# DATA PROTECTION AND FREEDOM OF INFORMATION POLICY

Approved By: Trust Board
Approval Date: October 2024

## CONTENTS

## 1. INTRODUCTION AND AIMS

The Girls' Learning Trust ('the Trust') aims to ensure that all personal data collected about staff, students, parents, carers, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law. This policy applies to all personal data, regardless of whether it is in paper or electronic format.

The Trust processes personal data relating to parents and carers, students, staff, governors, visitors and others, and therefore is a data controller. The Trust is registered with the ICO.

## 2. LEGISLATION AND GUIDANCE

This policy meets the requirements of the:

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

The policy is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the Department for Education (DfE) on generative artificial intelligence in education.

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

The policy complies with our funding agreement and our articles of association.

The policy should be read in conjunction with the following other relevant policies:

- Safeguarding and Child Protection Policy
- IT Policy
- Data and Records Retention Policy
- CCTV Policy
- Staff Code of Conduct

## 3. DEFINITIONS

| Term | Definition |
|---|---|
| Personal data | Any information relating to an identified, or identifiable, living individual. This may include the individual's:<br><br>▪ Name (including initials)<br>▪ Identification number<br>▪ Location data<br>▪ Online identifier, such as a username<br><br>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<br>▪ Political opinions<br>▪ Religious or philosophical beliefs<br>▪ Trade union membership<br>▪ Genetics<br>▪ Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes<br>▪ Health – physical or mental<br>▪ 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 natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. |
| Data processor | A natural or legal person, public authority, agency or other body which processes personal data on behalf of the 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. |

## 4. DATA PROTECTION PRINCIPLES

The UK GDPR is based on data protection principles that our Trust must comply with. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed.
- Accurate and, where necessary, kept up to date.
- Kept for no longer than is necessary for the purposes for which it is processed.
- Processed in a way that ensures it is appropriately secure.

## 5. DATA PROTECTION BY DESIGN AND DEFAULT

We will implement comprehensive measures to demonstrate that data protection is integrated into all our data processing activities, including:

- Appointing a DPO: a suitably qualified Data Protection Officer (DPO) will be appointed, equipped with the necessary resources to fulfil their duties and maintain their expert knowledge.
- Processing Necessity: we will only process personal data that is necessary for each specific purpose, always adhering to the data protection principles established by relevant laws.
- Data Protection Impact Assessments: these will be completed whenever our processing activities present a high risk to individuals' rights and freedoms, and when introducing new technologies.
- Policy Integration: data protection will be integrated into all internal documents, including this policy, related policies, and privacy notices.
- Staff Training: we will provide regular training for staff on data protection law, this policy, related policies, and other relevant matters, and maintaining records of attendance.

- Reviews and Audits: regular reviews and audits will be conducted to test our privacy measures and ensure compliance.
- Safeguards for Data Transfers: appropriate safeguards will be implemented if we transfer any personal data outside of the UK, ensuring compliance with differing data protection laws.

Maintaining records of our processing activities:

- For the benefit of data subjects, making available the name and contact details of our school 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.

## 6. ROLES AND RESPONSIBILITIES

This policy applies to all staff, governors and trustees, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Trust Board

The Trust Board has overall responsibility for ensuring our compliance with all relevant data protection obligations.

Data Protection Officer (DPO)

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. Specific responsibilities include:

- Monitoring Compliance: to ensure the organization complies with data protection laws and internal policies, conducting regular audits and reviews.
- Advising on Data Protection: to provide guidance on data protection impact assessments and other compliance activities, including advice on new projects and technologies.
- Training and Awareness: To educate staff on data protection principles and policies, conducting regular training sessions and maintaining records of attendance.
- Point of Contact: To act as the primary contact for data subjects and regulatory authorities regarding data protection matters, addressing concerns and handling data breach notifications.
- Policy Development: To assist in the creation and maintenance of data protection policies and procedures, ensuring they are up-to-date and effective in safeguarding personal data.

