# Data Protection and Freedom of Information Policy

| Document control table | |
|---|---|
| **Document title:** | Data Protection and FOI Policy |
| **Author (name & job title):** | Katy Bradford |
| **Version number:** | V3 |
| **Date approved:** | 18 May 2020 |
| **Approved by:** | OGAT Board |
| **Date of review:** | May 2022 |

**Document History**

| Version | Date | Author | Note of revisions |
|---|---|---|---|
| V1 | 5.2.18 | KB | This policy replaces and combines the previous Data Protection Policy and the FOI Publication Scheme. Updated to be GDPR compliant. |
| V2 | 23.9.19 | KB | Section added on DPIA and Privacy by Design |
| V3 | 18.5.20 | KB | Recording of meetings section added |

# DATA PROTECTION

## 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) and other related legislation.

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

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

## 2. Personal Data

2.1. 'Personal data' is information that identifies an individual, and includes information that would identify an individual to the person to whom it is disclosed because of any special knowledge that they have or can obtain[1]. A subset of personal data is known as 'special category personal data'. This special category data is information that relates to:

2.1.1. race or ethnic origin;

2.1.2. political opinions;

2.1.3. religious or philosophical beliefs;

2.1.4. trade union membership;

2.1.5. physical or mental health;

2.1.6. an individual's sex life or sexual orientation;

2.1.7. generic or biometric data for the purpose of uniquely identifying a natural person

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

[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.

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

2.4. The Trust does not intend to seek or hold 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).

## 3. The Data Protection Principles

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

3.1.1. Personal data shall be processed fairly, lawfully and in a transparent manner, and processing shall not be lawful unless one of the processing conditions can be met;

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

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

3.1.4. personal data shall be accurate and, where necessary, kept up to date;

3.1.5. personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose / those purposes;

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

3.2. In addition to this, the Trust is committed to ensuring that 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 7 and 8 below).

3.3. The Trust is committed to complying with the principles in 3.1 at all times. This means that the Trust will:

3.3.1. inform individuals as to the purpose of collecting any information from them, as and when we ask for it;

3.3.2. be responsible for checking the quality and accuracy of the information;

3.3.3. 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;

3.3.4. ensure that when information is authorised for disposal it is done appropriately;

3.3.5. 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;

3.3.6. share personal information with others only when it is necessary and legally appropriate to do so;

3.3.7. set out clear procedures for responding to requests for access to personal information known as subject access requests;

3.3.8. report any breaches of the GDPR in accordance with the procedure in paragraph 9 below.

## 4. Conditions for processing in the first data protection principle

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

4.2. 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.

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

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

4.5. 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.

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

## 5. Use of personal data by the Academy

5.1. 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 paragraph 3.1 above.

## Students

5.2. 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.

5.3. 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.

5.4. In particular, the Academy may:

5.4.1. 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;

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

5.4.3. 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;

5.4.4. Use photographs of students in accordance with the photograph policy.

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

## Staff

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

5.7. 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.

5.8. 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.

5.9. Any wish to limit or object to the uses to which personal data is to be put should be notified to the Director of Human Resources who will ensure that this is recorded, and adhered to if appropriate. If the Director of Human Resources 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

5.10. 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.

## 6. Security of personal data

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

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

## 7. Disclosure of personal data to third parties

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

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

7.1.2. For the prevention or detection of crime;

7.1.3. For the assessment of any tax or duty;

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

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

7.1.6. For the purpose of obtaining legal advice;

7.1.7. For research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress);

7.1.8. To publish the results of public examinations or other achievements of students of the Trust;

7.1.9. 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;

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

7.1.11. To provide information to the Examination Authority as part of the examination process; and

7.1.12. 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.

7.2. The DfE uses information about students for statistical purposes, to evaluate and develop education policy and to monitor the performance of the nation's education service as a whole. The statistics are used in such a way that individual 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.

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

7.4. All requests for the disclosure of personal data must be sent to the Academy Principal, 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.

## 8. Confidentiality of student concerns

8.1. 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.

8.2. 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 1.5).

8.3. All requests should be sent to the Academy Principal and must be dealt with in full without delay and at the latest within one month of receipt.

8.4. 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 Academy Principal must, however, be satisfied that:

8.4.1. the child or young person lacks sufficient understanding; and

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

8.5. 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 Academy Principal must be confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates.

8.6. 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).

8.7. A subject access request must be made in writing. The academy may ask for any further information reasonably required to locate the information.

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

8.9. 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.

8.10. All files must be reviewed by the Academy Principal before any disclosure takes place. Access will not be granted before this review has taken place.

8.11. 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.

## 9. Exemptions of access to data by subjects

9.1. 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.

9.2. 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.

