Data Protection and Freedom of Information Policy

Document control table	
Document title:	Data Protection and FOI Policy
Owners (name & job title):	Katy Bradford, Deputy Chief Executive Officer
Version number:	V6
Date approved:	4 December 2025
Approved by:	Audit & Risk Committee of the OGAT Board
Date of next review:	November 2026

Document History

Version	Date	Author	Note of revisions
V6	Nov 25	Fatima Yusuf	Additional legal basis for processing added. Data Protection Lead added for primary academies. Data Subject Access Request Complaint Procedure added.

1. Introduction

1.1. Outwood Grange Academies 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 and our academies 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), Data Protection Act 2018 (DPA) and other related legislation.

1.2. The Trust is a Data Controller meaning that it is legally responsible for handling (both storing and processing) the information, referred to in clause 1.1, in accordance with all relevant legislation.

1.3. The Trust is registered as a data controller with the ICO and will renew this registration on an annual basis.

1.4. The DPA and 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.

1.5. This policy will be updated as necessary to reflect best practice, or amendments made to data protection legislation, and shall be annually.

2. Purpose and Scope of this policy

2.1. The purpose of this policy is to ensure that the Trust and all of its employees are aware of the relevant data protection legislation in force and are handling data in compliance with this legislation.

2.2. In the course of their work many Trust employees will be required to take part in the acquisition, recording, handling, storage and processing of personal data and this must always be done in accordance with this policy and the relevant legislation.

2.3. This policy will help Trust employees to understand the meaning and significance of such legislation in relation to assisting the performance of the practical duties of their employment.

2.4. The Trust will ensure that (in addition to those employees directly involved in the handling of data) all members of staff, Trustees, Academy Council Governors, volunteers, trainees, external contractors and/or consultants and any partners of the Trust who may have access to any personal data will receive appropriate information and/or training to make them fully aware of their individual and corporate responsibilities in this regard.

2.5. Such information or training will include making all employees (and others listed in the preceding clause) aware that breaches of data protection legislation have the potential to expose both the individual and the responsible organisation to possible legal action (both criminal and civil).

3. Definitions

Data controller

A data controller is the individual or the legal person who controls and is responsible for the keeping and use of the personal information in either digital or paper format (or both). A data controller determines the purposes and means of processing personal data.

Data Processor
A data processor is responsible for processing the personal data on behalf of the data controller. Data processors must maintain records of personal data and processing activities.

Data Protection Legislation
The Data Protection Act 2018, General Data Protection Regulations 2018 and the Data Use and Access Act 2025 and any other legislation from time to time in force.

Data Subject
The person who the personal data belongs to.

ICO
Information Commissioner's Office; the office responsible for monitoring compliance with data protection laws and investigating and penalising breaches.

Personal data
Personal data is any information relating to an identified or identifiable natural person (data subject) which would allow you to identify (or makes it possible to identify) that person.

Processing
Processing refers to the recording, handling, using and sharing of personal data.

Subject Access Request
A data subject's right to request access to the information that a company or organisation holds about them including why they hold this information, what they do with this information and who they share it with.

Data Protection Impact Assessment
A process to help identify and minimise the data protection risks of a project which involves data processing; particularly useful when introducing a new data processing process, system or technology.

4. Personal Data

4.1. 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 e.g. if you were 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. A subset of personal data is known as 'special category personal data'. This special category data is information that relates to:

- Race or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Physical or mental health.
- An individual's sex life or sexual orientation.
- Generic or biometric data for the purpose of uniquely identifying a natural person.

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

4.3. 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).

5. Responsibilities and Requirements

5.1. This section of the policy sets out a summary of the key responsibilities and requirements of the Trust to ensure compliance with Data Protection legislation. The policy will go on to set out information that will ensure that these are met.

5.2. As a data controller the Trust is responsible for ensuring that it only collects the required data necessary to carry out its role as an educational provider. The Trust recognises that obtaining additional data to that which is necessary is contrary to the Data Protection Laws.

5.3. The Trust is responsible for obtaining, storing and handling all personal data in a secure manner and will keep records of what data is held and the purposes for which it is held.

