Ormiston Academies Trust

Ormiston Sudbury Academy
Special Category Data policy

Policy version control

Policy type	Statutory AND mandatory
Author	Alexandra Coughlan, OAT Data Protection and Complaints Manager
Approved by	Executive Team, May 2023
Release date	July 2023
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	New policy

Contents

1. Introduction

1.1. The Data Protection Act 2018 and the UK General Data Protection Regulation 2016 (UK GDPR) require a policy document to be in place where special category data or criminal offence data are being processed under certain grounds. The law puts in place extra protections for special category data and criminal convictions because of their sensitivity. This document explains how Ormiston Academies Trust meets these requirements when:

- Processing special category data on the grounds of substantial public interest; or
- Processing special category data for the purposes of carrying out the obligations and exercising specific rights under employment and social security and social protection law; or
- Where criminal offence data is being processed.

2. Scope

2.1. This policy applies to all employees of Ormiston Academies Trust including contract, agency and temporary staff, volunteers and employees of partner organisations working for the Trust. In this policy we refer to the "individual." By this we mean the data subject i.e. the identified or identifiable living individual to whom personal data relates.

3. What are special categories of data?

3.1. The categories of data within scope of this policy are personal data revealing an individual's:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data for the purpose of uniquely identifying a natural person
- data concerning health; or
- data concerning a natural person's sex life or sexual orientation.

4. Legal Basis for processing special category data

4.1. In order to process any personal data about an individual, we must firstly satisfy one of the lawful bases for processing personal data under Article 6 of the UK GDPR. In certain circumstances, Schedule 1 of the Data Protection Act must also be complied with. These lawful bases are:

a) Consent – the individual has given clear consent for their data to be processed for a specific purpose

b) Contract – the processing is necessary for a contract we have with the individual, or because the individual has asked us to take specific steps before entering into a contract

c) Legal obligation – the processing is necessary for us to comply with the law

d) Vital interests – the processing is necessary to protect someone's life

e) Public task – the processing is necessary for us to perform a task in the public interest, or for its official functions and the task or function has a clear basis in law

f) Legitimate interests – the processing is necessary for our legitimate interest or the legitimate interests of a third party, unless the interests of the individual override Ormiston Academies Trust's interests. However, this lawful basis does not apply to a public body, such as us, where we may rely on the public task ground instead.

4.2. In addition to the lawful basis to process personal data, special categories of personal data also require an additional lawful basis for processing under Article 9 of the UK GDPR. These lawful bases are as follows:

a) The individual has given explicit consent to the processing of those personal data for one or more specified purposes.

b) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights under employment, health and social security and social protection law and research; a full list can be found in Schedule 1 Part 1 of the Data Protection Act 2018. Health or social care purposes includes the following purposes:

- Preventative or occupational medicine
- The assessment of the working capacity of the employee

c) Processing is necessary to protect the vital interests of the individual or of another natural person where the individual is physically or legally incapable of giving consent.

d) Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the individuals concerned.

e) Processing relates to personal data which are manifestly made public by the individual

f) Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

g) Processing is necessary for reasons of substantial public interest but must be clearly demonstrated and assessed as part of the public interest test and evidenced throughout the decision making process. These grounds include the following (the full list of defined purposes may be found in Schedule 1 Part 2 of the Data Protection Act 2018):

- Statutory and government purposes

- Safeguarding of children or individuals at risk
- Legal claims
- Equality of opportunity or treatment
- Counselling
- Occupational pensions

h) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3.

i) Processing is necessary for reasons of public interest in the area of public health.

j) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

4.3. Deciding upon the correct lawful basis for processing data can be difficult and more than one may be applicable. We consult with the Data Protection Officer where appropriate. We must also comply with Schedule 1 of the Data Protection Act (as well as Articles 6 and Article 9), when we are processing data where the conditions relate to employment, health and research or substantial public interest as follows:

- Schedule 1, Part 1 of the Data Protection Act 2018 which provides that processing under points (b), (h), (i) or (j) of the UK GDPR above (conditions relating to employment, health and research).
- Schedule 1, Part 2 of the Data Protection Act 2018 in respect of point (g) above (substantial public interest)

4.4. The Schedules can be found in the Data Protection 2018 and further define the grounds thereby offering further protections. This policy satisfies the requirements of the Schedule. Our Privacy Notices, which may be found on our website, set out the types of special category data that we process.

