

Ormiston Academies Trust

Data Protection and Freedom of Information policy

Policy version control

Policy type	Statutory
Author	Alexandra Coughlan OAT Data Protection and Complaints Manager
Approved by	James Miller, May 22
Release date	May 2022
Review	Policies will be reviewed in line with OAT's internal policy schedule and/or updated when new legislation comes into force
Description of changes	Changes made May 2022 Appendix 1

Contents

Data Protection	3
1. Introduction	3
2. Personal data.....	3
3. Data protection principles.....	4
4. Conditions for processing fairly, lawfully and in a transparent manner	5
5. Use of personal data by Ormiston Academies Trust	6
Pupils.....	7
Workforce	7
Information relating to DBS checks	8
Other Individuals	8
6. Security of personal data	8
7. Data minimisation and pseudonymisation	8
8. Data protection impact assessments.....	8
9. Disclosure of personal data to third parties	9
10. Confidentiality of pupil concerns	10
11. Subject access requests.....	10
12. Exemptions to access by data subjects	11
13. Other rights of individuals	11
Right to object to processing.....	12
Right to rectification	12
Right to erasure	12
Right to restrict processing.....	12
Right to portability	13
14. Breach of any requirement of the UK GDPR	13
15. Data Protection Training	14
16. Contact.....	14
Freedom of Information and Environmental Information Regulations	15
1. Introduction.....	15
2. What is a request under FOI?	15
3. What is a request under the EIR?	15
4. Time limit for compliance	16
5. Procedure for dealing with a request.....	16
6. Responding to a request.....	17
7. Contact	17
8. Appendix 1.....	18

Data Protection

1. Introduction

- 1.1. The Ormiston Academies Trust (referred to as “The Trust” and any or all of its Academies) collects and uses certain types of personal information about staff, pupils, parents, and other individuals who come in contact with its Academies, in order to provide education and associated functions. Ormiston Academies 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, securely and in accordance with the United Kingdom General Data Protection Regulation (UK GDPR) and other related legislation.
- 1.2. The UK GDPR applies to all computerised data and manual files that 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 by a specific criterion.
- 1.3. All staff are required to read and confirm that they understand this policy.
- 1.4. This policy will be updated as necessary to reflect best practice, or amendments made to data protection legislation, this policy will be reviewed and updated as necessary every twelve months.

2. Personal data

- 2.1. ‘Personal data’ is information that identifies an individual. This includes information that would identify an individual because of any special knowledge that they have or can obtain¹. A sub-set of personal data is known as ‘special category personal data’. This special category data is information that reveals:
 - 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. Genetic or biometric data for the purpose of uniquely identifying a natural person.
- 2.2. Special Category Data is given special protection, and additional safeguards apply if this information is to be collected and used.
- 2.3. Information relating to criminal convictions shall only be held and processed where there is legal authority to do so.
- 2.4. The Academy does not intend to seek or hold Special Category Data (previously known as sensitive personal data) about staff or students except where the Academy has been notified of

¹ For example, if asked for information regarding all female employees, and you only have one female employee, this would be personal data

the information, or it comes to the Academy'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 pupils are under no obligation to disclose to the Academy their race or ethnic origin, political or religious beliefs, whether 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. Data protection principles

3.1. The six data protection principles as laid down in the UK GDPR are always followed:

- 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 in a form which permits identification of individuals 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 Ormiston Academies Trust is always committed to ensuring that, anyone dealing with personal data shall be mindful of the individual's rights under the law (as explained in more detail in paragraphs 11 and 13 below).

3.3. Ormiston Academies Trust and its Academies is always committed to complying with the principles in 3.1. This means that the Ormiston Academies Trust will:

- 3.3.1. Inform individuals about how and why we process their personal data through the privacy notices which we issue;
- 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 always follow the relevant security policy requirements;
- 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 UK GDPR in accordance with the procedure in paragraph 14 below.

