DATA PROTECTION AND FREEDOM OF INFORMATION POLICY

CONTENTS

REVIEW

Last reviewed: May 2018
To be reviewed: May 2021

Policies may be subject to review and revision at any time, notwithstanding that the next review date has not been reached. Review dates are for guidance only; all policies will remain in force until a review has taken place and been formally approved by the Trust.

1 INTRODUCTION

1.1 The Girls' Learning Trust ("the Trust") collects and uses certain types of personal information about staff, students, parents and other individuals who come into contact with the Trust in order to provide education and associated functions. The Trust may be required by law to collect and use certain types of information to comply with statutory obligations related to employment, education and safeguarding, and this policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the General Data Protection Regulation ("GDPR") and other related legislation.

1.2 The GDPR applies to all computerised data and manual files if they come within the definition of a 'filing system'. Broadly speaking, a filing system is one where the data is structured in some way that it is searchable on the basis of specific criteria (so you would be able to use something like the individual's name to find their information), and if this is the case, it does not matter whether the information is located in a different physical location.

1.3 This policy will be updated as necessary to reflect best practice, or amendments made to data protection legislation, and shall be reviewed at least every 3 years.

2 PERSONAL DATA

2.1 'Personal Data' is information that identifies an individual, and includes information that would identify an individual to the person to whom it is disclosed because of any special knowledge that they have or can obtain[1].

2.2 A sub-set of Personal Data is known as 'Special Category Personal Data'. This Special Category Personal Data is information that reveals:

2.2.1 race or ethnic origin;
2.2.2 political opinions;
2.2.3 religious or philosophical beliefs;
2.2.4 trade union membership;
2.2.5 physical or mental health;
2.2.6 an individual's gender or sexual orientation;
2.2.7 genetic or biometric data for the purpose of uniquely identifying a natural person.

Special Category Personal Data (also known as 'sensitive data') is given special protection, and additional safeguards apply if this information is to be collected and used.

2.3 Information relating to criminal convictions shall only be held and processed where there is legal authority to do so.

2.4 The Trust does not intend to seek or hold Special Category Personal Data (previously known as sensitive personal data) about staff or students except where the Trust has been notified of the information, it comes to the Trust's attention via legitimate means (e.g. a grievance), or it needs to be sought and held in compliance with a legal obligation or as a matter of good practice. Staff or students are under no obligation to disclose to the Trust their race or ethnic origin, political or

[1] For example, if asked for the number of female employees, and you only have one female employee, this would be personal data if it was possible to obtain a list of employees from the website.

religious beliefs, whether or not they are a trade union member or details of their sexual orientation (save to the extent that details of gender, marital status and/or parenthood are needed for other purposes, e.g. pension entitlements).

3 THE DATA PROTECTION PRINCIPLES

3.1 The six data protection principles as laid down in the GDPR are followed at all times:

3.1.1 Personal Data shall be processed fairly, lawfully and in a transparent manner, and processing shall not be lawful unless one of the processing conditions can be met (as explained in paragraph 4.1);

3.1.2 Personal Data shall be collected for specific, explicit, and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes;

3.1.3 Personal Data shall be adequate, relevant, and limited to what is necessary for the purpose(s) for which it is being processed;

3.1.4 Personal Data shall be accurate and, where necessary, kept up to date;

3.1.5 Personal Data processed for any purpose(s) shall not be kept in a form which permits identification of individual's data for longer than is necessary for that purpose / those purposes;

3.1.6 Personal Data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

3.2 In addition to this, the Trust is committed to ensuring that anyone dealing with personal data shall be mindful of the individual's rights under the law (as explained in more detail in paragraphs 7 and 8).