5.Lawful basis for processing criminal offence data

5.1. Criminal offence data includes information about criminal allegations, criminal offences, criminal proceedings and criminal convictions. Whenever we process criminal offence data, Ormiston Academies Trust satisfies one of the lawful basis processing under Article 6 of the UK GDPR (as per paragraph 4 above), Article 10 of the UK GDPR and a condition under Schedule 1 of the Data Protection Act 2018. We do not maintain a register of criminal convictions. When processing this type of data, we are most likely to rely on one of the following bases:

- The processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the individual in connection with employment, social security or social protection or
- Consent –where freely given. We acknowledge because of the potential for the imbalance of power that it may be difficult for consent to be deemed valid, and will only rely on this where no other ground applies.

6. How Ormiston Academies Trust meets the principles of the UK GDPR

6.1. Article 5 of the UK GDPR sets out the data protection principles. Below follow our procedures for ensuring that we comply with the principles when we are processing special category or criminal data:

- Principle 1 – Personal data shall be processed lawfully, fairly and in a transparent manner.

    - We ensure that personal data will only be processed where a lawful basis applies and where processing is otherwise lawful;
    - We only process personal data fairly and ensure that individuals are not misled. We publish our privacy notice on our website and keep it up to date. Where there have been significant changes, we will do what is reasonable to advise individuals of the changes;
    - We ensure that wherever consent is sought from individuals to process their data, that it is freely given, specific, informed and unambiguous of the individual's wishes.
    - Where we are processing criminal offence data, as part of our employment duties, our policies are clear to applicants in terms of what we do with their data, how it is taken into account and whether it is retained.

- Principle 2 – Personal data shall be collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. We will not use personal data for purposes that are incompatible with the purposes for which it was collected. If we use personal data for a new purpose that is compatible with the original, we will ensure that there is a lawful basis upon which the data can be processed. In deciding whether a purpose is compatible, in accordance with the guidance from the Information Commissioner's Office, we will take into account the following:

    - Any link between the original and new purpose
    - The context in which the original data was collected
    - The nature of the personal data – how sensitive is it?
    - The possible consequences to the individual
    - Whether appropriate safeguards are used – for example encryption, pseudonymisation.

The following purposes are stated by the UK GDPR to be compatible: Archiving in the public interest, Scientific or historic research purposes, and Statistical purposes. In appropriate cases, including where consent formed the original basis for processing, we will seek the individual's explicit consent to use the data in a way that was not originally envisaged.

- Principle 3 – Personal data will be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

    - We will only collect the minimum personal data that we need for the purpose for which it is collected.

- Principle 4 – Personal data will be accurate and where necessary kept up to date.

    - We will take particular care to do all that is reasonable to ensure the accuracy of the information where it has a significant effect on individuals.
    - At appropriate intervals, we will remind individuals, parents/carers of the need to ensure that the data that they provide is accurate and up to date. When we are advised of changes, we will ensure that our records are updated as soon as is practicable.
    - We review requests to have data erased or rectified as soon as possible, and usually within 30 days. We rectify inaccurate data.

- Principle 5 – Personal data should be kept in a form which permits the identification of individuals for no longer than is necessary for the purposes for which the personal data is processed:

    - We only keep personal data, including special category data in an identifiable form for as long as is necessary for the purposes for which it was collected, or where there is a legal obligation to do so;
    - We review what data we hold at appropriate intervals – for example upon the annual review of the Record of Processing Activities or sooner if needed;
    - We have a retention and disposal policy which governs how long all data including special category data shall be retained for. This policy is complied with and reviewed regularly;
    - Once the data is no longer needed, we delete it, securely destroy it in line with our retention and disposal policy, or render it permanently anonymous.
    - We do not retain DBS certificates for longer than 6 months.