5.4. The Trust is responsible for ensuring that it only shares data with third parties where this is necessary for providing the full educational experience for the children. The Trust is required to ensure that it only shares that data which is required by the third party for performing its function and it shares this data in a secure way.

5.5. The Trust is responsible for ensuring that any third party accessing or processing data controlled on behalf of the Trust will do so in a safe and secure manner and in compliance with the data protection laws in force.

5.6. The Trust is required to notify data subjects as to the personal data they hold in relation to that data subject as well as the legal basis for holding that data, how the data will be used, who the data may be shared with and how it is stored. This is done in the privacy notices (please see the clause in this policy entitled 'Privacy Notices' for further information).

5.7. The Trust is required to appoint a Data Protection Officer ('DPO')(more information about the role of the data protection officer is set out under the clause entitled 'Data Protection Officer' below).

5.8. The Trust is required to register itself as a data controller with the Information Commissioner's Office.

5.9. The Trust is required to obtain full records of all personal data held and maintain these records in accordance with the Records Management and Retention policy.

5.10. The Trust has an obligation to deal with any subject access requests in a timely manner (further information regarding this is set out under the Subject Access Request clause below).

5.11. The Trustees and Executive has overall responsibility for ensuring that the Trust complies with its obligations under the relevant data protection laws and this policy.

6. The Data Protection Principles

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

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.
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. personal data shall be adequate, relevant, and limited to what is necessary for the purpose(s) for which it is being processed.
4. personal data shall be accurate and, where necessary, kept up to date.
5. personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose / those purposes.
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.

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 clause 13,14 and 15 below).

6.2. The Trust is committed to complying with the principles in 6.1 at all times. This means that the Trust will:

- Inform individuals as to the purpose of collecting any information from them, as and when we ask for it.
- be responsible for checking the quality and accuracy of the information.
- 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.
- ensure that when information is authorised for disposal it is done appropriately.
- 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.
- share personal information with others only when it is necessary and legally appropriate to do so.
- set out clear procedures for responding to requests for access to personal information known as subject access requests.
- report any breaches of the GDPR in accordance with the procedure in clause 19 below.

7. The lawful bases for processing personal data in accordance with the first data protection principle

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

7.2. 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.

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

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

7.5. 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.

7.6. 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.

7.7. The processing is necessary for the purpose of a recognised legitimate interest.

8. Use of personal data by the Academy

8.1. The Trust holds personal data on students, 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 clause 5.1 above.

Students

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

8.3. The data is used in order to support the education of the students, to monitor and report on their progress, to provide appropriate pastoral care, and to assess how well the academy as a whole is doing, together with any other uses normally associated with this provision in an academy environment.

8.4. In particular, the Academy may:

- Transfer information to any association society or club set up for the purpose of maintaining contact with students or for fundraising, marketing or promotional purposes relating to the academy but only where consent has been obtained first.
- make personal data, including sensitive personal data, available to staff for planning curricular or extracurricular activities.
- keep the student's previous school informed of his / her academic progress and achievements e.g. sending a copy of the school reports for the student's first year at the academy to their previous school.
- Use photographs of students in accordance with the photograph policy and in line with pupil/parental consent.

Any wish to limit or object to any use of personal data should be notified to the DPO in writing, such notice will be acknowledged by the DPO in writing. If, in the view of the DPO, the objection cannot be maintained, the individual will be given written reasons why the academy cannot comply with their request.

Staff

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

8.6. 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.

8.7. 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.

8.8. Any objection or request to limit the use of personal data should be directed to the DPO, who will ensure it is recorded and adhered to if appropriate. If the DPO 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.

Individuals

8.9. The Trust may hold personal information in relation to other individuals who have contact with the academies, 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.

9. Consent

9.1. The Trust must obtain consent from parents/pupils for obtaining and processing certain personal data such as the use of photographs (particularly for marketing purposes such as brochures and websites).
9.2. The consent must be freely given, specific, informed and unambiguous and confirmed by a statement or clear affirmative action.
9.3. A record must be kept of all consents provided.
9.4. A consent form must set out the ways an individual may be able to change or withdraw their consent.
9.5. Employees must seek guidance from the DPO if they have any queries relating to obtaining consent.