3.3 The Trust is committed to complying with the principles in 3.1, and will:

3.3.1 Use Trust Privacy Notices to inform students, parents & carers, staff, trustees & members, school governors, volunteers & others of the purpose of collecting and processing information from them;

3.3.2 Operate a Trust Photographs and Media Policy to manage images of individuals;

3.3.3 Be responsible for checking the quality and accuracy of the information recorded, in so far as is reasonable practicable (including routine data updates for student data collated from parents & carers);

3.3.4 Undertake Data Processing Audits and maintain records of data processing activities;

3.3.5 Routinely review the records held to ensure that information is not held longer than is necessary, and that it is held in accordance with the Trust's Records Retention Policy;

3.3.6 Ensure that when information is authorised for disposal it is done appropriately;

3.3.7 Ensure appropriate security measures to safeguard personal information whether it is held in paper files or on our computer system in accordance with the Trust IT Policy, and follow the relevant security policy requirements at all times;

3.3.8 Share Personal Data with others only when necessary and legally appropriate to do so, and obtain Trust Data Processing Agreements with contractors and third parties that process Personal Data on our behalf;

3.3.9 Set out clear procedures for responding to requests for access to Personal Data known as Subject Access Requests, as explained in more detail in paragraph 9;

3.3.10 Report breaches of the GDPR in accordance with the procedure in paragraph 12.

4 PROCESSING CONDITIONS FOR THE FIRST DATA PROTECTION PRINCIPLE

4.1 One of the following data processing conditions must be met in accordance with para 3.1.1.:

4.1.1 The individual has given consent that is specific to the particular type of processing activity, and that consent is informed, unambiguous and freely given, or;

4.1.2 The processing is necessary for the performance of a contract, to which the individual is a party, or is necessary for the purpose of taking steps with regards to entering into a contract with the individual, at their request, or;

4.1.3 The processing is necessary for the performance of a legal obligation to which we are subject, or;

4.1.4 The processing is necessary to protect the vital interests of the individual or another, or;

4.1.5 The processing is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in us, or;

4.1.6 The processing is necessary for a legitimate interest of the Trust or that of a third party, except where this interest is overridden by the rights and freedoms of the individual concerned.

5 USE OF PERSONAL DATA BY THE TRUST

5.1 The Trust holds Personal Data on students, staff, contractors, volunteers and other individuals who come into contact with the Trust in order to provide education and associated functions[2]. In each case, the Personal Data must be treated in accordance with the data protection principles as outlined in paragraph 3.1.

Students

5.2 The Personal Data held regarding students includes contact details, date of birth, nationality, assessment / examination results, attendance information, characteristics such as ethnic group, special educational needs, eligibility for free school meals, pupil premium & 16-19 bursary, relevant medical information, relevant safeguarding information, photographs and biometric data (for cashless catering).

5.3 Personal Data is used in order to support the education of students, admissions to the schools, to monitor and report on their progress, to manage safeguarding and child protection matters, for communication of information about the school and Trust (such as newsletters and website materials), to provide appropriate pastoral care, recruitment and training purposes, and to assess how well the Trust as a whole is doing, together with any other uses normally associated with this provision in a school environment. These uses are covered by the processing conditions set out in paragraph 4.1, and the Trust does not need explicit consent from the individual.

5.4 Areas of school life in which the Trust does need to obtain explicit consent include:

5.4.1 Transferring information to any association, society, charity or club set up for the purpose of maintaining contact with current or former students and alumni, or for fundraising, marketing or promotional purposes, where the student/family has a choice to participate or not, and;

[2] The Trust's objects are set out in the GLT Articles of Association (published on our website).

5.4.2 Making Personal Data, including Special Category Personal Data, available to staff for planning extra-curricular activities (such as trips & visits), where participation in extra-curricular activities is a choice;

5.4.3 Using photographs of students, where consent is a choice, in accordance with the Trust Photograph and Media Policy, and;

5.4.4 Biometric data, used for cashless catering systems (where applicable).

Staff (including trustees & members, school governors & other volunteers)

5.5 The Personal Data held about staff may include name, contact details (including emergency next of kin and/or other personal contacts), date of birth, employment history, qualifications, contract of employment, information relating to career progression and appraisals, information relating to safer recruitment and DBS checks, references from former employers, occupational health referrals, details of pay and pensions (including bank details and National Insurance number), sickness and holiday records (absence), maternity/paternity/adoption arrangements, disciplinary, capability & grievance procedures, photographs and biometric data (for cashless catering). It may also include Special Category Personal Data such as ethnic group, relevant medical information and trade union membership (where you choose to supply this information to us).

