



DATA PROTECTION POLICY

READ ONLY

Responsible person: Oaks DPO

Approved by: Oaks Directors

Date approved: Summer 2018

Date for review: Summer 2020

Contents

1. Aims	3
2. Legislation and guidance	3
3. Definitions.....	3
4. The data controller	5
5. Roles and responsibilities	5
6. Data protection principles	6
7. Collecting personal data	6
8. Sharing personal data.....	8
9. Subject access requests and other rights of individuals	9
10. Parental requests to see educational records	11
11. Biometric recognition systems	12
12. CCTV	12
13. Photographs and videos	12
14. Data protection by design and default	13
15. Data security and storage of records	13
16. Disposal of records	14
17. Data breaches	14
18. Training	15
19. Monitoring arrangements	15
20. Links with other documents.....	15
Appendix A: Data Breach Procedure	16

1. AIM

Oaks Academy (The Trust) aim is to ensure all personal data collected about staff, children, parents, governors, visitors and other individuals is stored and processed in accordance with the General Data Protection Regulation (GDPR) and the provisions set out in the Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. LEGISLATION AND GUIDANCE

This policy meets the requirements of both the GDPR provisions and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and its code of practice for subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to the use of biometric data.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition The Trust, at its discretion, chooses to follow regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record and with The Trust's funding agreement and articles of association.

3. DEFINITIONS

Term	Definition
Consent	Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data set	A group of identified able data subjects, such as children, staff, parents, etc.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.

Data processor	A person or other body (other than an employee of the data controller), who processes personal data on behalf of the data controller.
Personal data	<p>Any information relating to an identified, or identifiable individual.</p> <p>This may include the individual's:</p> <ul style="list-style-type: none"> • Name (including initials) • Identification number • Location data • Online identifier, such as a username <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.</p>
Special categories of personal data	<p>Personal data which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none"> • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health - physical or mental • Sex life or sexual orientation
Processing	<p>Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.</p> <p>Processing can be automated or manual.</p>
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
Suppression List	A register recording the details of data subjects that do not consent to specific information being sent, emailed or copied to them.

4. THE DATA CONTROLLER

The Trust processes personal data relating to parents, children, staff, governors, visitors and others, and therefore is a data controller and is registered as a data controller with the ICO and renews this registration annually or as otherwise legally required.

5. ROLES AND RESPONSIBILITIES

This policy applies to all staff employed by The Trust and to external organisations or individuals working on its behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 The Trust Board. The board has overall responsibility for ensuring The Trust fully complies with all relevant data protection obligations.

5.2 Chief Executive Officer (CEO). The CEO acts as the representative of the Data Controller on a day-to-day basis.

5.3 Data Protection Officer (DPO). The DPO is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law and developing related policies and guidelines where applicable.

He/she will provide an annual report of their activities to the Audit and Risk Committee and, where relevant, report to the committee their advice and recommendations on data protection issues.

The DPO is also the point of contact for individuals whose data The Trust processes and for the ICO.

5.4 School Data Controllers (SDC). School Business Leaders are to be the SDCs for their schools. They are to be the first point of contact for staff and are responsible for:

- Contacting the DPO in the following circumstances:
 - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
 - If they have any concerns this policy is not being adhered to If they are unsure whether or not they have a lawful basis to use personal data in a particular way
 - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
 - If there has been a data breach
 - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
 - If they need help with any contracts or sharing personal data with third parties
- Ensuring the school's Suppression List is maintained and reviewed
- Maintaining an up-to-date a record of the school's data processors

- The provision of certificated secure document disposal for their school

5.5 All staff. Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting their SDC:
 - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
 - If they have any concerns that this policy is not being followed
 - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
- A data breach could potentially lead to a charge of gross misconduct and dismissal in accordance with Oaks Academy Disciplinary and Capability policy.

6. DATA PROTECTION PRINCIPLES

GDPR is based on the following data protection principles and states personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and is kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secured

This policy sets out how schools aim to comply with these principles.