4. Conditions for processing fairly, lawfully and in a transparent manner

- 4.1. The individual has given consent that is specific to the processing activity, and that consent is specific, 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 our legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if we are processing data to perform our official tasks.)

4.7 Special category data

4.8 Special category data is personal data that needs more protection because it is sensitive. In order to lawfully process special category data, we must identify both a lawful basis under Article 6 of the UK GDPR (see section 4.1-4.6 above) and a separate condition for processing under Article 9. These do not have to be linked.

4.9 There are 10 conditions for processing special category data in Article 9 of the UK GDPR. Five of these require us to meet additional conditions and safeguards set out in UK law, in Schedule 1 of the Data Protection Act 2018.

4.10 The UK GDPR defines special category data as:

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- data concerning health;
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

This does not include personal data about criminal allegations, proceedings or convictions, as separate rules apply.

4.11 In order for processing special category data to be lawful, one of the following conditions must be met:

- (a) Explicit consent
- (b) Employment, social security and social protection (if authorised by law)
- (c) Vital interests
- (d) Not-for-profit bodies
- (e) Made public by the data subject
- (f) Legal claims or judicial acts
- (g) Reasons of substantial public interest (with a basis in law)
- (h) Health or social care (with a basis in law)
- (i) Public health (with a basis in law)
- (j) Archiving, research and statistics (with a basis in law)

4.12 If we are relying on conditions (b), (h), (i) or (j), we also need to meet the associated condition in UK law, set out in Part 1 of Schedule 1 of the DPA 2018.

4.13 If we are relying on the substantial public interest condition in Article 9(2)(g), we also need to meet one of 23 specific substantial public interest conditions set out in Part 2 of Schedule 1 of the DPA 2018.

4.14 What are the substantial public interest conditions?

4.15 The 23 substantial public interest conditions are set out in paragraphs 6 to 28 of Schedule 1 of the DPA 2018:

- 6. Statutory and government purposes
- 7. Administration of justice and parliamentary purposes
- 8. Equality of opportunity or treatment
- 9. Racial and ethnic diversity at senior levels
- 10. Preventing or detecting unlawful acts
- 11. Protecting the public
- 12. Regulatory requirements
- 13. Journalism, academia, art and literature
- 14. Preventing fraud
- 15. Suspicion of terrorist financing or money laundering
- 16. Support for individuals with a particular disability or medical condition
- 17. Counselling
- 18. Safeguarding of children and individuals at risk
- 19. Safeguarding of economic well-being of certain individuals
- 20. Insurance
- 21. Occupational pensions
- 22. Political parties
- 23. Elected representatives responding to requests
- 24. Disclosure to elected representatives
- 25. Informing elected representatives about prisoners
- 26. Publication of legal judgments
- 27. Anti-doping in sport
- 28. Standards of behaviour in sport

5. Use of personal data by Ormiston Academies Trust

5.1. Ormiston Academies Trust processes personal data on pupils, staff and other individuals such as parents and visitors. In each case, the personal data must be processed in accordance with the data protection principles as outlined in paragraph 3.1 above.

Pupils

- 5.2. The personal data held regarding pupils includes contact details, assessment / examination results, attendance information, characteristics such as ethnic group, special educational needs, any relevant medical information, and photographs.
- 5.3. The data is used in order to support the education of the pupils, to monitor and report on their progress, to provide appropriate pastoral care, and to assess how well any of the Trust's Academies are performing as a whole is doing, together with any other uses normally associated with this provision in an educational environment.
- 5.4. The Ormiston Academies Trust may make use of limited personal data (such as contact details) relating to pupils, and their parents or carers for fundraising, marketing or promotional purposes and to maintain relationships with pupils of the Academy, but only where consent has been provided to this.
- 5.5. Ormiston Academies Trust may:
 - 5.5.1. Transfer information to any association, society or club that is set up for the purpose of maintaining contact with pupils or for fundraising, marketing or promotional purposes relating to Ormiston Academies Trust but only where consent has been obtained first;
 - 5.5.2. Make personal data, including sensitive personal data, available to staff for planning curricular or extra-curricular activities;
 - 5.5.3. Keep the pupil's previous school informed of his / her academic progress and achievements e.g. sending a copy of the school reports for a pupil's first year to their previous school;
 - 5.5.4. Use photographs of pupils in accordance with the photograph and video policy;
 - 5.5.5. Use biometric technology in accordance with the biometrics policy
- 5.6. Any wish to limit or object to any use of personal data should be notified to the Data Protection Lead who will consult the Data Protection Officer. This can be verbal or in writing. Notice will be acknowledged by Ormiston Academies Trust in writing. If, in the view of the Data Protection Officer, the objection cannot be maintained, the individual will be given written reasons why Ormiston Academies Trust cannot comply with their request.

