The right to data portability

This allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows moving, copying or transferring personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

The right to data portability only applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

4.7. The right to object

Individual have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority
- direct marketing
- processing for purposes of scientific/historical research and statistics.

4.8. Rights in relation to automated decision making and profiling.

The Trust does not carry out any processing operations that constitute automated decision making.

## 5. Responsibilities

5.1 The Trust Board

The Trust Board has responsibility for:

- Approving and reviewing this policy via delegation to the People Committee
- Ensuring the implementation of the Regulation, its policies, procedures and practices via delegation to the Chief Executive and Deputy Chief Executive

5.2 The Chief Executive and Deputy Chief Executive

Through delegation from the Trust Board, ensuring the implementation of the Regulation, this policy and the supporting processes, including:

- Ensuring that appropriate training takes place for all staff.
- Ensuring that complaints about the handling of personal data are investigated and dealt with effectively

5.3 The Data Protection Officer (DPO)

The role of the DPO is:

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.

- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees etc).
- To coordinate annual training for all staff and coordinate with Trust Directors for training in their areas.

The Trust DPO is Alison Hope, Trust Governance Manager. The DPO functionally reports to the Finance Director.

To provide for the independence of the Data Protection function, the DPO has a direct right of access to the Chair of the Trust Board and the Chief Executive, to whom all significant concerns relating to data protection and the GDPR are reported.

5.4 The Trust Governance Manager

The Trust Governance Manager is responsible to the Trust Board to ensure that:

- the Trust and its Academies are appropriately registered with the Information Commissioner's Office. It is the responsibility of the Trust Governance Manager to affect the registration and ensure that any changes required to the registration are implemented.
- this policy is implemented in the Trust and Academies' procedures and practices.
- the processes for managing complaints, Subject Access Requests and Freedom of Information requests are properly managed.
- this policy is brought to the attention of all employees, data subjects and that all staff, including temporary, volunteer, supply and agency personnel, receive appropriate training.
- good practice is encouraged by all staff and any breaches of the Regulation and this policy are dealt with appropriately. Refer to the Greenwood Academies Trust Data Security Breach Procedure section for further information.
- advice and guidance on the aspects of current data protection legislation are provided.

5.5 Central Team Directors

Each Director is responsible for:

- Documenting data records and processes for their individual areas.
- Ensuring staff training and awareness in data protection for their individual areas, supported by the DPO.

5.6 Academy Principals

Academy Principals have overall responsibility and are held accountable but may delegate to a member of their Senior Leadership Team.

Academy Principals are responsible for:

- Ensuring this policy is implemented in Academy procedures and practices.
- Ensuring the associated GAT policies and procedures governing the use, storage and disposal of data are adhered to and reporting any variances to the Trust Governance Manager.
- Ensuring positive engagement in staff training.
- Ensuring the Academy completes a Privacy Notice and displays it on their website.

- Ensuring staff carry out Privacy Impact Assessments if wishing to purchase new software or systems. IT must be contacted.

5.7 All Staff

All staff have a duty to observe and follow the principles of the GDPR Regulation. These guidelines are intended to assist staff to understand the aims and principles of the Regulation and to set out the main areas in which staff are likely to be affected by data protection issues in the course of their work.

All staff must participate in the online data protection training and complete the model within the agreed timeframe. Records of completion will be kept for logging purposes. Staff must ensure they understand how their work is affected by the Regulation and abide by the principles of the Regulation when processing any personal data. All staff must assess the information used in the course of their work and their responsibility for any personal data. All personal data collected should be factually accurate and relevant. Staff must respect that all sensitive data must be kept confidential and that any breaches of that confidentiality may result in legal action or a possible fine.

All staff must be aware of and ensure that they comply with this Policy. Consequences of non-compliance may include appropriate disciplinary or legal action being taken against the Trust, the Academy and/or the member of staff. A fine could be imposed and reputational loss could ensue as consequences of any negative publicity, particularly if a complaint is made to the ICO or an individual makes a claim for compensation against the organisation.

All contractors and volunteers employed by the Greenwood Academies Trust who have access to personal data are required to comply with this policy and its supporting policies as specified in the Data Protection schedule of their contract.

## 6. Access to Information

All individuals about whom the Trust or Academy holds personal information have the right to access information that relates to them, whether it is held electronically or in manual form.

