



Orange Tree School

Data Protection Policy

2026-2027

Orange Tree School (Main Site) and Ridgeway Hospital Provision



DOCUMENT DETAILS	
Applies To:	• All Staff • External suppliers or visitors • Regulatory / Legal bodies/LEAs • Other (e.g. Parents) • Hospital Staff
Policy Author:	Helen Carmel/Zoe Ramshaw
Approval Body:	Advisory Board – Peter Curtis
Frequency of review:	Annually
Last Update:	02/08/2026
Next Review Date:	02/08/2027

Policy Summary

Purpose

Orange Tree School is committed to protecting the privacy, dignity and personal information of pupils, staff, parents, carers and others whose data it processes.

This policy explains how the school collects, uses, stores, shares, retains and disposes of personal data in accordance with UK data protection law. It also sets out responsibilities for data security, subject access requests, photographs and recordings, CCTV, artificial intelligence and personal data breaches.

The policy applies to personal data held in both electronic and paper formats across the Main Site and Ridgeway Hospital Provision.

Core Principles

Orange Tree School will ensure that personal data is:

- processed lawfully, fairly and transparently;
- collected for clear and legitimate purposes;
- adequate, relevant and limited to what is necessary;
- accurate and kept up to date where required;
- retained only for as long as necessary;
- stored and processed securely; and
- handled in a way that respects the rights of individuals.

The school recognises that data protection supports safeguarding, professional trust, effective education and the safe operation of the school.

Key Expectations

- Staff must only access and use personal data where this is necessary for their role.
- Confidential information must be stored, discussed and shared securely.
- Personal data must not be shared without an appropriate lawful basis.
- Staff must follow the school's privacy notices, retention arrangements and information-sharing procedures.
- Subject access requests and other requests relating to individual rights must be forwarded promptly to the Data Protection Officer.
- Any actual or suspected personal data breach must be reported immediately to Helen Carmel, Business Manager, with Craig Hunter, IT Support Officer, involved where technical support is required.
- The Data Protection Officer, Aanika Patel, will provide independent advice and determine whether further action, including notification to the Information Commissioner's Office, is required.
- Personal or sensitive information must not be entered into unauthorised artificial intelligence tools or online platforms.

Related Policies and Documents

- Cyber Security Policy
- Online Safety Policy
- Safeguarding and Child Protection Policy
- CCTV Policy
- Mobile Phone and Personal Devices Policy
- Staff Code of Conduct
- Acceptable Use Agreement
- Records Retention Schedule
- Privacy Notices
- Personal Data Breach Procedure

Legislation and Guidance

This policy has been developed with regard to:

- UK General Data Protection Regulation;
- Data Protection Act 2018;
- Education (Independent School Standards) Regulations 2014;
- relevant Information Commissioner's Office guidance;
- Department for Education guidance on data protection in schools;
- Keeping Children Safe in Education, current edition;
- guidance relating to surveillance cameras, artificial intelligence and information security.

Contents

Policy Summary.....	3
1. Introduction.....	6
2. Legal and Regulatory Framework.....	6
3. Definitions.....	7
4. The data controller.....	8
5. Roles and Responsibilities.....	8
6. Data protection principles.....	10
7. Collecting personal data.....	10
8. Sharing personal data.....	12
9. <i>Subject access requests and other rights of individuals</i>	13
10. Parental requests to see the educational record.....	16
11. CCTV.....	16
12. Photographs and videos.....	17
13. Artificial intelligence (AI).....	17
14. Data protection by design and default.....	18
15. Data security and storage of records.....	19
16. Disposal of records.....	20
17. Personal data breaches.....	20
18. Training.....	21
19. Monitoring arrangements.....	21
20. Links with Other Policies.....	22
Appendix A – Personal Data Breach Procedure.....	23

1. Introduction

Orange Tree School is committed to protecting the personal information of pupils, families, staff, volunteers, contractors and all others whose data the school processes. Respecting privacy and handling information securely are fundamental to maintaining trust, safeguarding pupils and ensuring the effective operation of the school.