5.6 Personal Data is used to comply with legal obligations placed on the Trust in relation to employment and the education of students in a school environment. The Trust may pass information to other regulatory authorities where appropriate, and may use names in newsletters and website material. Personal Data will also be used when giving references, where the individual has put the Trust down as a referee. These uses are covered by the processing conditions set out in paragraph 4.1, and the Trust does not need explicit consent from the individual.

5.7 Disclosure Barring Service ('DBS') checks are carried out on the basis of the Trust's legal obligations in relation to the Safer Recruitment of Staff as stipulated in the Department for Education's statutory guidance for England 'Working together to safeguard children' and 'Keeping children safe in education'. The DBS information (which will include personal data relating to criminal convictions and offences) is further processed in the substantial public interest, with the objective of safeguarding children. Retention of the information is covered by the Trust's Records Retention Policy.

Access to the DBS information is restricted to staff that have a genuine need to have access to it for their job roles. In addition to the provisions of the GDPR and the Data Protection Act 2018, disclosure of this information is restricted by section 124 of the Police Act 1997 and disclosure to third parties will only be made if it is determined to be lawful.

5.8 Areas of school life in which the Trust does need to obtain explicit consent include:

5.8.1 Transferring information to any staff association, society, charity or club set up for the purpose of maintaining contact with current and former staff, or for fundraising, marketing or promotional purposes, where the member of staff has a choice to participate or not, and;

5.8.2 Making Personal Data, including Special Category Personal Data, available for planning extra-curricular activities (such as trips & visits), where staff leadership of extra-curricular activities is a choice, and;

5.8.3 Using photographs of staff and school life, where consent is a choice, in accordance with the Trust Photograph and Media Policy, and;

5.8.4 Biometric data, used for cashless catering systems (where applicable), and;

5.8.5 Driving for work including details of driving licence, car insurance and car MOT, in accordance with the Driving for Work risk assessment and Trust Expenses Policy.

Parents (including guardians and carers)

5.9 The Personal Data held about parents & carers may include emergency contact details (including other emergency contracts such as neighbours and grandparents), and relevant financial details (such as supporting evidence for free school meals or bursary applications).

At the start of the student's time at school, and periodically thereafter, the school will request the name and contact details of individuals to act as emergency contacts. The Trust (on behalf of the schools in the Trust) assesses that the effort involved for it to write to every emergency contact to provide them with privacy information is disproportionate in relation to the effect that the use of their Personal Data will have on them (contacting them in the event of an emergency). As such, the school does not actively provide privacy information to each emergency contact, however it does publish information in this policy on the use of emergency contact details. To further mitigate any risks, the Trust specifies strict limited use of emergency contact details, and places restrictions on its computer system so that only authorised members of staff have access to these details.

5.10 Areas of school life in which the Trust does need to obtain explicit consent include:

5.10.1 Fundraising activities and promotional materials seeking parental donations (for example to School Fund), where the parent or carer has a choice to participate or not. We will seek explicit consent to write to parents & carers in relation to this activity.

Other Individuals (such as contractors & guests)

5.11 The Trust may hold Personal Data in relation to other individuals who have contact with the school, such as guests and contractors. Such information shall be held only in accordance with the data protection principles, and shall not be kept longer than necessary.

6 SECURITY OF PERSONAL DATA

6.1 The Trust will take reasonable steps to ensure that members of staff will only have access to Personal Data where it is necessary for them to carry out their duties. All staff will be made aware of this Policy and their duties under the GDPR. The Trust will take all reasonable steps to ensure that all Personal Data is held securely and is not accessible to unauthorised persons.