10. Privacy Notices

10.1. Privacy notices should be prepared by the Trust in order to inform the data subjects about the data processing it carries out.
10.2. Privacy notices must include information such as the personal data required, why that personal data is required, what the personal data will be used for, how the personal data will be stored/shared/processed, who the DPO is and the rights that an individual has in relation to their personal data.
10.3. Privacy notices should be prepared for any personal data obtained by the school but will most commonly include a privacy notice for parents/children, for staff, for governors/volunteers and for recruitment candidates.
10.4. The Trust should ensure that the data subject has access to the privacy notice, e.g. by publishing the relevant privacy notices on to the Trust website.

11. Data Protection Officer

11.1. The Trust is classed as a public authority for the purposes of the DPA and therefore requires a DPO.
11.2. A DPO should be appointed by all Trusts and schools in England and the officer should be someone who is independent from the processing of personal data.
11.3. The DPO should have specialist knowledge of data protection laws and the requirements of the Trust for compliance, and should be someone who is able to advise and influence the senior leadership of the Trust.
11.4. The DPO will assist the Trust in monitoring internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments ('DPIA')(see clause 22) and act as a point of contact for data subjects and the supervisory authority (ICO).
11.5. The DPO's details must be made available to the data subjects, this is done through the privacy notices.
11.6. Please refer to Article 39 GDPR for a further definition of the tasks of the DPO.

12. Data Protection Lead

12.1. Each academy will have a designated Data Protection Lead (DPL). The Business Managers hold this role at the secondary academies, while the Senior Administrators are the DPL at the primary academies.

12.2. The DPL will be responsible for overseeing and implementing data protection practices in accordance with relevant regulations and trust policies in the academy.

12.3. The DPL will be responsible for monitoring staff compliance with annual data protection training requirements.

12.4. The DPL will be responsible for managing and supporting the Data Protection Officer in handling Subject Access Requests and Freedom of Information Requests within the academy.

12.5. The DPL shall ensure that any data breach that occurs in their academy is reported to the Data Protection Officer.

12.6. The DPL shall serve as a primary contact for data protection inquiries within the academy.

12.7. The DPL shall ensure good record management practices within the academy.

13. Security of personal data

13.1. 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.

13.2. Clause 13.1 above refers to all personal information held, whether that data is held electronically or on paper.

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

14. Disclosure of personal data to third parties

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

- To give a confidential reference relating to a current or former employee, volunteer or student for the prevention or detection of crime.
- For the assessment of any tax or duty.
- 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).
- For the purpose of, or in connection with, legal proceedings (including prospective legal proceedings).
- For the purpose of obtaining legal advice.
- For research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress).
- To publish the results of public examinations or other achievements of students of the Trust;
- To utilise the services offered through trusted third parties (such as educational technology and software) that act as data processors to offer services that will assist and enhance the delivery of educational services.
- To disclose details of a student's medical condition where it is in the student's interests to do so, for example for medical advice, insurance purposes or to organisers of academy trips.
- To provide information to another educational establishment to which a student is transferring.

- To provide information to the Examination Authority as part of the examination process. And 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.

14.2. 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 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.

14.3. 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.

14.4. All requests for the disclosure of personal data must be sent to the Data Protection Officer (dpo@outwood.com), 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.

14.5. If the Trust is sharing personal information with a third party, the Trust will ensure that the third party is compliant with the relevant data protection legislation. The Trust will also assess whether it is necessary to have a Data Sharing Agreement (also known as a Data Processing Agreement) in place with the third party.

14.6. Any disclosure of personal data with a third party must be carried out in a secure manner. For example, using a secure portal or via secure/encrypted email.

15. Confidentiality of student concerns

15.1. Where a student 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 academy 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 academy believes disclosure will be in the best interests of the student or other students.

15.2. For further information about handling confidential information, please refer to the Confidentiality Policy.

16. Subject Access Requests

16.1. 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 1.4).