7. COLLECTING PERSONAL DATA

7.1 Lawfulness, fairness and transparency. The Trust will only process personal data where there is a “lawful basis” (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone’s life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest**, and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual’s rights and freedoms are not overridden)

- The individual (or their parent/carer when appropriate in the case of a child) has freely given clear **consent**

The Trust will not often need to use consent, however, where it is sought the following is to apply:

- individuals are to have a positive opt-in, the use of pre-ticked boxes or any other method of default consent is not to be used;
- it is to be clear, concise, specific and ‘granular’ i.e. separate consent is obtained for each request, vague or blanket consent is not sufficient;
- requests for consent are to be separate from other terms and conditions;
- where consent is collected and used by a third party, the third party is to be named;
- explicit consent (used for special category data) requires a very clear and specific statement;
- individuals are to be told they can withdraw their consent at any time, how to withdraw their consent (the withdrawal process is to be clear and easy);
- schools are to keep evidence of consent i.e. who was asked, when were they asked, how they were asked (letter, software, etc.), what they were asked and what the rationale for their consent;
- consent is to be kept under review and refreshed if there are any changes;
- consent is not to be a precondition of a service;

Schools are to avoid over-reliance on consent, where it is required is to be freely given and care taken to ensure there is not an imbalance of power between the data subject and controller.

The Trust will meet one of the special category conditions for processing set out in the GDPR and DPA 2018:

- the data subject has given explicit consent;
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law
- processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- 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 data subjects;
- processing relates to personal data which are manifestly made public by the data subject;
- processing is necessary for the establishment, exercise or defence of legal claims;

- processing is necessary for reasons of substantial public interest;
- 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 law or pursuant to contract with a health professional;
- processing is necessary for reasons of public interest in the area of public health;
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Schools offering online services to children, such as classroom apps, and intend to rely on consent as a basis for processing, will need to obtain parental consent where the child is under the age of 13 (except for online counselling and preventive services).

7.2 Limitation, minimisation and accuracy. The Trust will only collect personal data for specified, explicit and legitimate reasons and will explain these reasons to individuals when the information is first gathered i.e. via a Privacy Notice.

Should The Trust want to use personal data for reasons other than those provided when the data was first obtained it must inform the individuals concerned before doing so and, where necessary, seek consent.

Staff must only process personal data where it is necessary in order carry out their job.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised and this should be undertaken in accordance with The Trust's Retention Schedule.

8. SHARING PERSONAL DATA

The Trust will not normally share personal data, but may do so where:

- There is an issue with a child or parent/carer that puts the safety of our staff at risk
- The Trust needs to liaise with other agencies - we will seek consent as necessary before doing this
- Suppliers or contractors need data to enable The Trust to provide services to staff and pupils - for example, IT companies. When doing this, The Trust will:
 - Only appoint suppliers or contractors that can provide sufficient guarantees they comply with data protection law
 - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of the shared personal data
 - Only share data and information that the supplier or contractor needs to carry out their service and to keep them safe while working with The Trust

The Trust will also share personal data with law enforcement and government bodies where are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided

Personal data may also be shared with emergency services and local authorities to help them to respond to an emergency situation that affects any of our children or staff.

Where personal data is transferred to a country or territory outside the European Economic Area, it will do so in accordance with data protection law.

9. SUBJECT ACCESS REQUESTS AND OTHER RIGHTS OF INDIVIDUALS

9.1 Subject access requests. Individuals have a right to make a ‘subject access request’ to gain access to personal information held about them. This includes:

- Confirmation their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be shared with
- How long the data will be stored for, or if this isn’t possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted using the appropriate request form, either by letter, email or fax to the school and the DPO informed.

School staff directly receiving a subject access request must immediately inform their SDC.

9.2 Children and subject access requests. Personal data about a child belongs to that child, and not the child’s parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children **below the age of 13** are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils may be granted without the express permission of the child. This is not a rule and a child's ability to understand their rights will always be judged on a case-by-case basis.

Children **aged 13 and older** are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of children may not be granted without the express permission of the child. This is not a rule and a child's ability to understand their rights will always be judged on a case-by-case basis.

Schools when seeking consent from a child, out of courtesy and to maintain good relations, should explain inform parents/carers about the reason for the request.

9.3 Responding to subject access requests. When responding to requests schools are to:

- Ask individuals to prove their identification
- Contact the individual via phone to confirm the request was made
- Respond without delay and within 1 month of receipt of the request
- Provide the information free of charge
- Inform and explain to individuals, where a request is complex or numerous, that the school requires an extension to the time limit and the information will be provided within 3 months from the original date of the request

The Trust will not disclose information if it:

- Might cause serious harm to the physical or mental health of the child or another individual
- Would reveal the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, The Trust may refuse to act on it, or charge a reasonable fee taking into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When refusing a request, The Trust will inform individuals why and they have the right to complain to the ICO.