As a specialist independent school for pupils with Education, Health and Care Plans (EHCPs), Orange Tree School routinely processes sensitive personal information to support education, safeguarding, health, wellbeing and regulatory responsibilities. The school recognises that much of this information is highly confidential and must be handled lawfully, fairly and securely at all times.

The school is committed to complying with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and other relevant legislation and guidance. Effective data protection is recognised as a shared responsibility, and all members of the school community are expected to understand and fulfil their responsibilities when handling personal information.

This policy applies to all personal data processed by Orange Tree School, whether held electronically, on paper or in any other format. It should be read alongside the School's Cyber Security Policy, Online Safety Policy, Safeguarding and Child Protection Policy and other related information governance policies.

2. Legal and Regulatory Framework

This policy has been developed with regard to:

- UK General Data Protection Regulation (UK GDPR);
- Data Protection Act 2018;
- Education (Independent School Standards) Regulations 2014;
- Education (Pupil Information) (England) Regulations 2005;
- Keeping Children Safe in Education (current edition);
- Information Commissioner's Office (ICO) guidance;
- Department for Education guidance on data protection in schools;
- Department for Education guidance on the use of Artificial Intelligence in education;
- ICO guidance on surveillance cameras and CCTV.

Orange Tree School recognises that effective data protection supports safeguarding, protects the rights and freedoms of individuals, promotes public confidence and contributes to the safe and effective operation of the school.

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR)

- Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO), Department for Education (DfE) guidance on generative artificial intelligence in education, and ICO guidance on the use of surveillance cameras.

It also complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005.

3. Definitions

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, living 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: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • 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.

TERM	DEFINITION
Data controller	A person or organisation that determines the purposes and the means of processing 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 breach	A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. The data controller

Our school processes personal data relating to parents and carers, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school is registered with the ICO as legally required.

5. Roles and Responsibilities

Advisory Board

The Advisory Board is responsible for:

- ensuring the school complies with its data protection obligations;
- receiving assurance that appropriate data protection arrangements are in place;
- monitoring significant data protection risks where appropriate;
- supporting a culture of good information governance across the school.

Headteacher

The Headteacher is responsible for:

- ensuring appropriate arrangements are in place to comply with data protection legislation;
- promoting a culture of confidentiality, accountability and good information governance;
- supporting the implementation of this policy across the school;
- ensuring appropriate resources are available to maintain effective data protection arrangements.

Business Manager (Helen Carmel)

The Business Manager has day-to-day operational responsibility for data protection within the main school. The lead teacher has oversight of this at Ridgeway.

Responsibilities include:

- overseeing the implementation of this policy;
- coordinating the school's response to suspected personal data breaches;
- supporting staff with operational data protection queries;
- liaising with the Data Protection Officer where specialist advice is required;
- working with the IT Support Officer to ensure appropriate technical and organisational security measures are maintained;
- ensuring data protection issues are appropriately recorded, monitored and reviewed.

Data Protection Officer (Aanika Patel)

The Data Protection Officer provides independent advice and oversight on behalf of the wider Ellern Mede organisation.

The DPO is responsible for:

- monitoring compliance with UK GDPR and the Data Protection Act 2018;
- advising the School on data protection legislation and best practice;
- supporting the management of subject access requests;
- advising on Data Protection Impact Assessments where required;
- determining whether personal data breaches require notification to the Information Commissioner's Office (ICO);
- acting as the School's principal point of contact with the ICO;
- providing independent advice to the Headteacher and Business Manager.

The Data Protection Officer can be contacted via:

data.protection@ellernmede.org

IT Support Officer (Craig Hunter)

The IT Support Officer supports the school's technical data security arrangements.

Responsibilities include:

- maintaining secure access to school systems;
- managing user accounts and permissions;
- supporting secure storage of electronic information;
- assisting with technical investigations following suspected personal data breaches;
- implementing security measures under the direction of the Business Manager.

All Staff

All staff are responsible for protecting personal information and complying with this policy.