16.2. A data subject has the right to find out what data is held about them and how that data is used. An individual should make a subject access request before exercising the other information rights set out in clause 18 below.

16.3. All requests should be sent to the Data Protection Officer (dpo@outwood.com) and must be dealt with in full without delay and at the latest within one month of receipt.

16.4. Where the request relates to a child and the child or young person does not have sufficient understanding to make his or her own request (usually those under the age of 13, or over 13 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 the child or young person lacks sufficient understanding and the request made on behalf of the child or young person is in their interests.

16.5. 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 academy 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.

16.6. 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).

16.7. A subject access request can be made verbally or in writing. In order to assist individuals in making such requests and to help us with processing the request, a subject access request form has been created and can be found in the Subject Access Request Policy. The academy may ask for any further information reasonably required to locate the information.

16.8. The academy has 1 month to respond to a Subject Access Request, this can be extended by a further 2 months for complex requests.

16.9. 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.

16.10. 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.

16.11. 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.

16.12. The individual who made the request should be supplied with certain information that explains why the academy is processing their data, how the data is used and who it is shared with. Such information is set out in the Privacy Notice, found on the Trust website.

16.13. The Trust must keep a record of all subject access requests received including the date the request was made, the nature of the request and whether the request was responded to within the required timescale.

16.14. Personal data about a child belongs to that child and not the child's parents/carers. Parents are able to make a subject access request on behalf of their child as set out in clauses 16.4 and 16.5 above. If a child over 13 years of age does not consent to personal data being provided to their parent, then we are not able to provide that data unless clause 16.15 applies.

16.15. People with parental responsibility are entitled to an annual report of their child's progress and attainment in the main subject areas taught unless they expressly ask not to receive the same (s.32(1)(f) The Education (Independent School Standards) Regulations 2014). Section 5 The Education (Pupil Information)(England) Regulations 2005 does not apply.

16.16. The Trust meets its obligations as set out in clause 16.15 above by the provision of Praising Stars reports.

17. Exemptions of access to data by subjects

17.1. 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.

17.2. 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.

18. Other rights of individuals

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

Right to object to processing

18.2. 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 7.5 and 7.6 above) where they do not believe that those grounds are made out.

18.3. Where such an objection is made, it must be sent to the DPO within 2 working days of receipt, and the DPO 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.

18.4. The DPO shall be responsible for notifying the individual of the outcome of their assessment within 5 of working days of receipt of the objection.

Right to rectification

18.5. 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 DPO 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.

18.6. 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 an internal review or an appeal direct to the Information Commissioner.

18.7. 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

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

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

18.9. 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

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

- Where the accuracy of data has been contested, during the period when the Trust is attempting to verify the accuracy of the data;
- Where processing has been found to be unlawful, and the individual has asked that there be a restriction on processing rather than erasure;
- 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;
- Where there has been an objection made under para 18.2 above, pending, and subject to, the outcome of any decision.

Right to raise a complaint

18.11. How to complain to us

- If you have concerns about how your Data Subject Request has been processed you have a right to raise a complaint with us in the first instance. Click here to fill a complaint form.

How we would handle your complaint

- Once your complaint has been received, we aim to acknowledge your complaint within 15 working days. The Data Protection Officer will investigate how your request was handled and review the information provided to you. The DPO will provide you with a response within one calendar month.

How to complain to the Information Commissioner's Office

- If you are unhappy with how we have handled your complaint, you can escalate this to the ICO at; https://ico.org.uk/make-a-complaint/.

19. Breach of any requirements of the GDPR

19.1. A data breach refers to any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. It includes breaches which resulted from both accidental and deliberate causes.

19.2. If a data breach is suspected, you must report this to the DPO and your Academy Principal as soon as the breach is discovered, without delay.

19.3. Once notified, the Data Protection Officer shall assess:

- The extent of the breach;
- The risks to the data subjects as a consequence of the breach;
- Any security measures in place that will protect the information;
- Any measures that can be taken immediately to mitigate the risk to the individuals.

19.4. Unless the Data Protection Officer concludes that there is unlikely to be any risk to the individual's rights and freedoms 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.