They will provide an annual report of their activities directly to the Trust board and, where relevant, report to the board their advice and recommendations on school data protection issues.
The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

The DPO for the Trust is appointed by Trust Board on a recommendation from the Chief Executive Officer.

The DPO is responsible for monitoring and reviewing this policy. This policy will be reviewed annually and approved by Trust Board.

Data Protection Lead

The Data Protection Lead for the Trust (who may also be the Data Protection Officer) is the operational lead for the policy. Specific responsibilities include:

- Implementing Policies: to develop and enforce data protection policies and procedures, ensuring they align with legal requirements and organizational needs.
- Managing Data Protection Activities: to oversee day-to-day data protection operations, including data handling practices, compliance checks, and risk assessments.
- Coordinating with the DPO: to work closely with the Data Protection Officer to ensure consistent application of data protection laws and address any issues or concerns.
- Training and Support: to provide support and training to staff on data protection issues, ensuring that they understand and adhere to relevant policies and procedures.
- Handling Data Requests: to manage and respond to data subject access requests, data breaches, and other data protection inquiries, ensuring timely and accurate resolution.

All staff

All staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address

All staff are responsible for contacting the DPO in the following circumstances:

- If they have any questions about the operation of this policy, data protection law, the retention of personal data, or the security of personal data.
- If they have any concerns that this policy is not being followed.
- If they are unsure whether they have a lawful basis to use personal data in a particular manner.
- If they need to obtain or record consent, draft a privacy notice, address data protection rights exercised by an individual, or transfer personal data outside the UK.
- If there has been a data breach.
- If they are engaging in a new activity that may impact the privacy rights of individuals.
- If they need assistance with contracts or sharing personal data with third parties.

## 7. COLLECTING PERSONAL DATA

7.1 Lawfulness, Fairness and Transparency

We will only process personal data where we have reason to do so under data protection law:

- The data needs to be processed so that the school can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract.
- The data needs to be processed so that the school can comply with a legal obligation.
- The data needs to be processed to ensure the vital interests of the individual or another person e.g. to protect someone's life.
- The data needs to be processed so that the school, as a public authority, can perform a task in the public interest or exercise its official authority.
- The data needs to be processed for the legitimate interests of the school (where the processing is not for any tasks the school performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden.
- The individual (or their parent/carer when appropriate in the case of a student) 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 student) 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 student) 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. This would be determined by the DPO with consideration to the Mental Capacity Act 2005 and other statutory guidance.
- The data has already been made manifestly public by the individual.
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights.
- The data needs to be processed for reasons of substantial public interest as defined in legislation.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law. We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect or use personal data in ways which have unjustified adverse effects on them.

7.2 Limitation, Minimisation and Accuracy

We will only collect personal data for specified, explicit, and legitimate reasons. We will explain these reasons to the individuals when we first collect their data. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs. We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate. In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Trust's record retention schedule.

## 8. SHARING PERSONAL DATA

We generally do not share personal data without consent. However, there are specific circumstances where sharing may be necessary, including:

- Safety Concerns: if there are issues involving a student or parent/carer that pose a risk to their safety, we may need to share relevant data.
- Agency Liaison: when liaising with other agencies, we will seek consent as required before sharing personal data.
- Service Providers: we may share appropriate data with suppliers or contractors (e.g., IT companies) to facilitate the delivery of services to our staff and students.

In these cases, we will:

- Select Compliant Partners: choose suppliers or contractors that guarantee compliance with UK data protection law.
- Establish Contracts: create agreements to ensure any shared data is processed fairly and lawfully.
- Limit Data Sharing: share only the data necessary for the supplier or contractor to perform their services.

We will also share personal data with law enforcement and government bodies when legally required and with emergency services and local authorities to assist in emergency situations involving our students or staff.

For international data transfers, we will ensure compliance with UK data protection laws.

