Combined Data Protection and FOI Policy

September 2021 – August 2022

Policy Owner:	Human Resources
Approved by:	Trust Board
Policy Version:	V1.0
Date Approved:	8th February 2022
Review Date:	September 2022

To be read in conjunction with the following policies and procedures:

Grievance Policy	Whistleblowing Policy
Capability Procedure	Equal Opportunities Policy
Probationary Policy	Staff Handbook
Professional Code of Conduct	Disciplinary Policy & Procedure
Dignity at Work Policy	Performance Management Policy
ICT Acceptable Use Policy	Freedom of Information Policy
Safeguarding and Child Protection Policy	Record Retention Policy

Document Review Control Information

Version	Date	Reviewer Name(s)	Comments
V 1.0	February 2022	SS/AH/LH	

This is a controlled document. Whilst this document may be printed, the electronic version posted on the shared drive is the controlled copy. Any printed copies of the document are not controlled.

Relevant legislation and guidance

Data Protection Act 2018	Employment Act 2002 and 2008
Equality Act 2010	Employment Relations Act 1999
Employment Rights Act 1996	Public Interest Disclosure Act 1998
Human Rights Act 1998	Freedom of Information Act 2000
The Education (Pupil Information) (England) Regulations 2000	
Computer Misuse Act 1990, amended by the Police and Justice Act 2006	
Written in line with ACAS Guidance, Codes of Practice and ICO advice	

Contents

1. Background

1.1 This combined Data Protection and Freedom of Information (FOI) Policy is reviewed on a regular basis by The Governing Bodies (GB) of the Northern Schools Trust (NST) schools.

1.2 Throughout this document the term Principal refers to the Principal or Head of Academy/School. The terms Trust and Schools refer to all Academies, Schools as well as the central team.

1.3 At all stages within this procedure, and in accordance with the Equality Act 2010 and the NST Equal Opportunity Policy, provision will be made for any reasonable adjustments to accommodate the needs of individuals.

1.4 The Trust processes Personal Data (as defined below) in order to enable it to provide education and other associated functions (and, additionally, where there is a legal requirement to process the personal data to ensure that it complies with its statutory obligations). This Data Protection Policy ("Policy") regulates the way in which the Trust obtains, uses, holds, transfers and processes Personal Data about individuals (including staff, learners, parents or carers and other individuals who come into contact with the Trust) and ensures all of its staff know the rules for protecting Personal Data. Further, it describes individuals' rights in relation to their Personal Data processed by the Trust.

1.5 This Policy applies to all staff employed by the Trust inclusive of staff employed at schools and academies governed by the Trust, temporary employees, agency workers and volunteers.

1.6 All staff, as defined in 1.5 above, are responsible for complying with this policy.

1.7 For the purposes of the Act, the Trust is the Data Controller.

2. Introduction

2.1 Northern Schools Trust ("the Trust") collects and uses certain types of personal information about staff, pupils, parents and other individuals who come into contact with the Trust in order 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 and other related legislation.

2.2 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.

2.3 This policy will be updated as necessary to reflect best practice, or amendments made to data protection legislation, and shall be reviewed every 2 years.

3. Personal Data

3.1 '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]. A sub-set of personal data is known as 'special category personal data'. This special category data is information that relates to:

3.1.1 race or ethnic origin;

[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.

3.1.2 political opinions;
3.1.3 religious or philosophical beliefs;
3.1.4 trade union membership;
3.1.5 physical or mental health;
3.1.6 an individual's sex life or sexual orientation;
3.1.7 genetic or biometric data for the purpose of uniquely identifying a natural person.

3.2 Special Category information is given special protection, and additional safeguards apply if this information is to be collected and used.

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

3.4 The Trust does not intend to seek or hold sensitive personal data about staff or students except where the Trust has been notified of the information, or it comes to the Trust's attention via legitimate means (e.g. a grievance) or 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 religious beliefs, whether or not they are a trade union member or details of their sexual life (save to the extent that details of marital status and / or parenthood are needed for other purposes, e.g. pension entitlements).