6.2 For further details regarding the security of IT systems, please refer to the Trust IT Policy.

7 DISCLOSURE OF PERSONAL DATA TO THIRD PARTIES

7.1 The following list includes the most usual reasons that the Trust will use when authorising disclosure of Personal Data to a third party:

7.1.1 To give a confidential reference relating to a current or former employee, volunteer or student;

7.1.2 For the prevention or detection of crime;

7.1.3 For the assessment of any tax or duty;

7.1.4 Where it is necessary to exercise a right or obligation conferred or imposed by law upon the Trust (other than an obligation imposed by contract);

7.1.5 For the purpose of, or in connection with, legal proceedings (including prospective legal proceedings);

7.1.6 For the purpose of obtaining legal advice;

7.1.7 For educational research, historical and statistical purposes;

7.1.8 To publish the results of public examinations or destination data ;

7.1.9 To disclose details of a student's medical condition where it is in the student's interests to do so and there is a legal basis[3] for doing so, for example for medical advice, social services, child protection, insurance purposes or to organisers of school trips;

7.1.10 To disclose student details, such as passport information, for the purposes of curriculum based school trips, or optional extra curricular activities (in which case consent will be separately sought);

7.1.11 To provide information to another educational establishment to which a student is transferring;

7.1.12 To provide information to an examination authority as part of the examination process;

7.1.13 To provide education and/or curriculum related on-line and IT services through third parties (such as 'MyMaths' on-line teaching tools, MintClass);

7.1.14 To disclose student information to employers providing a work experience placement`for students;

7.1.15 To disclose staff details in connection with payroll and pension services, occupational health, insurance and CPD/training providers;

7.1.16 To provide information to the relevant government department concerned with national education. At the time of the writing of this Policy, the government department concerned with national education is the Department for Education (DfE). The examination authorities may also pass information to the DfE;.

7.2 The DfE uses information about students for statistical purposes, to evaluate and develop education policy and to monitor the performance of the nation's education service as a whole. The statistics are used in such a way that individual students cannot be identified from them. On occasion the DfE may share the Personal Data with other Government Departments or agencies strictly for statistical or research purposes.

7.3 The Trust may receive requests from third parties (i.e. those other than the data subject, the Trust, and employees of the Trust) to disclose personal data it holds about students, their parents or guardians, staff or other individuals. This information will not generally be disclosed unless one of the specific exemptions under data protection legislation which allow disclosure applies; or where necessary for the legitimate interests of the individual concerned or the Trust.

7.4 Where Personal Data is disclosed to third parties, the Trust will establish a Data Processing Agreements with the third party.

7.5 Any query or uncertainty regarding a request for the disclosure of Personal Data must be forwarded to the Data Protection Officer (contact details in paragraph 13).

[3] The legal basis will vary in each case but will usually be based on explicit consent, the vital interests of the student, or reasons of substantial public interest (usually safeguarding the student or other individuals).

8 CONFIDENTIALITY OF STUDENT DATA

8.1 Personal Data can be shared with students once they are considered old enough and this information will also normally be shared with parents/carers. In general, a student is regarded (in English law) as having ownership of their own data rights as soon as they have the capacity and understanding to manage them. This is generally assumed from the age of 12, unless the student does not have sufficient understanding to make his or her own decisions.

8.2 If a student seeks to raise concerns regarding confidentiality of data with a member of staff and expressly withholds their agreement to their Personal Data being disclosed to their parents or carer, the Trust will maintain confidentiality unless it has reasonable grounds to believe that the student does not fully understand the consequences of withholding their consent, or where the Trust believes disclosure will be in the best interests of the student or other students in line with the Trust's Child Protection & Safeguarding Policy. Disclosure for a safeguarding purpose will be lawful because it will be in the substantial public interest. Notification must be sent in writing to the Data Protection Officer who will assess (in consultation with the relevant Head of Year) the individual student's request for privacy. If accepted, the parent or carer of the student will be notified of the decision.