Staff must:

- access personal information only where necessary for their role;
- keep information secure and confidential;
- follow the school's retention and information-sharing procedures;
- report suspected personal data breaches immediately to Helen Carmel, copying Craig Hunter where technical support is required;
- cooperate with any investigation relating to a personal data breach;
- complete mandatory data protection training.

6. Data protection principles

Orange Tree School will ensure that all personal data is processed in accordance with the principles set out within the UK General Data Protection Regulation (UK GDPR). These principles underpin all aspects of the school's information governance arrangements and apply to every member of the school community who handles personal information.

Personal data will be:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, kept up to date;
- retained only for as long as necessary;
- processed securely to protect against unauthorised or unlawful access, loss, destruction or damage.

7. Collecting personal data

Orange Tree School processes personal information to fulfil its educational, safeguarding, employment and legal responsibilities. Personal data is collected and processed only where there is a lawful basis to do so and only where it is necessary for the School to carry out its functions.

Special Category Data

As a specialist SEND school, Orange Tree School routinely processes special category personal data relating to pupils' health, special educational needs, safeguarding, therapeutic support and wellbeing. Such information will only be processed where there is a lawful basis and an additional condition for processing under UK GDPR and the Data Protection Act 2018.

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have 1 of 6 'lawful bases' (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 or another person i.e. 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 or exercise its official authority
- The data needs to be processed for the legitimate interests of the school (where the processing is not for any tasks the school performs as a public authority) 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 pupil) has freely given clear consent

For special categories of personal data, we will also meet 1 of the special category conditions for processing 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

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given consent
- 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 or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights
- The data needs to be processed for reasons of substantial public interest as defined in legislation

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

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect or use personal data in ways which have unjustified adverse effects on them.

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.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, 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 the school's record retention schedule.

8. Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations 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 that can provide sufficient guarantees that they comply with UK data protection law
- Establish a contract with the supplier or contractor 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

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

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 internationally, we will do so in accordance with UK data protection law.

The School will only share personal information where there is a lawful basis to do so, taking account of safeguarding responsibilities, statutory duties and the rights of individuals. Where appropriate, information sharing agreements or data processing agreements will be established to ensure personal information is protected.

9. Subject access requests and other rights of individuals

Orange Tree School recognises that individuals have important rights in relation to their personal information under UK data protection legislation. The school is committed to responding to requests promptly, fairly and in accordance with statutory requirements.

Staff Guidance

If any member of staff receives:

- a Subject Access Request;
- a request to amend personal information;
- a request to erase information;
- a request to restrict processing;
- a request relating to data protection rights;

Staff must not attempt to respond themselves. The request should be forwarded immediately to Zoe Ramshaw (Headteacher) and Helen Carmel (Business Manager), who will coordinate the school's response in consultation with Aanika Patel (Data Protection Officer).

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 or another supervisory authority
- 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
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

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

If staff receive a subject access request in any form, they must immediately forward it to the DPO.

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 aged 12 and above 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 pupils at our school may not be granted without the express permission of the pupil. This is not a rule 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. We will inform the individual of this within 1 month, and explain why the extension is necessary

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or 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

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

The school will maintain appropriate records of requests received, and responses provided to demonstrate compliance with UK GDPR.

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
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing that has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- 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 DPO. If staff receive such a request, they must immediately forward it to the DPO.

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. As an independent school, there is no automatic parental right of access to your child's educational record, however, we will provide this information upon request.

The school will aim to do this within 15 days except during school shut down periods (school holidays), there may also be an extension to the 15 days if the records cover a long span of time. The school may charge a fee to cover the costs. This is costed depending on the size of the documentation requested.

This right applies as long as the pupil concerned is aged under 18.

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. This could also include any safeguarding records.

Requests should be submitted in writing to the school via reception@orangetreeschool.org. The school will acknowledge receipt and advise parents of the next steps, any applicable costs and expected timescales.

11. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will follow the [ICO's guidance](#) for the use of CCTV and comply with data protection principles.