19.5. In assessing the risk to the rights and freedoms the DPO should have regard to Recital 85 GDPR.

19.6. The Information Commissioner shall be told:

- Details of the breach, including the volume of data at risk, and the number and categories of data subjects;
- The contact point for any enquiries (which shall usually be the Data Protection Officer);
- The likely consequences of the breach;
- Measures proposed or already taken to address the breach.

19.7. 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.

19.8. Data subjects shall be told:

- The nature of the breach;
- Who to contact with any questions, this should be the DPO.
- Measures taken to mitigate any risks.

19.9. 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 Executive Team and a decision made about implementation of those recommendations.

19.10. The Trust must keep a record of all breaches, whether these required reporting to the ICO or not. This record is kept on the Trust's Data Breach Log and must include whether the matter was reported to the ICO.

19.11. For further information regarding the process for dealing with a data breach, including the form to complete if you suspect a data breach, please refer to the Trust's Data Breach Guidance and Reporting Form.

20. CCTV

20.1. The Trust may use CCTV in and around each of the Academies to ensure the safety of all children and staff whilst in the Academy. The Trust will comply with the ICO's code of practice for the use of CCTV at all times.

20.2. The Trust are not required to ask permission from individuals for using the CCTV but must make it clear that CCTV is in use. This is done by making the CCTV cameras clearly visible and by displaying signs explaining that CCTV is in use.

20.3. Whilst an individual may make a Subject Access Request to view CCTV footage, the Trust will need to consider the points made in clause 14 above in deciding whether it is appropriate to allow such a request.

20.4. Please refer to the Trust's CCTV policy for further information on the use of CCTV.

21. Recording of meetings and conversations

21.1. Under data protection legislation, an audio or video recording of a conversation where any individual can be identified from the recording and/or the conversation is the personal data of that individual.

21.2. You must have an appropriate lawful basis for recording the conversation and individuals must be aware that they are being recorded. Consent will likely be the most relevant basis for processing.

21.3. If an individual does not know in advance that his or her conversation is being recorded, and a lawful basis for processing has not been identified, then that individual's rights to 'fair and lawful processing' will have been breached and this would need to be reported to the ICO.

22. Data Protection Impact Assessments (DPIAs)

22.1. A Data Protection Impact Assessment (DPIA) is a process whereby potential privacy issues and risks are identified and examined from the perspective of all stakeholders and allows the Trust to anticipate and address the likely impacts of new initiatives and put in place measures to minimise or reduce the risks.

22.2. As the use of technology and the collection and storage of personal data grows, the need to ensure that it is properly managed and maintained increases. It is a requirement of GDPR that a Data Protection Impact Assessment (DPIA) is carried out in certain circumstances.

22.3. The impact assessment covers not only the protection of personal data but broader privacy of individuals and therefore could also be referred to as a Privacy Impact Assessment (PIA). These procedures are designed to minimise the risk of harm that can be caused by the use or misuse of personal information by addressing data protection and privacy concerns at the design and development stage of a project.

22.4. Conducting a DPIA should benefit the Trust by managing risks, avoiding unnecessary costs, avoiding damage to reputation, ensuring legal obligations are met and improving the relationship with stakeholders. The term project is used in a broad and flexible way and means any plan or proposal.

22.5. Examples of the types of projects that need a DPIA are:

- A new IT system storing and accessing personal data
- A data sharing initiative where two or more organisations seek to pool or link sets of personal data
- A proposal to identify people in a particular group or demographic and initiate a course of action (e.g. identifying students believed to be at risk)
- A new surveillance system such as CCTV
- A new database which consolidates information held by separate parts of an organisation

22.6. When does a DPIA need to be done?

A DPIA should be done as part of the initial phase of a project to ensure that risks are identified and taken into account before the problems become embedded in the design and cause higher costs due to making changes at a later stage. Also, if there is a change to the risk of processing for an existing project, a review should be carried out. In the context of this guidance a project could include the development or enhancement of any activity, function or processing such as a system, database, programme, application, service or scheme.