A data subject is entitled to request a copy of the information related to her/him which will be supplied by the Trust or Academy unless the supply is not possible or would involve disproportionate effort.

The right of access extends to children and young people who understand what it means to exercise that right.

The GDPR states that, if consent is the basis for processing a child's personal data, a child under the age of 13 cannot give that consent themselves and instead, consent is required from a person holding 'parental responsibility'.

The Trust/Academy will comply with Freedom of Information Requests as defined in the Greenwood Academies Trust Freedom of Information Procedure.

For Subject Access Requests for personal information, the Trust/Academy will ensure that requests for access are dealt with within the timescale specified by legislation. The Trust's Data Subject Access Request Procedure provides detailed guidance about how requests should be dealt with.

All requests must be forwarded to the Trust Governance Manager for processing in the first instance.

Any person wishing to exercise their right of access should obtain a copy of the above procedures by writing to the Trust or Academy or by visiting the Trust or individual Academy websites.

## 7. Records Management

In order to fully understand and manage the information held by the Trust, in order to protect it and be able to exploit its potential, an Information Asset Register (IAR) will be implemented as a simple way to manage the organisation's assets and the risks to them.

Through its Record Management Policy, the Trust will ensure the systematic management, use and disposition of all records and the information they contain throughout their lifecycle. Effective records management ensures that a body of reliable evidence can be called upon by the Trust if required to justify any actions, or defend its position and to demonstrate its accountability and good standards of corporate governance.

## 8. Disclosure of Personal Data

The following attempts to illustrate when personal data can be disclosed. This list is not exhaustive and, if further guidance is required, staff should contact the Trust Governance Manager.

### 8.1 Staff Who Need to Know

Access to personal data will be provided to members of staff who need to know it in order to carry out their normal duties. However, only access to the data that is required will be provided.

### 8.2 Purposes Specified

Data will only be disclosed for use for the purposes specified when it was collected and any additional purpose of which the data subject has been notified. Any other use amounts to unlawful processing. For example, if information has been collected in order to pay school uniform grants in previous years, the Academy will not be allowed to use that information as a mailing list for a library service without having first notified the data subjects of the intention to do so and given data subjects the opportunity to opt out of such processing.

### 8.3 Specific Agreement of Data Subject

Data subjects should be made aware, via the relevant Privacy Notice, that their personal data may be disclosed to various third parties, without needing specific consent, during the normal course of business activities. Data may be used for other purposes such as Ofsted Inspections or other governmental/regulatory activity, accounting and statistical analysis, Internal and External Audit and also to prevent or detect fraud or other crimes for example. In all other cases, data will only be disclosed to a third party if the data subject has given specific consent, ideally in writing.

### 8.4 Telephone Enquiries/ Home Addresses and Telephone Numbers

Requests from third parties are often made by telephone, giving the added problem of verifying the identity of the caller. Even when the call appears to be genuine, personal data must not be disclosed (save where necessary for one of the purposes mentioned above and where the identity of the caller, purpose of the enquiry and proposed use of the information have been verified).

Where appropriate, the caller will be asked to put their request in writing or an offer will be made to contact the data subject concerned, on behalf of the caller and pass on any message.

Home addresses or personal telephone numbers of staff or other data subjects must not be given out to third parties unless the individual has given permission to do so.

Alternative approaches include taking the caller's contact details and advising that a message will be passed on requesting that the caller is contacted, or offering to forward correspondence to a pupil or a member of staff on behalf of the caller.

It is important to take care when handling such requests. An individual's pupil/staff status is personal data. The Trust or Academy should be careful to neither confirm nor deny that the person is a pupil or member of staff at the Academy or that the person is otherwise known to the Trust or Academy.

8.5 The Police

Disclosures to the Police are not compulsory except in cases where the Trust or Academy is served with a Court Order requiring information. Requests from the Police for access to information must be made, in writing, from one of the Constabulary's Data Protection officers. In cases where the Trust or Academy has not been served with a Court Order but receives a request, consideration must be given to the implications of disclosure before any action is taken and to the nature of the information sought and the reasons for the request. Advice should be sort from the Trust Governance Manager.