Workforce

- 5.7. The personal data held about staff will include contact details, employment history, information relating to career progression, performance management, information relating to DBS checks, and photographs and occupational pensions.
- 5.8. The data is used to comply with legal obligations placed on the Trust in relation to employment, and the education of children in a school environment. The Trust may pass information to other regulatory authorities, where appropriate, and may use names and photographs of staff in publicity and promotional material. Personal data will also be used when giving references.
- 5.9. Staff should note that information about disciplinary action may be kept for longer than the duration of the sanction. Although treated as "spent" once the period of the sanction has expired, the details of the incident may need to be kept for a longer period.
- 5.10. Any wish to limit or object to the uses to which personal data is to be put should be notified to the Data Protection Officer (dpo@ormistonacademies.co.uk), who will ensure that this is recorded and adhered to, if appropriate. If the Data Protection Officer is of the view that it is not

appropriate to limit the use of personal data in the way specified, the individual will be given written reasons why the Trust cannot comply with their request.

Information relating to DBS checks

- 5.11. DBS checks are carried out on the basis of the academy trust's legal obligations in relation to the safer recruitment of Staff as stipulated in the Independent School Standards Regulations and the DBS information (which will include personal data relating to criminal convictions and offences) is further processed in the substantial public interest, with the objective of safeguarding children. Retention of the information is covered by the Records Retention Policy.
- 5.12. Access to the DBS information is restricted to those staff who have a genuine need to have access to it for their job roles. In addition to the provisions of the UK GDPR and the Data Protection Act 2018, disclosure of this information is restricted by section 124 of the Police Act 1997 and disclosure to third parties will only be made if it is determined to be lawful.

Other Individuals

- 5.13. Ormiston Academies Trust or any of its Academies may hold personal information in relation to other individuals who have contact with the Academy, 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. Ormiston Academies Trust will take reasonable steps to ensure that members of staff will only have access to personal data as necessary for them to carry out their duties. All staff will be made aware of this Policy and their duties under the UK GDPR. Ormiston Academies 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 ICT systems, please refer to the eSafety and eSecurity policy.

7. Data minimisation and pseudonymisation

- 7.1. Ormiston Academies Trust will ensure that it only processes the data that is necessary to achieve the specific purpose.
- 7.2. In order to do this, the Trust will:
 - 7.2.1. Minimise the processing of personal data, for example, through redaction and the deletion of long emails trails.
 - 7.2.2. Pseudonymise personal data where possible, for example, using a key rather than full names eg child 1, child 2 etc.

8. Data protection impact assessments

- 8.1. Where processing of personal data is likely to result in a high risk to individuals, Ormiston Academies Trust will carry out a data protection impact assessment (“DPIA”). A DPIA will always be carried out if the processing includes special category data.
- 8.2. Ormiston Academies Trust may also carry out a DPIA for any other major project which requires the processing of personal data.