## 9. SUBJECT ACCESS REQUESTS AND OTHER RIGHTS OF INDIVIDUALS

9.1 Subject Access Requests

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

- Confirmation that their personal data is being processed and access to a copy of the data.
- The purposes of the data processing and the categories of personal data concerned
- Who the data has been, or will be, shared with, and 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 to the school or directly to the Trust, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual.
- Correspondence address.
- Contact number and email address.
- Details of the information requested.

If staff receive a subject access request in any form, they must immediately forward it to the DPO.

9.2 Children and Subject Access Requests

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

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students at our school may not be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to Subject Access Requests

When responding to requests, we may take the following steps:

- Identification: To verify identity and protect personal data, we may ask for two forms of ID.
- Phone Confirmation: We may call to confirm that the request is genuine and prevent fraud.
- Response Time: We aim to respond within one month. If more ID is needed, the one-month period starts once we receive it.
- No Fees: We provide the requested data for free.
- Extended Time for Complex Requests: For complex cases, we may need over two months. We will inform the individual of the extension and the reason within the first month.

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

- Harm to Physical or Mental Health: disclosure of certain information might cause serious harm to the physical or mental health of the student or another individual. This includes sensitive data whose release could negatively impact their well-being, such as medical records or psychological assessments.
- Risk of Revealing Abuse: if the information would reveal that a child is being or has been abused, or is at risk of abuse, and disclosing this information would not be in the child's best interests, we may withhold it. This ensures that sensitive information, which could potentially exacerbate the child's situation or cause harm, remains protected.
- Inclusion of Third-Party Data: if the requested information contains personal data about another individual, and we cannot reasonably anonymize it, we will not disclose it without the third party's consent. It would be unreasonable to proceed with sharing such data if it involves another person's information and we do not have their permission.
- Sensitive Document Categories: certain documents that fall into sensitive categories, such as those related to criminal investigations, immigration matters, legal proceedings, legal professional privilege, management forecasts, confidential references, or exam scripts, may be exempt from disclosure. These documents often contain highly sensitive information where releasing them could compromise legal processes, confidentiality, or proprietary information.

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.

9.4 Other Data Protection Rights of the Individual

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

- Withdraw Consent: they can stop the processing of their personal data at any time.
- Rectify, Erase, or Restrict: they can request correction, deletion, or restriction of their data under certain conditions.
- Prevent Marketing: they can object to the use of their data for direct marketing.
- Object to Processing: they can object to processing based on public interest, authority, or legitimate interests.
- Challenge Automated Decisions: they can contest decisions made solely by automated processes.
- Data Breach Notification: they have the right to be informed if a data breach poses high risks to them.
- Complaint to ICO: they can file a complaint with the ICO if their rights are violated.
- Data Portability: they can request their data in a transferable, machine-readable format under certain conditions outlined by the ICO.

Individuals should submit any request to exercise these rights to the DPO.

## 10. PARENTAL REQUESTS TO SEE THE EDUCATIONAL RECORD

Parents or guardians may request access to their child's educational record under the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018. As academies are not subject to the Education (Student Information) (England) Regulations 2005, such requests are processed as Subject Access Requests (SARs).

To submit a request, parents must contact the relevant school in writing. The school will respond within one month, as per GDPR requirements. In cases where the request is complex or involves large amounts of data, the response time may be extended by up to two additional months, with written notice provided.

All shared personal data will be handled securely, and necessary redactions will be made to protect third-party privacy and sensitive information.

## 11. BIOMETRIC RECOGNITION SYSTEMS

When we use students' biometric data as part of an automated biometric recognition system (e.g., fingerprint scans for school dinners), we comply with the Protection of Freedoms Act 2012. Parents/carers will be notified before implementing any biometric system or before their child first participates. Written consent from at least one parent or carer will be obtained before collecting and processing any biometric data from their child. Parents/carers and students have the right to opt out of using the biometric system, and we will provide alternative means of accessing services, such as paying for school dinners with cash. Consent can be withdrawn at any time, and any captured data will be deleted.