9.4 Other data protection rights of the individual. In addition to the right to make a subject access request, and to receive information when collecting data, individuals also have the right to:

- At any time, withdraw their consent to processing
- Ask The Trust to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent the use of their personal data for direct marketing
- Challenge processing, which has been justified based on “public interest”
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit a request to exercise these rights, using the relevant request form, to their school, who will inform the DPO.

Staff receiving such requests should immediately inform their SDC.

10. PARENTAL REQUESTS TO SEE EDUCATIONAL RECORDS

As an academy, parents or those with parental responsibility, do not have a legal right to access to their child’s educational record (which includes most information about a child).

However, in the interest of transparency The Trust, at its discretion, chooses to follow regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child’s educational record.

Schools are to provide the information, free of charge, within 15 school days of receipt of a written request.

11. BIOMETRIC RECOGNITION SYSTEMS

(Note that in the context of the Protection of Freedoms Act 2012, a “child” means a person under the age of 18.)

Schools using pupil’s biometric data as part of an automated biometric recognition system, for the payment of food, library and door access systems for example, are to comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. Schools are to obtain written consent from at least one parent or carer before collecting any biometric data from their child and the processing of it.

Parents/carers and children have the right to choose not to use the biometric system(s). If this is the case schools are to provide alternative means of accessing the relevant services for those individuals, for example, the provision of swipe cards.

Parents/carers and children, at any time, can withdraw from participating in the biometric recognition system(s), by withdrawing their consent. If consent is withdrawn schools are to ensure any relevant data already captured is deleted.

As required by law, if a child refuses to participate in, or continue to participate in the processing of their biometric data, schools will not process that data irrespective of any consent given by the child's parent(s)/carer(s).

Where staff or other adults use biometric system(s), schools will also obtain their consent before they participate in it and provide alternative means of accessing the relevant service if they object. If consent is withdrawn schools are to ensure any relevant data already captured is deleted.

12. CCTV

The Trust use CCTV at various school sites for safety and adheres to the ICO's code of practice for the use of CCTV.

The Trust does not need to ask individuals' permission to use CCTV, but it is made clear at the relevant school sites that individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining CCTV is in use.

Enquiries about the CCTV systems should be directed to school SDC.

13. PHOTOGRAPHS AND VIDEOS

As part of The Trust's activities, schools may take photographs and record images of individuals.

Schools are to obtain written consent from parents/carers (and from children aged 12 and under) for photographs and videos to be taken of their child for communication, marketing and promotional materials.

Where schools need consent, they will clearly explain how the photograph and/or video will be used to both the parent/carer and child. Where parental consent is not needed, schools will clearly explain to the child how the photograph and/or video will be used. Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers campaigns and The Trust's media company
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, schools are to delete the photograph or video and not distribute it further.

When using photographs and videos in this way schools will not include any other personal information about the child, to ensure they cannot be identified.

Further information about the taking and use of images can be found in the following policies:

- Child Protection and Safeguarding
- ICT Acceptable Usage
- E-Safety
- Social Media
- Staff Code of Conduct

14. DATA PROTECTION BY DESIGN AND DEFAULT

The Trust has measures in place to demonstrate that data protection has been integrated into data processing activities, including:

- The appointment of a suitably qualified DPO, and ensuring he/she has the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law
- Completing privacy impact assessments where the processing of personal data presents a high risk to the rights and freedoms of individuals and when introducing new technologies
- Integrating data protection into internal documents and related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies, any other data protection matters and record attendance to training
- Regularly conducting reviews and audits to test privacy measures and check compliance
- Maintaining records of our processing activities, including:
 - For the benefit of data subjects, making available the name and contact details of the DPO
 - The use of Privacy Notices to inform all data sets about the information held, how it is used and if it is shared, with whom
 - Maintaining an internal record of the type of data The Trust collects, how it uses it, the relevance of the data to the data sets, where the data is stored and the retention period for the data

15. DATA SECURITY AND STORAGE OF RECORDS

The Trust will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure and against accidental or unlawful loss, destruction or damage. In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept secured when not in use
- Papers containing confidential personal data are not left on office and classroom desks, on staffroom tables, pinned to notice/display boards or left anywhere else where there is general access, or it is included in the risk assessment.
- Where personal information needs to be taken off-site, staff must sign it in and out from the school office
- Passwords are to comply with the Trust's Information Security
- Portable devices such as USB sticks or external hard drives are not permitted regardless of encryption, as these pose additional risks to the security of the network.
- Staff, children or governors are not allowed to store personal information on their personal devices and are expected to follow the same security procedures as for school-owned equipment (see the ICT Acceptable Usage and E-Safety policies)
- Where personal data is shared with a third party, The Trust undertakes due diligence and reasonable steps to ensure it is stored securely and is adequately protected

16. DISPOSAL OF RECORDS

Personal data that is no longer needed, is inaccurate or out of date and cannot or does not need to be rectified is to be disposed of securely.