4. The Data Protection Principles

4.1 The six data protection principles as laid down in the GDPR are followed at all times:
4.1.1 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;
4.1.2 Personal data shall be collected for specific, explicit, and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes;
4.1.3 personal data shall be adequate, relevant, and limited to what is necessary for the purpose(s) for which it is being processed;
4.1.4 personal data shall be accurate and, where necessary, kept up to date;
4.1.5 personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose / those purposes;
4.1.6 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.

4.2 In addition to this, the Trust is committed to ensuring that at all times, anyone dealing with personal data shall be mindful of the individual's rights under the law (as explained in more detail in paragraphs 8 and 9 below).

4.3 The Trust is committed to complying with the principles in 4.1 at all times. This means that the Trust will:
4.3.1 inform individuals as to the purpose of collecting any information from them, as and when we ask for it;
4.3.2 be responsible for checking the quality and accuracy of the information;
4.3.3 regularly review the records held to ensure that information is not held longer than is necessary, and that it has been held in accordance with the data retention policy;
4.3.4 ensure that when information is authorised for disposal it is done appropriately;
4.3.5 ensure appropriate security measures to safeguard personal information whether it is held in paper files or on our computer system, and follow the relevant security policy requirements at all times;
4.3.6 share personal information with others only when it is necessary and legally appropriate to do so;
4.3.7 set out clear procedures for responding to requests for access to personal information known as subject access requests;

4.3.8 report any breaches of the GDPR in accordance with the procedure in paragraph 10 below.

5. Conditions for Processing in the First Data Protection Principle

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

5.2 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.

5.3 The processing is necessary for the performance of a legal obligation to which we are subject.

5.4 The processing is necessary to protect the vital interests of the individual or another.

5.5 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.

5.6 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

6. Use of Personal Data by the Trust

6.1 The Trust holds personal data on pupils, staff and other individuals such as visitors. In each case, the personal data must be treated in accordance with the data protection principles as outlined in paragraph 4.1 above.

Pupils

6.2 The personal data held regarding pupils includes contact details, assessment / examination results, attendance information, characteristics such as ethnic group, special educational needs, any relevant medical information, and photographs.

6.3 The data is used in order to support the education of the pupils, to monitor and report on their progress, to provide appropriate pastoral care, 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.

6.4 The Trust may make use of limited personal data (such as contact details) relating to pupils, and their parents or guardians for fundraising, marketing or promotional purposes and to maintain relationships with pupils of the Trust, but only where consent has been provided to this.

6.5 In particular, the Trust may:

6.5.1 transfer information to any association society or club set up for the purpose of maintaining contact with pupils or for fundraising, marketing or promotional purposes relating to the Trust but only where consent has been obtained first;

6.5.2 make personal data, including sensitive personal data, available to staff for planning curricular or extra-curricular activities;

6.5.3 keep the pupil's previous school informed of his / her academic progress and achievements e.g. sending a copy of the school reports for the pupil's first year at the Trust to their previous school;

6.5.4 Use photographs of pupils in accordance with the photograph policy.

6.6 Any wish to limit or object to any use of personal data should be notified to the Data Protection Officer in writing, which notice will be acknowledged by the Trust in writing. If, in the view of

The Data Protection Officer, the objection cannot be maintained, the individual will be given written reasons why the Trust cannot comply with their request.

Staff

6.7 The personal data held about staff will include contact details, employment history, information relating to career progression, information relating to DBS checks, photographs.

6.8 The data is used to comply with legal obligations placed on the Trust in relation to employment, and the education of children in a school environment. The Trust may pass information to other regulatory authorities where appropriate, and may use names and photographs of staff in publicity and promotional material. Personal data will also be used when giving references.

6.9 Staff should note that information about disciplinary action may be kept for longer than the duration of the sanction. Although treated as "spent" once the period of the sanction has expired, the details of the incident may need to be kept for a longer period.

6.10 Any wish to limit or object to the uses to which personal data is to be put should be notified to the Data Protection Officer who will ensure that this is recorded, and adhered to if appropriate. If the Data Protection Officer is of the view that it is not appropriate to limit the use of personal data in the way specified, the individual will be given written reasons why the Trust cannot comply with their request.

Other Individuals

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

7. Security of Personal Data

7.1 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 information is held securely and is not accessible to unauthorised persons.