- Principle 6 – Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. Extra care is taken with special category and criminal offence data;

    - We adopt a risk-based approach to taking data offsite. Unless absolutely necessary, hard copies of sensitive personal data will not be removed from our premises. Any decision to remove the information must be based on the business need of Ormiston Academies Trust or in the best interests of the individual, rather than for the convenience of the individual member of staff. It is always preferable for any sensitive data to be accessed via an appropriately encrypted means

rather than via hard copy, when off-site. If there is no reasonable alternative to removing hard copies from Ormiston Academies Trust's site, the following procedure will apply:

- A record of what information has been removed will be logged on site with the office so that there is a record of what has been removed – for example health data in trip packs;
- Information will be transported and stored in a lockable case wherever possible;
- Wherever possible, information that is removed from site will be pseudonymised by using a "key" held by the office on site;
- We adopt a risk- based approach, for example hard copy personal data with lower sensitivity (e.g. exercise books) may be taken off site, but if left in a vehicle must be locked in the boot, never left in a visible place, only for the shortest period of time and never overnight. Special Category Data (e.g. SEND, Safeguarding, Health data) must be kept on the staff member's person at all times.
- Sensitive personal data must be returned to the academy's premises at the end of the working day, if not on a residential school trip. If this is not practicable, and a staff member needs to retain the information in their personal possession, this must be discussed in advance with a member of the Senior Leadership Team including what measures will be taken to safeguard the information, given the risks that are beyond a staff member's control in so doing and the potential consequences ensuing. The relevant member of the Senior Leadership Team must record their decision.

- Data will be tidied away when not in use (e.g. when staff undertake marking at home, it must be out of sight of family members, not left out and tidied away afterwards).
- Only those who have need to access the data concerned will be granted permission and access to it.
- Our data security policy / acceptable use / remote working policies describe our requirements around bring your own device, remote working and password protection.

- Principle 7 - Accountability In addition, to complying with the principles above, we are required to demonstrate how we evidence our compliance with them. The ways in which we do so include:

    - Data Protection Impact Assessments (DPIA) It is a statutory requirement that any processing of personal data which may result in a high risk to the data protection rights of the individual be assessed by means of a Data Protection Impact Assessment. Even though a DPIA may be required in other circumstances, examples of high-risk activities include:
        - Processing of special category data or criminal convictions on a large scale
        - Systematic monitoring of a publicly accessible area on a large scale
        - Automated decision making with legal or similar significant effect.

6.2. Prior to the assumption of any such activity, we will consult with the Data Protection Officer to assess risks based on an initial screening process. If required, a full DPIA will be undertaken to determine whether this activity should proceed. We keep DPIAs under review, and will revisit them in the event of significant changes. The DPIA will:

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

6.3. Those staff members handling data and in particular special category data will be trained in how to handle it, to an appropriate standard. This may include additional training on systems that handle sensitive personal data, which will be undertaken before the member of staff has full access to the system. Records will be maintained of the training undertaken.

6.4. Policies related to the handling of data and associated documentation will be regularly reviewed on a rolling basis and updated in accordance with new guidance, legislation and practice. They will be publicised to staff who will be required to familiarise themselves with them.

6.5. The Record of Processing Activities will be maintained and reviewed at least annually.

6.6. Where any breaches of personal data have occurred, the reasons for this will be reviewed and changes made to practice and procedure as appropriate; and

6.7. Stakeholders will manage risks and compliance using the annual compliance statement provided by the Data Protection Officer and/or a Risk Register.

7.Monitoring and Compliance

7.1. This policy will be reviewed annually, unless a change to legislation, practice or incident require a sooner review. Compliance with this policy shall be monitored through a review process. This will be agreed with the Data Protection Officer, and compliance will be reported to the executive team. Should it be found that this policy has not been complied with, or if an intentional breach of the policy has taken place, the organisation, in consultation with the executive team, shall have full authority to take the immediate steps considered necessary, including disciplinary action.