Oakwood Community School
Data Protection Policy

Ratified by the board: _____

Due for renewal: September 2022

Contents

---

1. Aims

Oakwood Community School aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and 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 the GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

TERM	DEFINITION
Personal Data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data, which is more sensitive and so needs more protection, including information about an individual's: • 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	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data Subject	The identified or identifiable individual whose personal data is held or processed.
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.

TERM	DEFINITION
Personal Data Breach	breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The Data controller

The School processes personal data relating to parents, pupils, staff, proprietors, volunteers, visitors and others, and therefore is a data controller.

5. Roles and responsibilities

This policy applies to all staff employed by the School, its parent company and to external organisations, volunteers and other individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Proprietary Board

The Proprietary Board has overall responsibility for ensuring that the School complies with all relevant data protection obligations.

5.2 Data Protection Officer

As an independent school, we are not legally required to appoint a data protection officer (DPO). This is because we are not part of a public body. The first point of contact for individuals whose data the school processes should be the Head Teacher.

5.3 All staff

All members of 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 the Head Teacher 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 that this policy is not being followed
- If they are unsure whether 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 UK
- 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.

6. Data Protection principles

The UK GDPR is based on data protection principles that our School must comply with. Oakwood Community School has adopted the principles to underpin its Data Protection Policy: The principles require that all personal data shall be:

(1) processed lawfully, fairly and in a transparent manner;

(2) collected for specified, explicit and legitimate purposes;

(3) adequate, relevant and limited to what is necessary;

(4) accurate and, where necessary, kept up to date;

(5) kept no longer than is necessary for the purposes for which it is processed;

(6) processed in a way that ensures it is appropriately secure;

This policy sets out how the School aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

Oakwood Community School shall only process personal data where it has one of 6 'lawful bases' (legal reasons) available to the School to do so under data protection law:

1. 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

2. The data needs to be processed so that the school can comply with a legal obligation

3. The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life

4. The data needs to be processed so that the school can perform a task in the public interest, and carry out its official functions

5. 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

6. The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given explicit consent
- The data needs to be processed to perform or exercise obligations or rights in relation to employment, social security or social protection law
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual
- The data needs to be processed for the establishment, exercise or defence of legal claims
- The data needs to be processed for reasons of substantial public interest as defined in legislation

- The data needs to be processed for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with guidance set out in the Information and Records Management Society's toolkit for schools.

We will keep data accurate and, where necessary, up to date.

8. Sharing personal data

We will not normally share personal data with anyone else except as set out in the School's Privacy Notice. GDPR and the DPA 2018 also allow information to be shared where:

• There is an issue with a pupil or parent/carer that puts the safety of our staff at risk

• We need to liaise with other agencies – we will seek consent as necessary before doing this

• Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with UK 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 any personal data we share.
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we 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 our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the UK, we 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 that the school holds about them. This includes:

- Confirmation that 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
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO
- 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 may be submitting in writing or verbally and can be sent either to the Head teacher or a member of staff. To enable the request to be accurately responded to, the applicant should be encouraged to make the request in writing and to set out:

- Name of individual
- Name of School
- Correspondence address
- Contact number and email address
- Details of the information requested.

If staff receive a subject access request, they must immediately forward it to the Headteacher, who will ensure that the Proprietary Board/HR Manager is informed.

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 person should have parental responsibility for the child, and 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, subject access requests from those with parental responsibility for pupils at our school will in general be granted without requiring the express permission of the pupil.

These are not fixed rules and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous, or where it is impractical to comply within a month due to school closure. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts
- Is contained in adoption or parental order records

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes 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 we refuse a request, we will tell the individual why, and tell them 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 (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time, where processing is based on the consent of the pupil or parent

- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Challenge decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- 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 any request to exercise these rights to the Headteacher. If staff receive such a request, they must immediately forward it to the Headteacher.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

11. CCTV

We use CCTV in some external locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use. Any enquiries about the CCTV system should be directed to the Headteacher.

12. Photographs and videos

As part of our school activities, the school may take photographs and record images of individuals within the school. The school will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Uses may include:

• Within school on notice boards and in school newsletters, brochures etc.

• Outside of school by external agencies such as the school photographer, newspapers, campaigns

• Online on our school website or social media pages.

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

See our Safeguarding policy and our Acceptable Use Policy for more information on our use of photographs and videos.

13. Data protection by design and default

The School shall put measures in place to show that it has integrated data protection into all of its data processing activities, including:

• 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 (see section 6)

• Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies

• Integrating data protection into internal documents including this policy, any related policies and privacy notices

• Training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance

• Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant

- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply

• Maintaining records of our processing activities, including:

- For the benefit of data subjects, making available the name and contact details of our school and all information we are required to share about how we use and process their personal data (via our privacy notices)
- For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

14. Data security and storage of records

The School 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 under lock and key when not in use

• Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access

• Staff must ensure passwords are hard for anyone else to guess by incorporating numbers and mixed case into it.

• Encryption software is used to protect all portable devices and removable media on which personal information is stored, such as laptops and USB devices

• Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

15. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. For example, the School will shred or incinerate paper-based records and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

16. Personal data breaches

The School shall take all reasonable steps to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1.