In compliance with the law, we will not process a student's biometric data if they refuse to participate, regardless of parental consent. For staff members or other adults using the school's biometric systems, we will also obtain consent before their first use and provide alternatives if they object. They can withdraw consent at any time, and any collected data will be deleted.

## 12. CLOSED CIRCUIT TELEVISION (CCTV)

We use CCTV in various locations around the school site to ensure it remains safe. We will follow the ICO 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.

Please see the separate CCTV Policy for the Trust.

## 13. PHOTOGRAPHS AND VIDEOS

As part of our activities, we may take photographs and record images of individuals within our schools. We will obtain written consent from parents/carers, or students aged 18 and over, for photographs and videos to be taken of students 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 the student. Where we don't need parental consent, we will clearly explain to the student 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 students are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or students where appropriate) have agreed to this.

Please see the separate Photograph and Media Policy for the Trust.

## 14. ARTIFICIAL INTELLIGENCE (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, students and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. The Trust recognises that AI has many uses to help students learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots. If personal and/or sensitive data is entered into an unauthorised generative AI tool, the Trust will treat this as a data breach and will follow the personal data breach procedure set out in Appendix One.

## 15. 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. In particular we take the following steps:

- Secure Storage: Paper records and portable devices with personal data are securely locked when not in use.
- Confidential Paper Handling: Confidential documents must not be left unattended and should be stored in locked cabinets.
- Off-Site Data Management: Personal data taken off-site must be signed in and out to track its location and access.
- Strong Passwords: Devices must be secured with a password of appropriate strength.
- Device Encryption: Laptops, USB drives, and portable devices are encrypted to protect data if lost or stolen.
- Personal Device Security: Personal devices used for school data must follow the same

security measures, including strong passwords and encryption.

- Security Audits: Regular audits and risk assessments are conducted to address vulnerabilities.
- Two-Factor Authentication: 2FA is used for accessing sensitive systems and data.
- Data Backup: Regular, encrypted backups ensure data recovery in case of loss or corruption.
- Data Disposal: Personal data is securely disposed of by shredding documents and wiping electronic devices.

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.

### 16. DISPOSAL OF RECORDS

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. For example, we will shred 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 school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Please see the separate Data and Records Retention Policy for the Trust.

### 17. PERSONAL DATA BREACHES

The Trust will make all reasonable endeavours to ensure that there are no personal data breaches. In the event of a suspected data breach, we will follow the procedure set out in Appendix 1.

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

### 18. TRAINING

All staff and volunteers are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development.

## FREEDOM OF INFORMATION

### 19. INTRODUCTION

The Trust is subject to the Freedom of Information Act 2000 (FOI) as a public authority, and, as such, must comply with any requests for information in accordance with the principles laid out in the Act.

### 20. WHAT IS A REQUEST UNDER FOI?

Any request for any information from the Trust is technically a request under the FOI, whether or not the individual making the request mentions the FOI. However, the Information Commissioners Office (ICO) has stated that routine requests for information (such as a parent requesting a copy of a policy) can be dealt with outside of the provisions of the Act.

In all non-routine cases, if the request is simple and the information is to be released, then the individual (within the school or Trust staff) who received the request can release the information but must ensure that this is done within the timescale set out below. A copy of the request and response should then be sent to the Data Protection Officer.

All other requests should be referred in the first instance to the Data Protection Officer, who may

allocate another individual to deal with the request. This must be done promptly, and in any event within two school days of receiving the request.

When considering a request under FOI, that release under FOI is treated as release to the general public, and so once it has been released to an individual, anyone can then access it, and it is not possible to restrict access when releasing by marking the information "confidential" or "restricted".

## 21. TIME LIMIT FOR COMPLIANCE

The Trust must respond as soon as possible, and in any event, within 20 working days of the date of receipt of the request. For an academy trust, when calculating the 20-working day deadline, a "working day" is a school day (one in which students are in attendance), subject to an absolute maximum of 60 normal working days (not school days) to respond.