The Trust or Academy may be required to provide an explanation for any disclosure of the Data Subject's personal information at a later date and must be able to provide justifiable reasons for doing so, for example where the Trust or Academy believes that failure to release the information would prejudice a criminal investigation. In such cases the Trust Governance Manager must make a clear and accurate record of the circumstances, the advice sought and the decision making process followed so that there is clear evidence of the reasoning and the prevailing circumstances. The GDPR Regulation allows organisations to disclose personal data where necessary relating to criminal convictions and offences under the control of official authority or when processing is authorised by state law providing for appropriate safeguards for the rights and freedoms of data subjects.

8.6 Education Records

All requests for the data held in Education Records by pupils or parents/legal guardians are treated as a Data Subject Access Request and must be cleared by the Trust Governance Manager and the Academy Principal.

All requests for data from third parties must conform to the principles of the GDPR Regulation and must be covered with a Data Sharing Agreement. All Data Sharing Agreements taken out by the Trust or Academy must undergo a Privacy Impact Assessment as defined in the Greenwood Academies Trust Privacy Impact Assessment guidance and the results of the assessment to be kept on file with the Data Sharing Agreement.

8.7 Examination Results

The Academy must ensure that strict confidentiality and secure office practices are followed while papers, including examination coursework, are being marked and while results are being compiled.

The GDPR Regulation does not give pupils the right to access their own examination scripts but it does allow access to comments made upon them by examiners. However, pupils are able, under subject access rights, to see the breakdown of marks awarded for particular questions or sections of examinations.

Examination marks should not be shared, either verbally or in writing, with any other person unless the individual pupil has given their permission e.g. the displaying of examination results on a Academy notice board or a list sent around the classroom is prohibited. Exceptions are other Trust or Academy staff relevant to their role, Ofsted and the DfE.

8.8 E-mail Addresses

Personal email addresses must not be disclosed for non-work purposes. If asked to disclose another member of staff's personal email address, the caller can be asked to give her/his email address and told that it will be passed on to the individual s/he is trying to contact 'if' she/he is a member of the Trust or Academy. It is not appropriate to disclose a colleague's work email details to someone who claims she/he wishes to contact her/him regarding a non-work related matter.

8.9 Photographs and Films

Where it is wished for photographs to be taken or film recordings to be made of staff and/or pupils, as individuals, as small groups or organised groups, the individual(s) concerned must give their consent and be informed of the purpose(s) for which the information is to be used. For pupils under the age of 13, a Trust consent form ('Photographs and Films – How we use your information') is given for completion by parents in all Trust Academies at the point of entry. If this form is not completed and returned to the Academy, it is assumed the Trust/Academy does not have consent to photograph or film that pupil. Even if the Trust/Academy *does* receive consent, we will not photograph or film a pupil if they do not wish to take part on the day.

Once a pupil reaches the age of 13, under Regulation guidelines, consent will be sought from them personally.

For general photographs or video recordings of the Academy grounds and public places, whereby individuals cannot be identified, consent is not required.

A parent may change their mind about consent, even after signing the above consent form but they must inform the Academy that they wish to withdraw their child from photographs or filming. Likewise, a pupil aged 13 or over may change their mind about consent but must inform the Academy.

Photos/films of pupils may be kept and used after a pupil has left an Academy but only for the original purpose(s) stated in the signed consent form. If the Trust wish to use photos / films for a different purpose to that which was originally explained to the pupils in question, renewed consent will need to be sought, regardless of whether or not the pupil is still at the Academy.

Parents are reminded that, if they attend an Academy event, they should only take photographs of or film their own child(ren) unless they seek the consent of other children's parents/guardians.

All images will be stored securely and safely and Academies will be expected to delete images after a reasonable time has passed.

Please refer to the Trust Media Protocol for further information.

8.10 CCTV

The Academy must ensure any recorded images are stored securely and in a location/on a medium where only authorised persons have access to them. The recorded images must only be retained long enough for any incident to come to light (e.g. for a theft to be noticed). The Academy may disclose recordings to a law enforcement agency in order to help with the prevention or detection of crime but must not release the images to any other third party.

Further guidance on the use of CCTV can be found in the Trust CCTV policy and on the Information Commissioners website under 'Topic guides for organisations':

http://ico.org.uk/for_organisations/data_protection/topic_guides

8.11 Equal Opportunities Monitoring

The GDPR Regulation specifically allows for processing of data on racial or ethnic origin, religion and disability if it is necessary for keeping under review the existence, or absence, of equality of opportunity. The collection of this information is exclusively used for the statistical evaluation of the Trust's equal opportunities policy within recruitment and employment.