8.3 There is no automatic parental right of access to the student's educational record when the student's school is an academy (or part of a multi-academy trust). This is because the regulations that confer that right on parents do not apply to academies.

9 SUBJECT ACCESS REQUESTS

9.1 Anyone who makes a request to see any Personal Data held about them by the Trust is making a Subject Access Request. All information relating to the individual, including that held in electronic or manual files should be considered for disclosure, provided that they constitute a 'filing system' (see paragraph 1.2).

9.2 All Subject Access Requests received by the Trust, or any school within the Trust, must be referred to the Data Protection Officer (contact details in paragraph 13) within 2 school days of receipt at the Trust/school. On receipt the DPO must deal with the request in full and respond within one month of receipt.[4]

9.3 Where a student does not have sufficient understanding to make his or her own request (usually those under the age of 12, or over 12 but with a special educational need which makes understanding their information rights more difficult), a person with parental responsibility can make a request on their behalf in writing to the Data Protection Officer. The Data Protection Officer must, however, be satisfied that:

- 9.3.1 the student lacks sufficient understanding; and
- 9.3.2 the request made on behalf of the student is in their interests.

9.4 Any individual, including a student with ownership of their own information rights, may appoint another person to request access to their records. In such circumstances the Trust must have

[4] The Department for Education, Data Protection Toolkit for Schools, published 23rd April 2018, acknowledges that the education sector is largely unique in having school closure periods during which it may not be possible to respond within the timeframe set out in GDPR. It recommends explaining that for most of the year the Trust aims to respond in a timely manner, but that during school closure periods (as advertised on the school websites) this may not be possible. As a minimum, the Trust will respond to the request within one month to acknowledge receipt and indicate a proposed date for compliance as soon as reasonably practicable once the school is back in term-time operation.

written evidence that the individual has authorised the person to make the application and the Data Protection Officer must be confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates. Students may authorise their parents to make a request and it is the Trust's policy to request student authorisation for this from Year 8 onwards unless the student does not have sufficient understanding, as covered in paragraph 9.3.

9.5 Access to records will be refused in instances where an exemption applies, for example, information sharing may place the individual at risk of significant harm or jeopardise police investigations into any alleged offence(s).

9.6 A Subject Access Request must be made in writing to the Data Protection Officer and should be specific about the personal information sought. The Trust may ask for any further information reasonably required to provide the information, and may request clarification of the information sought.

9.7 An individual only has the automatic right to access information about themselves, and care needs to be taken not to disclose the Personal Data of third parties where consent has not been given, or where seeking consent would not be reasonable, or it would not be appropriate to release the information. Particular care must be taken in the case of any complaint or dispute to ensure confidentiality is protected.

9.8 All files must be reviewed by the Data Protection Officer before any disclosure takes place. Access will not be granted before this review has taken place.

9.9 Where all the data in a document cannot be disclosed a permanent copy will be made and the data obscured (or retyped if this is more sensible). A copy of the full document and the altered document will be retained, with the reason why the document was altered.

10 EXEMPTIONS TO ACCESS BY DATA SUBJECTS

10.1 Where a claim to legal professional privilege could be maintained in legal proceedings, the information is likely to be exempt from disclosure unless the privilege is waived.

10.2 Where safeguarding and child protection considerations apply.

10.3 There are other exemptions from the right of subject access (such as breaches of ethics in regulated professions). If the Trust intends to apply any of them to a request, then it will explain which exemption is being applied and why.

11 OTHER RIGHTS OF INDIVIDUALS

11.1 The Trust has an obligation to comply with the rights of individuals under the law and takes these rights seriously. The following sets out how the Trust will comply with the rights to:

11.1.1 Object to Processing;
11.1.2 Rectification;
11.1.3 Erasure; and
11.1.4 Data Portability.

Right to object to processing

11.2 An individual has the right to object to the processing of their Personal Data on the grounds of pursuit of a public interest or legitimate interest (paragraphs 4.1.5 and 4.1.6) where they do not believe that those grounds are adequately established.