22.7. The time and effort put into carrying out the DPIA should be proportionate to the risks. A DPIA does not have to be conducted as a completely separate exercise and it can be useful to consider privacy issues in a broader policy context such as information security. The DPIA does not necessarily need to start and finish before a project can progress further but it can run alongside the project development process.

22.8. The GDPR requires that a DPIA is carried out in the following cases:

- When the processing involves systematic and extensive evaluation of personal information particularly in cases of automatic processing or profiling where decisions are made that could have a significant or legal impact on an individual.
- When processing on a large scale of special categories of data or data relating to criminal convictions and offences
- The monitoring of a publicly accessible area on a large scale
- Any other cases specified by the Information Commissioner

22.9. It is the responsibility of the person leading the project to carry out a DPIA. As part of the process the Data Protection Officer must be consulted but it is not the Data Protection Officer who carries out the DPIA.

22.10. The Assessment should be signed off by the SIRO or Director of Data before data is shared.

23. Data Protection by Design and Default

23.1. Data Protection by design (also called Privacy by design) is an approach to handling personal data that promotes privacy and data protection compliance from the start rather than considered as an afterthought. All staff and agents of the Trust are required to apply the data protection by design principles when developing a new project or reviewing existing projects that involve the use or storage of personal data.

23.2. The guidelines below explain the types of project when this might be relevant, what data protection by design is and what measures can be put in please to protect personal data.

23.3. Under GDPR the Trust has an obligation to consider data privacy during the initial design stages of a project as well as throughout the lifecycle of the relevant data processing. By imposing a specific 'privacy by design' requirement, the GDPR emphasises the need to implement appropriate technical and organisational measures to ensure that privacy and the protection of data is not an after-thought.

23.4. Examples of the types of projects where privacy should be considered include:

- Building new IT systems for storing or accessing personal data
- Developing policies or strategies that have privacy implications
- Embarking on a data sharing initiative
- Using data for new purposes

23.5. In addition to meeting legal requirements, taking a proactive approach to privacy will reduce the likelihood of fines or financial losses due to data protection breaches and help build reputation and stakeholder confidence.

23.6. Privacy by Design is an approach to protecting privacy by embedding it into the design specifications of technologies, business practices and physical infrastructure. This means building in privacy during the design phase of any project. Seven foundation principles of Privacy by Design were first developed by Dr Ann Cavoukian in the 1990s.

23.7. These can be summarised as:

- Use proactive rather than reactive measures - anticipate, identify and prevent privacy invasive events before they happen.
- Privacy should be the default position - personal data must be automatically protected in any system of business practice, with no action required by the individual to protect their privacy.

- Privacy must be embedded and integrated into the design of systems and business practices.

- All legitimate interests and objectives are accommodated in a positive-sum manner - both privacy and security are important, and no unnecessary trade-offs need to be made to achieve both.
- Security should be end-to-end throughout the entire lifecycle of the data - data should be securely retained as needed and destroyed when no longer needed.
- Visibility and transparency are maintained - stakeholders should be assured that business practices and technologies are operating according to objectives and subject to independent verification.
- Respect user privacy by keeping the interests of the individual uppermost with strong privacy defaults, appropriate notice and user friendly options.

23.8. Data Protection Impact Assessment (DPIA) (see clause 22) should be carried out as part of the initial phase of a project or when an existing project is being reviewed. If data protection or privacy implications are identified then measures should be built into the project during the early stages to ensure that risks to privacy are minimised or eliminated.

23.9. Below are some examples of measures that can be taken during the project development or review to protect the personal data of individuals, not all these examples will be applicable in all circumstances:

- Data minimisation – this includes retention minimisation (only keeping personal data for as long as it is required), collection minimisation (only collecting the personal information that is required) and use minimisation (only use personal data when it is absolutely required therefore reducing the chance of individuals being identified).
- Deletion – Having automated deletion processes for particular personal data to ensure it is flagged for deletion after a particular period.
- Anonymisation – The data is held in a form where the individuals are no longer identifiable and it is unlikely that any individuals can be re-identified by combining the data with other data e.g. data matching. The GDPR emphasises that anonymization or pseudonymisation should be used wherever possible particularly in relation to historical or scientific research or for statistical purposes.
- Pseudonymisation – The identity of an individual is disguised for instance by replacing identifying fields with artificial identifiers or pseudonyms. When data has been pseudonymised it still retains a level of detail which allows tracking back of the data to its original state. This is in contrast to anonymised data where reverse compilation should be impossible.
- Differential privacy – Random 'noise' is injected into the results of dataset queries to provide a mathematical guarantee that the presence of any one individual in a dataset will be masked. This technique may be useful for research data. Software evaluates the privacy risks or a query and determines the level of noise to introduce into the result before releasing it.
- Synthetic data – As long as the number of individuals in the dataset is large enough, it is possible to generate a dataset composed entirely of 'fictional' individuals or altered identities that retain the statistical properties of the original dataset.
- Privacy by Default – The system is set up so the default settings are the ones that provide maximum protection against privacy risks i.e. technical and organisational measures are put in place to ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed. This may mean that the default position would not allow full functionality of the product, unless the user explicitly chooses it.

- User Access controls – The amount of personal data that authorised users have access to should be limited to the information they need to know to fulfil their roles.
- Data subject Access - Individuals should be able to access their own personal data and be informed of its use and disclosures. If individual users can't access the systems directly themselves it should be set up in a way that allows data to be collated with ease in order to comply with subject access requests.
- User friendly systems – Privacy related functions should be user friendly. For instance users should be able to easily update their details or extract information that relates to them.
- Accuracy – The design should incorporate checks to ensure accuracy and completeness of data and that it is as up-to-date as is necessary to fulfil the specified purposes.
- Compliance – The design should include processes to monitor, evaluate, and verify compliance (e.g. with legal requirements, policies and procedures).
- State of the art – State of the art technology and organisation measures should be used where possible, however this needs to be balanced against reasonable costs. Old technology should be replaced where possible and software and patches kept up-to-date. In deciding what measures are appropriate, account should be taken of the nature, scope, context and purposes of processing as well as the risks, likelihood and severity for the rights and freedoms of individuals.
- Security – Security measures should include processes for secure destruction, appropriate encryption, and strong access control and logging methods.
- Suppression of data – The system should be set up to allow the suppression of data of individuals who have objected to receiving direct marketing or those who want to object to decisions being made about them based on automated processing including profiling. Where appropriate the system should also allow data portability in accordance with the GDPR and the right of individuals to request the transmission of their personal data to another data controller in a machine-readable format.
- Data processors – Contracts with data processors need to set out how risk/liability will be apportioned between the parties in relation to implementation of 'privacy by design' and 'privacy by default' requirements.
- Tenders – Privacy issues should be considered as part of public tenders.
- Transfers outside EEA – Particular consideration should be given to protecting personal data when data is likely to be transferred outside the EEA.

23.10. These are some example measures that can be taken and not all of them will be appropriate for every project or system, however, it is likely that most projects will benefit from taking some of the steps outlined above. The DPIA should be used to record the privacy measures that are designed into the project.

24. Remote Working

24.1. If a staff member is required to work remotely and that work involves the processing of personal data, then the staff member should ensure that such data is processed in a secure manner.

24.2. Remote working should be carried out on a password protected laptop/computer and, where possible, personal information should not be saved anywhere other than the Trust's secure network.

24.3. When processing personal data remotely, staff should not allow other people to view the personal data.

24.4. When working remotely, if a staff member is required to share personal data, they should ensure that they adopt a secure method of data sharing and adhere to the basis for sharing as set out in the privacy notice.

24.5. Staff should have regard to the IT/ Staff Acceptable Use Policy and the Records Management and Retention Policy.

25. Breach of Policy

25.1. The DPO and Deputy Chief Executive Office (DCEO) are responsible for reviewing and monitoring compliance with this policy.

25.2. Any breaches of this policy should be reported to the DPO to be investigated. A breach of this policy could lead to a report being made to the ICO, a report being made to HR to follow the disciplinary procedure or both.

26. Contact

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