When appropriate, the School shall 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 pupils eligible for the pupil premium

• Safeguarding information being made available to an unauthorised person

• The theft of a school laptop containing non-encrypted personal data about pupils

17. Training

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

18. Links with other policies

This data protection policy is linked to our:

- Information Security
- Safeguarding Policy
- Acceptable Use Policy

Appendix 1:

Personal data breach procedures

If staff become aware that information has not been handled according to procedures and there is a data breach or potential security incident, they must report it in accordance with this procedure.

When appropriate, the School will report the data breach to the ICO within 72 hours in accordance with the requirements of the GDPR.

1. Data protection breaches occur where personal data is lost, damaged, destroyed, stolen, misused and/or accessed unlawfully.

2. Examples of how a breach may occur include:

a. Theft of data or equipment on which data is stored;
b. Loss of data or equipment on which data is stored;
c. Inappropriate access controls allowing unauthorised use;
d. Accidental Loss;
e. Destruction of personal data;
f. Damage to personal data;
g. Equipment failure;
h. Unlawful disclosure of personal data to a third party;
i. Human error;
j. Unforeseen circumstances such as fire or flood;
k. Hacking attack; or
l. 'Blagging' offences where information is obtained by deceiving the organisation which holds it.

3. If any member of staff of the School, or member of the Proprietary Board, discovers that data has been lost, or believes that there has been a breach of the data protection principles in the way that data is handled, you must immediately or no later than within 24 hours of first coming to notice, inform the Headteacher.

4. Upon being notified, the Headteacher will assess whether a breach of personal information has occurred, and the level of severity. If a breach has occurred but the risk of harm to any individual is low (for example, because no personal information has left the control of the School), then the Headteacher will undertake an internal investigation to consider whether the Information Security Policy was followed, and whether any alterations need to be made to internal procedures as a result.

5. In all other cases, the incident must be notified to the Proprietary Board Chair immediately, who must follow the Information Commissioner's Office guidelines on notification and recording of the breach. The priority must then be to close or contain the breach to mitigate / minimise the risks to those individuals affected by it. All School staff and Proprietary Board members are expected to work in partnership with the Headteacher and/or HR Manager in relation to the following matters

Notification of Breaches

Any member of staff or Proprietary Board member who becomes aware of a personal information breach should provide full details to the Headteacher for the School within 24 hours of being made aware of the breach. The Headteacher will then complete the Data Breach Record Form and Incident Log.

When completing the form details should be provided of the reporter's name, the date/time of the breach, the date/time of detecting the breach, and basic information about the type of breach and information about personal data concerned. Details of what has already been done to respond to the risks posed by the breach should also be included.

Containment and Recovery

The initial response is to investigate and contain the situation and a recovery plan including, damage limitation. There may be input from specialists such as IT, HR and legal and in some cases contact with external third parties.

• Seek assistance in the containment exercise. This could be isolating or closing a compromised section of the network, recovery of released documents, finding a lost piece of equipment or simply changing any related access codes

• Establish whether there is anything that can be done to recover any losses and limit the damage the breach can cause.

• As well as the physical recovery of equipment, this could involve the use of backup records to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts.

• Consider whether any individual affected by the data breach should be notified

Assessing the Risks

Levels of risk can be very different and vary on an individual breach of data security depending what is lost/damaged/stolen. For example, if a case file is lost then risks are different depending on type of data and its sensitivity with potential adverse consequences for individuals. The Headteacher should consider the following points:

• What type of data is involved?

• How sensitive is the data?

• If data has been lost or stolen, are there any protections in place such as encryption?

• What has happened to the data?

• If data has been stolen, could it be used for purposes which are harmful to the individuals to whom the data relate? If it has been damaged, this poses a different type and level of risk.

• Regardless of what has happened to the data, what could the data tell a third party about the individual? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people

• How many individuals' personal data has been affected by the breach?

• Who are the individuals whose data has been breached?

• What harm can come to those individuals?

• Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?

• Are there wider consequences to consider such as a risk to life?

• Loss of public confidence in the School? All staff and Proprietary Board members should establish whether there is anything they can do to recover any losses and limit the damage the breach can cause.

Appendix 2: Personal data breach Incident Report Form

This form should be used to provide information to the Headteacher when there has been a serious breach and consideration needs to be given to whether the breach should be reported to the ICO.

The aim of the form is to gather detailed information in order to understand the gravity of the breach, including its impact and what must be done to reduce the risk to personal data and the individuals concerned.

It is imperative that as much information as possible is provided. The information will be used to review policies and procedures and assess whether changes are required.

Breach log no: _____ Breach log reference: _____

1. Details of the breach

a) Date and Time of the Incident

b) Number and description of individuals whose data is affected

c) Nature of the breach

d) Description of how breach occurred

2. Reporting

a) When was the breach reported to you?

b) How did you become aware of the breach?

3. Personal Data

a) Full description of personal data involved (without identifying individuals)

b) Have all of the affected individuals been informed of the breach?

c) If not, why?

d) Has the personal data in this incident been inappropriately processed or further disclosed?

4. Consequence of the breach?

a) Describe the risk of harm to individuals as a result of this breach?

b) Is there a risk of identity fraud as a result of this breach?

c) Has a formal complaint been received from any of the individuals affected by the breach? If yes, please provide details?

5. Measures taken or to be taken?

a) What immediate action was taken?

b) Has the data been retrieved? – If yes, please specify the date and time. Has any further action been taken to minimise the possibility of a repeat of such an incident?

c) Has there been a breach of policies and procedures?

Completed by:

Name: _____

Job title:_____

Signature:_____

Date:_____