11.3 Where such an objection is made, it must be sent to the Data Protection Officer within 2 school days following receipt, and the Data Protection Officer will assess whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the individuals, or whether the information is required for the establishment, exercise or defence of legal proceedings.

The Data Protection Officer is responsible for notifying the individual of the outcome of their assessment as soon as reasonably practicable (usually within 30 school days[5] following receipt of the objection).

Right to rectification

11.4 An individual has the right to request the rectification of inaccurate data without undue delay. Where any request for rectification is received by the Trust or schools within, it should be sent to the Data Protection Officer within 2 school days of receipt, and where adequate proof of inaccuracy is given, the data shall be amended as soon as reasonably practicable, and the individual notified.

11.5 Where there is a dispute as to the accuracy of the data, the request and reasons for refusal shall be noted alongside the data, and communicated to the individual. The individual shall be given the option of a review under the Trust Complaints Policy (students & parents/carers), or the Trust Grievance Policy (staff) or an appeal direct to the Chair of the Trust, or an appeal direct to the Information Commissioner's Office ("ICO").

11.6 An individual also has a right to have incomplete information completed by providing the missing data, and any information submitted in this way shall be updated without undue delay.

Right to erasure

11.7 Individuals have a right, in certain circumstances, to have data permanently erased without undue delay. This right arises in the following circumstances:

11.7.1 where the Personal Data is no longer necessary for the purpose or purposes for which it was collected and processed;

11.7.2 where consent is withdrawn and there is no other legal basis for the processing;

11.7.3 where an objection has been raised under the right to object, and found to be legitimate;

11.7.4 where Personal Data is being unlawfully processed (usually where one of the conditions for processing in paragraph 4.1 cannot be met);

11.7.5 where there is a legal obligation on the Trust to delete.

11.8 The Data Protection Officer will make a decision regarding any application for erasure of Personal Data, and will balance the request against the exemptions provided for in the law. Where a decision is made to erase the data, and this data has been passed to other data

[5] A 'school day' is one in which students are in attendance.

controllers, and / or has been made public, reasonable attempts to inform those controllers of the request shall be made.

Right to restrict processing

11.9 In the following circumstances, processing of an individual's Personal Data may be restricted:

11.9.1 where the accuracy of data has been contested, during the period when the Trust is attempting to verify the accuracy of the data;

11.9.2 where processing has been found to be unlawful, and the individual has asked that there be a restriction on processing rather than erasure;

11.9.3 where data would normally be deleted, but the individual has requested that their information be kept for the purpose of the establishment, exercise or defence of a legal claim;

11.9.4 where there has been an objection made (paragraph 11.2) pending the outcome of any decision.

Right to portability

11.10 If an individual wants to send their Personal Data to another organisation they have a right to request that the Trust provides their information in a structured, commonly used, and machine readable format. As this right is limited to situations where the Trust is processing the information on the basis of consent or performance of a contract, the situations in which this right can be exercised are quite limited. If a request for this is made, it should be forwarded to the Data Protection Officer within 2 school days of receipt, and the Data Protection Officer will review and revert as necessary.

12 BREACH OF ANY REQUIREMENT OF THE GDPR

12.1 Any and all breaches of the GDPR, including a breach of any of the data protection principles shall be reported as soon as it is/they are discovered, to the Data Protection Officer.

12.2 Once notified, the Data Protection Officer shall assess:

12.2.1 the extent of the breach;

12.2.2 the risks to the data subjects as a consequence of the breach;

12.2.3 any security measures in place that will protect the information;

12.2.4 any measures that can be taken immediately to mitigate the risk to the individuals.

12.3 Unless the Data Protection Officer concludes that there is unlikely to be any risk to individuals from the breach, it must be notified to the Information Commissioner's Office (ICO) within 72 hours of the breach having come to the attention of the Trust, unless a delay can be justified.