9. Disclosure of personal data to third parties

- 9.1. The following list includes the most usual reasons that Ormiston Academies Trust will authorise disclosure of personal data to a third party:
 - 9.1.1. For the prevention or detection of crime;
 - 9.1.2. For the assessment of any tax or duty;
 - 9.1.3. 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);
 - 9.1.4. For the purpose of, or in connection with, legal proceedings (including prospective legal proceedings);
 - 9.1.5. For the purpose of obtaining legal advice;
 - 9.1.6. For research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress);
 - 9.1.7. To publish the results of public examinations or other achievements of pupils of the Trust;
 - 9.1.8. To disclose details of a pupil's medical condition where it is in the pupil's interests to do so and there is a legal basis for doing so, for example for medical advice, insurance purposes or to organisers of school trips; The legal basis will vary in each case but will usually be based on explicit consent, the vital interests of the child or reasons of substantial public interest (usually safeguarding the child or other individuals) to provide information to another educational establishment to which a pupil is transferring;
 - 9.1.9. To provide information to the Examination Authority as part of the examination process; and
 - 9.1.10. 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).
 - 9.1.11. The Examination Authority may also pass information to the DfE.
- 9.2. The DfE uses information about pupils for statistical purposes, to evaluate and develop education policy and to monitor the performance of the nation's education service as a whole. The statistics are used in such a way that individual pupils cannot be identified from them. On occasion the DfE may share the personal data with other Government Departments or agencies strictly for statistical or research purposes.
- 9.3. Through any of its Academies, Ormiston Academies Trust may receive requests from third parties (i.e. those other than the data subject, the Academy, and employees of the Academy) to disclose personal data it holds about pupils, their parents or guardians, staff or other individuals. This information will not generally be disclosed unless one of the specific exemptions under data protection legislation which allow disclosure applies; or where necessary for the legitimate interests of the individual concerned or Ormiston Academies Trust or one of its Academies.
- 9.4. The Principal has the authority to make decisions about systematic sharing or one-off disclosures and must liaise with their Data Protection Lead and Trust's Data Protection Officer before making their final decision. All requests for the disclosure of personal data must be sent to the Principal or Data Protection lead who will review with the Data Protection Officer, who will then decide

whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of that third party before making any disclosure.

10. Confidentiality of pupil concerns

10.1. Where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents or carer, the Trust will maintain confidentiality unless it has reasonable grounds to believe that the pupil does not fully understand the consequences of withholding their consent, or where the Trust believes disclosure will be in the best interests of the pupil or other pupils. Please also refer the OAT policy on child protection. Disclosure for a safeguarding purpose will be lawful because it meets a condition for processing under the substantial public interest article 9 lawful basis.

11. Subject access requests

11.1. The individual's full subject access right is to know:

- Whether personal data about him or her are being processed
- The purposes of the processing
- The categories of personal data concerned
- The recipients or categories of recipient to whom their personal data have been or will be disclosed
- The envisaged period for which the data will be stored or where that is not possible, the criteria used to determine how long the data are stored
- The existence of a right to request rectification or erasure of personal data or restriction of processing or to object to the processing
- The right to lodge a complaint with the Information Commissioner's Office
- Where the personal data are not collected from the individual, any available information as to their source
- Details of the safeguards in place for any transfers of their data to locations outside the European Economic Area.

11.2. Anybody who makes a request to see any personal information held about them by Ormiston Academies 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, if they constitute a "filing system" (see clause 1.2).

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

11.4. Where a child or young person does not have sufficient understanding to make his or her own request (usually those under the age of 12, or over 12 but with a special educational need which makes understanding their information rights more difficult), a person with parental responsibility can make a request on their behalf. The Data Protection Officer will liaise with the Academy to satisfy that:

- 11.4.1. The child or young person lacks sufficient understanding; and
- 11.4.2. The request made on behalf of the child or young person is in their interest.

11.5. 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,

Ormiston Academes Trust must have written evidence that the individual has authorised the person to make the application and the Data Protection Officer with assistance from the Academy must be confident of the identity of the individual making the request and of the authorisation by the individual to whom the request relates.