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.

CCTV images will be retained securely for a period determined by the school's retention schedule unless required for the investigation of an incident or to meet a legal obligation.

The school operates CCTV in accordance with its separate CCTV Policy. Any enquiries regarding the operation of the School's CCTV system should be directed to Helen Carmel, Business Manager.

12. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and the pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

Where the school takes photographs and videos, 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
- 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.

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

The school recognises that many pupils have individual safeguarding considerations or parental preferences regarding photography. Staff are responsible for checking current consent records before taking or publishing photographs or videos of pupils and must follow the School's safeguarding and data protection procedures at all times.

13. Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. Orange Tree School recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, Orange Tree School will treat this as a data breach, and will follow the personal data breach procedure outlined in appendix A.

Where AI tools are approved for educational or administrative purposes, staff must use them responsibly and professionally, ensuring that confidential, safeguarding or personal information is not entered into publicly available AI platforms unless authorised by the school.

14. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have 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 (see section 6)
- Completing data protection 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 (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly 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:
 - o For the benefit of data subjects, making available the name and contact details of our school and DPO, and all information we are required to share about how we use and process their personal data (via our privacy notices)
 - o For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure

Where personal data is transferred outside the UK, the school will ensure appropriate safeguards are in place, including UK adequacy regulations or approved contractual safeguards.

Orange Tree School will ensure that data protection considerations are incorporated into the planning of new systems, projects, technologies and ways of working. Where appropriate, advice will be sought from the Data Protection Officer before implementation.

15. Data security and storage of records

We 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
- Confidential documents should not be left unattended in classrooms, meeting rooms, shared offices or other areas where they could be accessed by unauthorised individuals.
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office

Wherever possible, staff should access information remotely through secure school systems rather than transporting paper records.

- Staff must take reasonable steps to ensure that personal information is not left unattended in vehicles, public places or unsecured locations and should only remove information from the school where this is necessary for their role.
- Passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our ICT and internet acceptable use policy)
- Safeguarding records are stored separately from the main pupil file and subject to enhanced access controls.
- 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

Electronic information will be protected through the technical and organisational measures described within the School's Cyber Security Policy.

16. Disposal of records

The school maintains a formal data retention schedule informed by statutory requirements and sector guidance (including ISBA and IRMS). Staff must comply with the retention schedule at all times.

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, we 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.

The School's Records Retention Schedule will be reviewed periodically to ensure continued compliance with statutory requirements and best practice.

17. Personal data breaches

Orange Tree School recognises that, despite appropriate safeguards, personal data breaches may occasionally occur. All actual or suspected personal data breaches will be treated seriously and managed promptly in accordance with this policy and Appendix A.

Any member of staff who becomes aware of a suspected personal data breach must immediately inform Helen Carmel (Business Manager). Where the breach involves electronic systems or devices, Craig Hunter (IT Support Officer) should also be informed to provide technical support. Helen Carmel will coordinate the School's operational response and liaise with the Data Protection Officer as required.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix A.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. 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

Failure to follow this policy or report a breach may result in disciplinary action.

18. Training

All staff and members of the Advisory Board will receive data protection training appropriate to their role as part of induction and at regular intervals thereafter.

Training may include:

- confidentiality;
- subject access requests;
- information sharing;
- data breaches;
- cyber awareness;
- artificial intelligence;
- safeguarding information.

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

19. Monitoring arrangements

Monitoring and Review

The Headteacher has overall responsibility for ensuring that effective data protection arrangements are maintained across Orange Tree School.

Day-to-day operational oversight is delegated to Helen Carmel (Business Manager), who works closely with the Data Protection Officer (Aanika Patel) and the IT Support Officer (Craig Hunter) to ensure compliance with this policy.

The effectiveness of this policy will be monitored through:

- review of data protection incidents and breaches;

- monitoring of Subject Access Requests;
- review of staff training;
- audits of data security arrangements;
- advice from the Data Protection Officer;
- review of changes to legislation and statutory guidance.