## 10. Other rights of individuals

10.1. 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:

10.1.1. object to processing;

10.1.2. rectification;

10.1.3. erasure; and

10.1.4. data portability

### Right to object to processing

10.2. 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 4.5 and 4.6 above) where they do not believe that those grounds are made out.

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

10.4. The Academy Principal 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

10.5. 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 Academy Principal 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.

10.6. 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.

10.7. 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

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

10.8.1. Where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed;

10.8.2. Where consent is withdrawn and there is no other legal basis for the processing;

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

10.8.4. personal data is being unlawfully processed (usually where one of the conditions for processing cannot be met);

10.8.5. Where there is a legal obligation on the Trust to delete.

10.9. 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

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

10.10.1. Where the accuracy of data has been contested, during the period when the Trust is attempting to verify the accuracy of the data;

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

10.10.3. 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;

10.10.4. Where there has been an objection made under para 8.2 above, pending the outcome of any decision.

## 11. Breach of any requirement of the GDPR

11.1. Any there has been an objection made under para 8.2 above, pending the outcome of any decision.

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

11.2.1. The extent of the breach;

11.2.2. The risks to the data subjects as a consequence of the breach;

11.2.3. Any security measures in place that will protect the information;

11.2.4. Any measures that can be taken immediately to mitigate the risk to the individuals.

11.3. 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.

11.4. The Information Commissioner shall be told:

11.4.1. Details of the breach, including the volume of data at risk, and the number and categories of data subjects;

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

11.4.3. The likely consequences of the breach;

11.4.4. Measures proposed or already taken to address the breach.

11.5. 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.

11.6. Data subjects shall be told:

11.6.1. The nature of the breach;

11.6.2. Who to contact with any questions

11.6.3. Measures taken to mitigate any risks.

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

## 12. Data Protection Impact Assessments (DPIAs)

12.1 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.

12.2 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.

12.3 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.

12.4 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.

12.5 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

12.6 When does a DPIA need to be done?

12.6.1 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 causes 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.

12.6.2 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.

12.7 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

12.8 The Assessment 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.

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

13 Data Protection by Design and Default

13.1 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 involves the use or storage of personal data.

13.2 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.

13.3 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.

13.4 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

13.5 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.

13.6 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.

13.7 These can be summarised as:

1 Use proactive rather than reactive measures - anticipate, identify and prevent privacy invasive events before they happen.

2 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

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

4 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.

5 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.

6 Visibility and transparency are maintained - stakeholders should be assured that business practices and technologies are operating according to objectives and subject to independent verification.

7 Respect user privacy by keeping the interests of the individual uppermost with strong privacy defaults, appropriate notice and user friendly options.

13.8 Data Protection Impact Assessment (DPIA) (see section 8) 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.

13.9 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:

13.9.1 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) and use minimisation (only use personal data when it is absolutely required therefore reducing the chance of individuals being identified).

13.9.2 Deletion – Having automated deletion processes for particular personal data to ensure it is flagged for deletion after a particular period.

13.9.3 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.

13.9.4 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.

13.9.5 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.

13.9.6 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.

13.9.7 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.

13.9.8 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.

13.9.9 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.

13.9.10 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.

13.9.11 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.

13.9.12 Compliance – The design should include processes to monitor, evaluate, and verify compliance (e.g. with legal requirements, policies and procedures)

13.9.13 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.

13.9.14 Security – Security measures should include processes for secure destruction, appropriate encryption, and strong access control and logging methods.

13.9.15 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.

13.9.16 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.

13.9.17 Tenders – Privacy issues should be considered as part of public tenders.

13.9.18 Transfers outside EEA – Particular consideration should be given to protecting personal data when data is likely to be transferred outside the EEA.

13.10 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.

## 13. Recording of meetings or conversations

15.1 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.

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.

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.

## 14. Contact

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

# 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 Academy Principal.

2.3. All other requests should be referred in the first instance to the Academy Principal, 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 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 reallocate 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 spreadsheet and release the total figures, this would be information "held" by the Trust. If the Trust would have to go through a number of spreadsheets 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 applicant's personal data. This must be dealt with under the subject access regime in the DPA, detailed in paragraph 9 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 3.1 of the DPA policy above;

4.3.3. Section 41 – information that has been sent to the Academy (but not the Academy'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 Academy intends to publish at a future date;

4.3.6. Section 43 – information that would prejudice the commercial interests of the Academy 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 Academy, would prejudice the effective conduct of the Academy. 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. Dealing with Vexatious or Repeated Requests

Should an applicant make a 'vexatious' or 'repeated' request for identical or substantially similar information, the academy/trust will inform the applicant in writing that they will not fulfil the request. When responding in this manner we will offer assistance to the individual, by indicating why they consider the request is vexatious or repeated.

## 7. Contact

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