## 22. PROCEDURE FOR DEALING WITH A REQUEST

When a request is received that cannot be dealt with by simply providing the information, it should be referred in the first instance to the Data Protection Officer within 2 school days, who may re-allocate to an individual with responsibility for the type of information requested.

The first step in responding is to determine if the Trust holds the requested information in any format, which it does if the information exists in computer or paper format. If minimal effort is required to compile the information from different sources, the Trust is considered to hold it. However, if significant manipulation is needed, the requester should be informed and given the option to refine their request. For example, if the Trust needs to sum totals in a spreadsheet, it holds that information. If it involves searching through multiple spreadsheets to provide a total, it may not hold the information, depending on the effort required.

The second stage is to decide whether the information can be released, or whether one of the exemptions set out in the Act applies to the information. Common exemptions that might apply include:

- Section 40 (1) – the request is for the applicants Personal Data. This must be dealt with under the Subject Access Request regime in the GDPR, detailed in the policy above.
- Section 40 (2) – compliance with the request would involve releasing third party personal data, and this would be in breach of the GDPR principles as set out in the policy above.
- Section 41 – information that has been sent to the Trust (but not the Trust's own information) which is confidential.
- Section 21 – information that is already publicly available, even if payment of a fee is required to access that information.
- Section 22 – information that the Trust intends to publish at a future date.
- Section 43 – information that would prejudice the commercial interests of the Trust and / or a third party.
- Section 38 – information that could prejudice the physical health, mental health or safety of an individual (this may apply particularly to safeguarding information).
- Section 31 – information which may prejudice the effective detection and prevention of crime – such as the location of CCTV cameras.
- Section 36 – information which, in the opinion of the Chair of the Trust, would prejudice the effective conduct of the Trust. There is a special form for this on the ICO's website to assist with the obtaining of the chair's opinion.

## 23. RESPONDING TO A REQUEST

When responding to a request where the Trust has withheld some or all of the information, the Data

Protection Officer must explain why the information has been withheld, quoting the appropriate section number and explaining how the information requested fits within that exemption. If the public interest test has been applied, this also needs to be explained. The letter should end by explaining to the requestor how they can complain – either by reference to an internal review or by writing to the Information Commissioners Office.

**APPENDIX ONE: PERSONAL DATA BREACH PROCEDURE**

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

On finding or causing a breach or potential breach, the staff member, governor or data processor must immediately notify the Data Protection Officer (DPO).

The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people

Staff and volunteers will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation.

If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the relevant members of the Executive Leadership Team and Trust Board.

The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers).

The DPO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool.

The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored appropriately.

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line within 72 hours of the school's awareness of the breach.

As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned.
    - The categories and approximate number of personal data records concerned.
- The name and contact details of the DPO.
- A description of the likely consequences of the personal data breach.
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the Trust's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining

information as soon as possible.

Where the Trust is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:

- A description, in clear and plain language, of the nature of the personal data breach.
- The name and contact details of the DPO.
- A description of the likely consequences of the personal data breach.
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.

The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.

The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- The facts and cause of the breach.
- The effects of the breach.
- Action taken to contain the breach and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals).

Records of all breaches will be stored appropriately. The DPO and relevant staff member will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

<u>Actions to Minimise the Impact of Data Breaches</u>
We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

<u>Sensitive Information Being Disclosed via Email (Including Safeguarding Records)</u>
If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.

Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.

If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the IT Team to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence).

In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.

The DPO will endeavour to obtain a written response from all the individuals who received the data, confirming that they have complied with this request.

The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

If safeguarding information is compromised, the DPO will inform the Designated Safeguarding Lead and discuss whether the school should inform any, or all of its local safeguarding partners.

**APPENDIX TWO: DATA PROTECTION OFFICER DETAILS**

The Trust Board has appointed the following staff member as Data Protection Officer for the Trust:

Dr Thomas Flynn
Chief Executive Officer
DataProtection@girlslearningtrust.org