7.2 For further details as regards security of IT systems, please refer to the ICT Policy.

8. Disclosure of Personal Data to Third Parties

8.1 The following list includes the most usual reasons that the Trust will authorise disclosure of personal data to a third party:

- 8.1.1 To give a confidential reference relating to a current or former employee, volunteer or pupil;
- 8.1.2 for the prevention or detection of crime;
- 8.1.3 for the assessment of any tax or duty;
- 8.1.4 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);
- 8.1.5 for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings);
- 8.1.6 for the purpose of obtaining legal advice;
- 8.1.7 for research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress);
- 8.1.8 to publish the results of public examinations or other achievements of pupils of the Trust;
- 8.1.9 to disclose details of a pupil's medical condition where it is in the pupil's interests to do so, for example for medical advice, insurance purposes or to organisers of school trips;

8.1.10 to provide information to another educational establishment to which a pupil is transferring;

8.1.11 to provide information to the Examination Authority as part of the examination process; and

8.1.12 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 Authority may also pass information to the DfE.

8.2 The DfE uses information about pupils 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 pupils 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.

8.3 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 pupils, 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.

8.4 All requests for the disclosure of personal data must be sent to The Data Protection Officer, who will review and decide whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of that third party before making any disclosure.

9. Confidentiality of Pupil Concerns

9.1 Where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents or guardian, the Trust will maintain confidentiality unless it has reasonable grounds to believe that the pupil does not fully understand the consequences of withholding their consent, or where the Trust believes disclosure will be in the best interests of the pupil or other pupils. Further details can be found in the school's Child Protection Policy.

Subject Access Requests

9.2 Anybody who makes a request to see any personal information 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 clause 2.2).

9.3 All requests should be sent to The Data Protection Officer within 3 working days of receipt, and must be dealt with in full without delay and at the latest within one month of receipt.

9.4 Where a child or young person 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. The Data Protection Officer must, however, be satisfied that:

9.4.1 the child or young person lacks sufficient understanding; and;

9.4.2 the request made on behalf of the child or young person is in their interests.

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

9.6 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).

9.7 Subject access requests can be submitted in any form, but we may be able to respond more quickly if they are made in writing and include:
9.7.1 Name of the individual;
9.7.2 Correspondence address;
9.7.3 Contact number and email address;
9.7.4 Details of the information requested;
If staff receive a subject access request in any form they must forward it to the DPO.

9.8 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, and 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.

9.9 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.

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

9.11 When responding to requests, we:
9.11.1 May ask the individual to provide 2 forms of identification
9.11.2 May contact the individual via phone to confirm the request was made
9.11.3 Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
9.11.4 Will provide the information free of charge
9.11.5 May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

9.12 We may not disclose information for a variety of reasons, such as if it:
9.12.1 Might cause serious harm to the physical or mental health of the pupil or another individual;
9.12.2 Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests;
9.12.3 Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it;
9.12.4 Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts.

9.12 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.

9.14 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.

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 There are other exemptions from the right of subject access. If we intend to apply any of them to a request then we will usually 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 section 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 (grounds 5.5 and 5.6 above) where they do not believe that those grounds are made out.

11.3 Where such an objection is made, it must be sent to The Data Protection Officer within 2 working days of 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.

11.4 The Data Protection Officer shall be responsible for notifying the individual of the outcome of their assessment within ten working days of receipt of the objection.

Right to rectification

11.5 An individual has the right to request the rectification of inaccurate data without undue delay. Where any request for rectification is received, it should be sent to The Data Protection Officer within 2 working 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.

11.6 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 data protection complaints procedure, or] an appeal direct to the Information Commissioner.

11.7 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

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

- 11.8.1 where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed;
- 11.8.2 where consent is withdrawn and there is no other legal basis for the processing;
- 11.8.3 where an objection has been raised under the right to object, and found to be legitimate;
- 11.8.4 where personal data is being unlawfully processed (usually where one of the conditions for processing cannot be met);

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

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

Right to restrict processing

11.10 In the following circumstances, processing of an individual's personal data may be restricted:

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

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

11.10.3 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;

11.10.4 where there has been an objection made under para 9.2 above, pending the outcome of any decision.