The Trust, where possible, will ensure anonymity of information when meaningful monitoring is required. The equal opportunities monitoring form, which collects information for this purpose, must be removed from all applications before any assessment of suitability for the post is considered.

8.12 Websites

Data placed on the Trust's or an Academy's website and made available via the Internet will be available in countries which do not have a data privacy regime considered adequate by the EU. Where the Trust or Academy wishes to make staff/pupil personal data available in this way, the consent of the staff and/or pupil(s) concerned must be obtained. Consent can be withdrawn at any point.

Website pages are sometimes used to collect personal data such as names and addresses of individuals who request Trust or Academy information e.g. from those who are registering to attend an Open day. The relevant web page should indicate the purpose or purposes for which the data is collected, the recipients to whom it may be disclosed and an indication of the time period for which it will be kept (e.g. "while we process your application", rather than a specific date).

All sites that collect information from site visitors must provide a Privacy Statement. The purpose of this statement is to help individuals to decide whether they want to visit the site and, if so, whether to provide any personal information. Privacy Statements must be prominently displayed.

The above does cover all requirements and consideration must be given to the intended audience and the use their data may be put to deliver Trust obligations. All Privacy Statements need to be reviewed by the Trust Governance Manager before they are published.

## 9. Monitoring and Review

The Data Protection Officer will report to the Trust Board, via the People Committee, on any relevant aspects of the working of this policy (including non-compliance) as appropriate.

# Data Security Breach Procedure

## Introduction

The Trust holds a large amount of data / information, both in hard and soft copy. This includes personal or confidential information (about people) and also non-personal information which could be sensitive or commercial, for instance financial data.

Care should be taken to protect this type of data / information to ensure it is not changed (either accidentally or deliberately), lost, stolen or falls into the wrong hands and that its authenticity and integrity is maintained.

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

### 1. What is a Breach?

1.1 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.

### 2. Reporting the Breach

2.1 Data security breaches should be reported immediately to the Service Desk 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 Service Desk will keep a log of this information. If a breach occurs out of Academy hours, you must notify the Service Desk as soon as is physically possibly.

The Service Desk contact details are:

**Email:** servicedesk@greenwoodacademies.org

**Tel:** 0115 748 3370 or 5050 internal dial

You must also notify your Principal immediately.

### 3. Investigation and Risk Assessment

3.1 The IT Director will instigate a Computer Emergency Response Team (CERT), who will be responsible for investigating data breaches. An investigation will be started within 24 working hours of the breach being discovered.

Depending on the type of breach, CERT team members may consist of:

- IT Director
- Technical Services Manager
- Service Delivery Manager
- Trust Governance Manager/Data Protection Officer
- Data Owner
- Data Users
- Central Team Directors

3.2 The investigation will establish the nature of the breach, the type of data involved, whether the data is personal data relating to individuals and, if so, who are the subjects and how many are involved.

3.3 The investigation will consider the extent of the sensitivity of the data and a risk assessment performed as to what might be the consequences of its loss, for instance whether harm could come to individuals or to the institution.

3.4 On completion of the investigation, a report will be completed within ten (10) working days.

## 4. Containment and Recovery

4.1 The Team will determine the appropriate course of action and the required resources needed to limit the impact of the breach. This might require isolating a compromised section of the network, alerting relevant staff or shutting down critical equipment.

4.2 Appropriate steps will be taken to recover data losses and resume normal business operation. This might entail attempting to recover any lost equipment, using backup mechanisms to restore compromised or stolen data and changing compromised passwords.

4.3 Advice from experts across the Trust may be sought eg, the Trust Governance Manager, Director of Human Resources, Education Director.

## 5. Notification

5.1 The Chief Executive and Deputy Chief Executive will be notified by the CERT Team following a critical data breach involving large amounts of data or a significant number of people whose personal data has been breached. They will make a decision to notify the Trust Board based on the seriousness of the breach.

5.2 The Chief Executive and/or Deputy Chief Executive will make a decision to inform any external organisation such as the police or other appropriate regulatory body.

5.3 If a personal data breach has occurred, the Trust Governance Manager must be informed. They must inform the Information Commissioner's Office within seventy two (72) hours of notification of the breach.

5.4 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.

## 6. Review

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

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