12.4 The Information Commissioner Office shall be told:

12.4.1 details of the breach, including the volume of data at risk, and the number and categories of data subjects;

12.4.2 the contact point for any enquiries (which shall usually be Data Protection Officer);

12.4.3 the likely consequences of the breach;

12.4.4 measures proposed or already taken to address the breach.

12.5 If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals then the Data Protection Officer shall notify the data subjects of the breach without undue delay

unless the data would be unintelligible to those not authorised to access it, or measures have been taken to mitigate any risk to the affected individuals.

12.6 Data subjects shall be told:

12.6.1 the nature of the breach;

12.6.2 who to contact with any questions

12.6.3 measures taken to mitigate any risks.

12.7 The Data Protection Officer shall then be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented. Any recommendations for further training or a change in procedure shall be reviewed by the Trust Board and a decision made about implementation of those recommendations.

13 CONTACT DETAILS

13.1 Contact details for the **Data Protection Officer** are as follows:

Jennifer Smith
Chief Executive Officer
Girls' Learning Trust

BY EMAIL (preferred): dataprotection@girlslearningtrust.org
BY POST (may take longer, especially during school closure periods):
Girls' Learning Trust
Ewell Road
Cheam SM3 8AB

If anyone has any concerns or questions in relation to this policy they should contact the Data Protection Officer.

13.2 Contact details for the **Information Commissioners Office** are as follows:

BY EMAIL (preferred): www.ico.org.uk/concerns
BY POST:
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

BY PHONE: 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate number.

FREEDOM OF INFORMATION POLICY

14 INTRODUCTION

14.1 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.

15 WHAT IS A REQUEST UNDER FOI

15.1 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.

15.2 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.

15.3 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 2 school days of receiving the request.

15.4 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".

16 TIME LIMIT FOR COMPLIANCE

16.1 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.

17 PROCEDURE FOR DEALING WITH A REQUEST

17.1 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.

17.2 The first stage in responding is to determine whether or not the Trust "holds" the information requested. The Trust will hold the information if it exists in computer or paper format. Some requests will require the Trust to take information from different sources and manipulate it in some way. Where this would take minimal effort, the Trust is considered to "hold" that information, but if the required manipulation would take a significant amount of time, the requestor should be contacted to explain that the information is not held in the manner requested, and offered the opportunity to refine their request. For example, if a request

required the Trust to add up totals in a spread sheet and release the total figures, this would be information "held" by the Trust. If the Trust would have to go through a number of spread sheets and identify individual figures and provide a total, this is likely not to be information "held" by the Trust, depending on the time involved in extracting the information.

17.3 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:

17.3.1 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 paragraph 9 of the Data Protection Policy above;

17.3.2 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 paragraph 3.1 of the DPA policy above;

17.3.3 Section 41 – information that has been sent to the Trust (but not the Trust's own information) which is confidential;

17.3.4 Section 21 – information that is already publicly available, even if payment of a fee is required to access that information;

17.3.5 Section 22 – information that the Trust intends to publish at a future date;

17.3.6 Section 43 – information that would prejudice the commercial interests of the Trust and / or a third party;

17.3.7 Section 38 – information that could prejudice the physical health, mental health or safety of an individual (this may apply particularly to safeguarding information);

17.3.8 Section 31 – information which may prejudice the effective detection and prevention of crime – such as the location of CCTV cameras;

17.3.9 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.

17.4 The sections mentioned in italics are qualified exemptions. This means that even if the exemption applies to the information, the Trust will also have to carry out a public interest test, balancing the public interest in the information being released, as against the public interest in withholding the information.

18 RESPONDING TO A REQUEST

18.1 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.

18.2 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.

19 CONTACT DETAILS

19.1 All FOI requests, and any questions about this policy, should be directed in the first instance to the Data Protection Officer who can be contacted using the details set out in paragraph 13.