- 11.6. Access to records will be refused in instances where an exemption applies, for example, where information sharing may place the individual at risk of significant harm or jeopardise police investigations into any alleged offence(s).
- 11.7. A subject access request may be made verbally or in writing. For clarity, we prefer requests to be made in writing where possible. Ormiston Academies Trust may ask for any further information reasonably required to locate the information but only where there is a need.
- 11.8. An individual only has the 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.
- 11.9. Any complex files must be reviewed by the Data Protection Lead or Data Protection Officer before any disclosure takes place. Access will not be granted before this review has taken place.
- 11.10. Where all the data in a document cannot be disclosed, a permanent copy should be made, and the data permanently 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.
- 11.11. Parents at academy schools do not have an automatic right to their child's data (maintained schools are subject to separate regulations regarding children's education records). A request for the educational record of a pupil will be treated in the same way as a SAR. The academy will seek consent from a pupil with capacity (which will be considered on a case by case basis but is generally presumed around the age of 12 and respond to the request within one month of receiving this).

12. Exemptions to access by data subjects

- 12.1. 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.
- 12.2. 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.

13. Other rights of individuals

- 13.1. 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:
 - 13.1.1. Object to processing;
 - 13.1.2. Rectification;
 - 13.1.3. Erasure;

- 13.1.4. Restriction of processing; and
- 13.1.5. Data portability.

Right to object to processing

- 13.2. 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 adequately established.
- 13.3. Where such an objection is made, it must be sent to the Trust's Data Protection Officer within 2 working days of receipt, and the objection will be assessed to determine 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.
- 13.4. The Data Protection and Complaints team will be responsible for notifying the individual of the outcome of their assessment within fifteen working days of receipt of the objection.

Right to rectification

- 13.5. 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 Trusts Data Protection Officer within 2 working days of receipt, and where adequate proof of inaccuracy is given, the data shall be amended as soon as reasonably practicable, and the individual notified.
- 13.6. 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.
- 13.7. 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

- 13.8. Individuals have a right, in certain circumstances, to have data permanently erased without undue delay. This right arises in the following circumstances:
 - 13.8.1. Where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed;
 - 13.8.2. Where consent is withdrawn and there is no other legal basis for the processing;
 - 13.8.3. Where an objection has been raised under the right to object, and found to be legitimate;
 - 13.8.4. Where personal data is being unlawfully processed (usually where one of the conditions for processing cannot be met);
 - 13.8.5. Where there is a legal obligation on the Trust to delete.
- 13.9. The Data Protection Officer will decide 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

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

- 13.10.1. Where the accuracy of data has been contested, during the period when the Trust is attempting to verify the accuracy of the data;
- 13.10.2. Where processing has been found to be unlawful, and the individual has asked that there be a restriction on processing rather than erasure;
- 13.10.3. 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;
- 13.10.4. Where there has been an objection made under para 13.2 above, pending the outcome of any decision.

Right to portability

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

14. Breach of any requirement of the UK GDPR

14.1. All breaches of the UK GDPR, including a breach of any of the data protection principles shall be reported as soon as it is / they are discovered, to the local Data Protection Lead (DPL) for the site. The DPL will then complete a Breach Report form providing as much information as possible and send this to DPO@OrmistonAcademies.co.uk. There must be no delay in completing this form and sending to OAT.

14.2. Once notified, the Data Protection Officer (DPO) shall assess:

- 14.2.1. The extent of the breach;
- 14.2.2. The risks to the data subjects as a consequence of the breach;
- 14.2.3. Any security measures in place that will protect the information;
- 14.2.4. Any measures that can be taken immediately to mitigate the risk to the individuals;
- 14.2.5. Any long-term changes required.

14.3. Unless the DPO 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.

14.4. The Information Commissioner shall be provided with a redacted copy of the breach report where required.

14.5. If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals then the DPL or other appropriately nominated person 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.

14.6. Data subjects shall be told:

- 14.6.1. The nature of the breach;

- 14.6.2. Who to contact with any questions;
- 14.6.3. Measures taken to mitigate any risks.

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

- 14.8. There are three actions which can be prosecuted as a criminal offence under the Data Protection Act.