Right to portability

11.11 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 will be quite limited. If a request for this is made, it should be forwarded to The Data Protection Officer within 2 working 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 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 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 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 The 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 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 board and a decision made about implementation of those recommendations.

13. CCTV

13.1 We use CCTV in various locations around the school sites to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

13.2 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.

13.3 Any enquiries about the CCTV system should be directed to Adam Hewitt, DPO.

14. Photographs and videos

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

14.2 We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

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

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

14.5 Where the school takes photographs and videos, uses may include:
14.5.1 Within school on notice boards and in school magazines, brochures, newsletters, etc.;
14.5.2 Outside of school by external agencies such as the school photographer, newspapers, campaigns;
14.5.3 Online on our school website or social media pages.

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

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

14.8 See our Child Protection and Safeguarding Policy/Photography Policy for more information on our use of photographs and videos.

15. Data protection by design and default

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

15.1.1 Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge;

15.1.2 Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6);

15.1.3 Completing data protection impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process);

15.1.4 Integrating data protection into internal documents including this policy, any related policies and privacy notices;

15.1.5 Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance;

15.1.6 Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant;

15.1.7 Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply;

15.1.8 Maintaining records of our processing activities, including:

15.1.8.1 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);

15.1.8.2 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.

16. Data security and storage of records

16.1 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:

16.2.1 Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use;

16.2.2 Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access;

16.2.3 Where personal information needs to be taken off site, staff must sign it in and out from the school office;

16.2.4 Passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites;

16.2.5 Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices;

16.2.6 Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our Online Safety Policy/Acceptable Use Agreement);

16.2.7 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 (see section 8).

17. Disposal of records

17.1 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.

17.2 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.

18. Personal data breaches

18.1 The school will make all reasonable endeavours to ensure that there are no personal data breaches.

18.2 In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

18.3 When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches in a school context may include, but are not limited to:

18.3.1 A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium;

18.3.2 Safeguarding information being made available to an unauthorised person;

18.3.3 The theft of a school laptop containing non-encrypted personal data about pupils.

19. Training

19.1 All staff and governors are provided with data protection training as part of their induction process.

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

20. Monitoring arrangements

20.1 The DPO is responsible for monitoring and reviewing this policy.

20.2 This policy will be reviewed annually and approved by the full Trust board.

21. Links with other policies

21.1 This data protection policy and FOI Policy is linked to our:

21.1.1 Acceptable Use Policy

21.1.2 Protection of Biometric Information Policy

21.1.3 Child Protection and Safeguarding Policy

21.1.4 Online Safety Policy

22. Contact

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

Contact details

Name: Adam Hewitt
Role: Data Protection Officer
Contact: A.Hewitt@Lifesciencesutc.co.uk
By phone: via 0151 230 1320

Freedom of Information

1. Introduction

1.1 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.

2. What is a Request Under FOI

2.1 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 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.

2.2 In all non-routine cases, if the request is simple and the information is to be released, then the individual 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.

2.3 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 3 working days of receiving the request.

2.4 When considering a request under FOI, you must bear in mind 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 you cannot restrict access when releasing by marking the information “confidential” or “restricted”.

3. Time Limit for Compliance

3.1 The Trust/Academy 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 when calculating the 20 working day deadline, a “working day” is a school day (one in which pupils are in attendance), subject to an absolute maximum of 60 normal working days (not school days) to respond.”

4. Procedure for Dealing with a Request

4.1 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, who may re-allocate to an individual with responsibility for the type of information requested.

4.2 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.

4.3 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:

4.3.1 Section 40 (1) – the request is for the applicants personal data. This must be dealt with under the subject access regime in the DPA, detailed in paragraph 10 of the DPA policy above;

4.3.2 Section 40 (2) – compliance with the request would involve releasing third party personal data, and this would be in breach of the DPA principles as set out in paragraph 4.1 of the DPA policy above;

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

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

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

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

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

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

4.3.9 Section 36 – information which, in the opinion of the chair of governors 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.

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

5. Responding to a Request

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

5.2 The letter should end by explaining to the requestor how they can complain – either by reference to an internal review by a governor, or by writing to the ICO.

6. Contact

6.1 Any questions about this policy should be directed in the first instance to the Data Protection Officer.