Schools are to shred or incinerate paper-based records and overwrite or delete electronic files. When using third party organisations to safely dispose of records, schools are to obtain sufficient guarantees from their supplier to satisfy themselves that they are complying with data protection law.

Before disposing of documents schools are to check the Retention Schedule to confirm retention dates.

17. DATA BREACHES

Schools are to make all reasonable endeavours to ensure personal data is protected and there are no data breaches.

In the unlikely event of a data breach or a suspected data breach, schools are to follow the procedure set out in annex A.

When appropriate, the DPO will report the data breach to the ICO within 72 hours. Such breaches, in a school context, may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of children eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school device containing non-encrypted personal data

18. TRAINING

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

Where changes to legislation, guidance or the school's processes make it necessary data protection will form part of continuing professional development.

19. MONITORING ARRANGEMENTS

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated when there are changes to DPA 2018, guidance provided by case law or changes which will affect The Trust's practice.

20. LINKS WITH OTHER DOCUMENTS

This policy links with:

- Article 13 Notices (Privacy Notices for each data set)
- Article 14 Notices (Privacy Notice informing data subjects that data, concerning them, has been received from a third party)
- Data Breach Register
- Data Sets and Data Register
- Data Protection Impact Assessment Form
- Freedom of Information Policy
- Retention Schedule
- Subject Request Forms
- Data Processor Register - Template for schools
- Suppression List - Template for schools
- Information Security Policy

DATA BREACH PROCEDURE

This procedure is based on “guidance on personal data breaches” produced by the ICO.

1. On finding a breach or potential breach, the school or data processor must immediately notify the DPO.
 2. The DPO will undertake an initial investigate to determine whether a breach has occurred. He / She will consider whether personal data has been accidentally or unlawfully:
 - Altered
 - Destroyed
 - Lost
 - Published or made available to an inappropriate audience
 - Stolen
 - Made available to unauthorised people
 3. The DPO is to brief the CEO.
 4. The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.
 5. The DPO will decide if the breach must be reported to the ICO. This will be judged on a case-by-case basis. The DPO is to take into consideration whether the breach is likely to negatively affect people’s rights and freedoms, cause them any physical, material or non-material damage (e.g. emotional distress) through:
 - Damage to reputation
 - Discrimination
 - Financial loss
 - Identify theft or fraud
 - Loss of confidentiality
 - Loss of control over their data
 - Unauthorised reversal of pseudonymisation (for example, key-coding)
 - Any other significant economic or social disadvantage to the individual(s) concerned
- If it is likely that there will be a risk to people’s rights and freedoms, the DPO must notify the ICO.
6. The DPO will document the decision (either way), in case it is challenged later by the ICO or an individual affected by the breach. Documented decisions are stored in a spreadsheet on The Trust’s computer network.

7. Where the ICO must be notified, the DPO will complete the 'report a breach' page on the ICO's website within 72 hours. As required, the DPO will set out:
 - a. A description of the nature of the personal data breach including, where possible:
 - The categories and approximate number of individuals concerned
 - The categories and approximate number of personal data records concerned
 - b. The name and contact details of the DPO.
 - c. A description of the likely consequences of the personal data breach.
 - d. A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

If all the above details are not yet known, the DPO will report as much as he/she can within the 72 hours timeframe. The report will explain there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

8. The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
 - a. The name and contact details of the DPO
 - b. A description of the likely consequences of the personal data breach
 - c. A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
9. The DPO will notify any relevant third parties who can help mitigate the loss to individuals - for example, the police, insurers, banks or credit card companies.
10. The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
 - a. Facts and cause
 - b. Effects
 - c. Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
 - d. Records of all breaches will be stored spreadsheet on The Trust's computer network
11. The DPO and CEO will meet to review the breach and lessons learnt. This meeting will happen as soon as reasonably practicable.