- 14.9. Section 170: to knowingly or recklessly obtain, disclose or procure personal data without the consent of the data controller. This includes accessing personal data for which you have no business need to access, including that of a partner, friend or child.

- 14.10. Section 171: to knowingly or recklessly re-identify information that is de-identified personal data without the consent of the controller responsible for de-identifying the personal data. This means when data has been pseudonomised (for example replacing the name of the data subject with an unrelated code or key so they can no longer be identified) it is a criminal offence to put the two sets of information back together again so the data subject can be identified again without permission from the relevant data controller.

- 14.11. Section 173: to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure in the context of a data subject access request.

15. Data Protection Training

- 15.1. The Trust will ensure that all employees receive adequate training in respect of their data protection responsibilities for their roles and responsibilities. Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to data subject requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

- 15.2. All new employees must complete online data protection training as part of their induction training, and before they have access to any personal data.

- 15.3. All employees are required to complete online data protection training every year and further training at such other times that the Trust may reasonable require, for instance in relation to changes to data protection laws.

16. Contact

- 16.1. If anyone has any concerns or questions in relation to this policy, they should contact the Trust's Data Protection Officer via dpo@ormistonacademies.co.uk or;

Data Protection Officer
Ormiston Academies Trust (OAT)
One Victoria Square
Birmingham
West Midlands B1 1BD

Freedom of Information and Environmental Information Regulations

1. Introduction

- 1.1. The Trust is subject to the Freedom of Information Act 2000 (FOI) and the Environmental Information Regulations 2004 (EIR) as a public authority, and as such, must comply with any requests for information in accordance with the principles laid out in both.

2. What is a request under FOI?

- 2.1. Any request for any information from the Trust or any of its Academies is technically a request under the FOI, whether the individual making the request mentions the FOI. However, the ICO has stated that routine requests for information (such as a parent requesting a copy of a policy) can be dealt with outside of the provisions of the Act.
- 2.2. In all non-routine cases, if the request is simple and the information is to be released, then the individual who received the request can release the information but must ensure that this is done within the timescale set out below. A copy of the request and response should then be sent to the Data Protection and Complaints team.
- 2.3. All other requests should be sent in the first instance to the DPO inbox (dpo@ormistonacademies.co.uk) where it will be allocated to the Data Protection and Complaints team 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. (see 4.0 below).
- 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. What is a request under the EIR?

- 3.1. The Environmental Information Regulations 2004 provide public access to environmental information held by public authorities. The Regulations do this in two ways:
 - public authorities must make environmental information available proactively;
 - members of the public are entitled to request environmental information from public authorities.
- 3.2. While it is rare that the Trust would receive a request under EIR rather than FOI, it is possible. Environmental information is any information on:

- the state of the elements of the environment and the interaction among these elements;
- factors affecting or likely to affect those elements;
- measures or activities affecting or likely to affect those factors or elements, or designed to protect those elements;
- reports on the implementation of environmental legislation;
- cost–benefit and other economic analyses and assumptions used within the framework of those measures and activities; and
- the state of human health and safety, conditions of human life, cultural sites and built structures in as much as they are or may be affected by those elements.

3.3 In a school context the most likely areas for requests under EIR would be energy production or consumption and waste management, but there are other areas that may be covered, for example if bats were found to be inhabiting a building.

3.4 As with FOI requests, there are a series of reasons or ‘exceptions’ why it may not be appropriate to release environmental information. These are broadly comparable to the exemptions provided under the FOI Act but there are differences.

3.5. If you are ever unsure how to deal with a request, please contact the DPO for advice.

4. Time limit for compliance

4.1. Ormiston Academies 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.

5. Procedure for dealing with a request

5.1. 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 DPO inbox where it will be allocated to a member of the Data Protection and Complaints team. The request will be assessed and then may be forwarded to an individual with responsibility for the type of information requested.

5.2. The first stage in responding is to determine whether the Trust “holds” the information requested. This could either be centrally or at an individual school level. 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 in excess of 18 hours, the request will be refused under section 12 of the FOIA and the requester offered the opportunity to refine their request. For example, if a request required the Trust to add up totals in a spread sheet and release the total figures, this would be information “held” by the Trust. If the Trust would have to go through a number of spread sheets and identify individual figures and provide a total, this is likely not to be information “held” by the Trust, depending on the time involved in extracting the information.

- 5.3. 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:
- 5.3.1. 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;
 - 5.3.2. 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;
 - 5.3.3. Section 41 – information that has been sent to the Trust (but not the Trust’s own information) which is confidential;
 - 5.3.4. Section 21 – information that is already publicly available, even if payment of a fee is required to access that information;
 - 5.3.5. *Section 22* – information that the Trust intends to publish at a future date;
 - 5.3.6. *Section 43* – information that would prejudice the commercial interests of the Trust and / or a third party;
 - 5.3.7. *Section 31* – information which may prejudice the effective detection and prevention of crime – such as information about cyber security measures;
 - 5.3.8. Section 12 – provision of the information would exceed the cost limit (as per 5.2 above)
- 5.4. The sections mentioned previously 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. Section 43 also requires a prejudice test, to determine whose interests are prejudiced.

6. Responding to a request

- 6.1. When responding to a request where the Trust has withheld some or all the information, the Trust must usually 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. Very occasionally it may be possible to neither confirm nor deny whether information is held by the Trust. In this situation it would not be appropriate to explain the exemption that has been relied upon.
- 6.2. The letter should end by explaining to the requestor how they can complain – either by reference to an internal review by the Data Protection Officer, or by writing to the ICO.

7. Contact

- 7.1. Any questions about this policy should be directed in the first instance to the Data Protection and Complaints Manager. The Data Protection and Complaints Manager will ensure a suitable response to the enquirer on behalf of the Trust’s Data Protection and Complaints Team.
- 7.2. Email: dpo@ormistonacademies.co.uk or write to:

Ormiston Academies Trust (OAT)
One Victoria Square
Birmingham
West Midlands B1 1BD

8. Appendix 1

Old Section	New Section	Change
4	4	4.1 added specific 4.6 added 4.7-4.15 added
5	5	5.5.5 added 5.6 added 'this can be verbal or'
7	7	7.2.2 amended example of pseudonomised
8	8	8.1 added 'a DPIA will always be carried out if the processing includes special category data'
9	9	9.1.1 removed references
10	10	10.1 changed to 'meets a condition for processing under the substantial public interest article 9 lawful basis'
11	11	11.7 'but only where there is a need' added 11.9 changed to 'any complex' 11.10 'permanently' added
13	13	13.1.3 numbering added 13.1.4 restriction of processing added 13.4/13.11 regional co-ordinator changed to Data Protection and Complaints team 13.10.4 changed to 13.2
14	14	14.4 where required added 14.7 numbering added 14.8-14.11 added
Freedom of Information	Freedom of Information and Environmental Information Regulations	Title changed
1	1	1. 'and the Environmental Information Regulations 2004 (EIR)' added The act changed to 'both'
2	2	2.3 executive assistant changed to Data Protection and Complaints team
	3	added
3	4	Numbering changed

4	5	<p>5.1 Executive assistant changed to 'a member of the Data Protection and Complaints team The request will be assessed and then may be forwarded...' 5.2 Should the request.... Deleted. Section 12 explanation included Academy replaced with Trust Executive assistant replaced with Data Protection and Complaints team 5.3 academy replaced with Trust 5.3.7 section 38 example removed Section 31 example 'location of CCTV cameras' replaced with 'information about cyber security measures' 5.3.8 added 5.4 prejudice test added</p>
5	6	6.1 'usually' added. Also 'very occasionally.....' added
6	7	<p>7.1 executive assistant replaced with Data Protection and Complaints Manager 'and complaints' added 7.2 email address added and 'or write to'</p>