This policy will be reviewed annually, or sooner where required by changes in legislation, guidance or following a significant data protection incident.

20. Links with Other Policies

- Cyber Security Policy
- Online Safety Policy
- CCTV Policy
- Safeguarding and Child Protection Policy
- Mobile Phone and Personal Devices Policy
- Staff Code of Conduct
- Privacy Notices
- Records Retention Schedule
- Acceptable Use Agreement

Appendix A – Personal Data Breach Procedure

1. Purpose

Orange Tree School is committed to responding promptly and effectively to any actual or suspected personal data breach. This procedure explains how breaches must be reported, assessed, contained, recorded and reviewed.

It applies to personal data held electronically on paper or in any other format.

A personal data breach is a security incident that results in personal data being accidentally or unlawfully:

- lost, stolen or destroyed;
- altered;
- accessed by an unauthorised person;
- disclosed or sent to the wrong person;
- made unavailable when it is required; or
- otherwise processed without appropriate authority.

Examples may include:

- confidential information emailed to the wrong recipient;
- an EHCP, medical report or safeguarding document shared incorrectly;
- loss or theft of a laptop, telephone, storage device or paper file;
- unauthorised access to a school account or information system;
- confidential information left unsecured;
- personal information entered into an unauthorised artificial intelligence platform;
- a cyber incident involving pupil, staff or family information;
- hard-copy reports sent to the wrong pupil or family; or
- a third-party supplier experiencing a breach involving school information.

2. Immediate Reporting

Any member of staff, member of the Advisory Board, contractor or data processor who discovers or suspects a personal data breach must report it immediately. This includes incidents involving email, electronic systems, accounts, school devices or other technology.

Report immediately to Helen Carmel, Business Manager. Where the incident involves technology, also notify Craig Hunter, IT Support Officer. Helen Carmel will inform the Headteacher and Data Protection Officer where appropriate.

The Data Protection Officer must be informed without delay:

Aanika Patel, Data Protection Officer by emailing data.protection@ellernmede.org

Staff must not wait until they have gathered all the facts before reporting a concern. Prompt reporting is essential because a notifiable breach must be reported to the Information Commissioner's Office, where feasible, within 72 hours of the school becoming aware of it.

3. Immediate Action by Staff

Where it is safe and appropriate to do so, the person discovering the breach should:

- take reasonable steps to prevent further loss, disclosure or access;
- preserve relevant evidence, messages and records;
- attempt to recall an email sent to an incorrect recipient;
- lock or disconnect an affected device if instructed;
- record when and how the concern was discovered;
- avoid deleting relevant emails, files or system information; and
- follow any instructions provided by the Business Manager or IT Support Officer.

Staff must not independently contact the ICO, affected individuals, the media or external organisations unless authorised to do so.

4. Operational Coordination

Helen Carmel will coordinate the school's operational response.

This will include:

- opening a breach record;
- establishing the known facts and timeline;
- assessing the immediate risk;
- coordinating containment and recovery;
- notifying the Headteacher where appropriate;
- involving Craig Hunter where technical support or investigation is required;
- seeking specialist assistance from Netec where necessary; and
- referring the matter promptly to the Data Protection Officer.

Craig Hunter will support the response where the incident involves technology by:

- securing affected systems or accounts;
- resetting passwords or access permissions;
- preserving relevant technical evidence;
- supporting recovery of information or devices;
- liaising with Netec under the direction of Helen Carmel; and
- documenting technical actions taken.

5. Role of the Data Protection Officer

The Data Protection Officer is:

Aanika Patel and her email is: data.protection@ellernmede.org.

The Data Protection Officer will provide independent advice and will:

- advise whether a personal data breach has occurred;
- support the assessment of risks to affected individuals;
- advise whether the breach must be reported to the ICO;
- advise whether affected individuals must be informed;
- support preparation of any required notifications;
- advise on legal, regulatory and documentation requirements; and
- maintain appropriate oversight of the school's response.

The school remains responsible as data controller for decisions and actions taken. The DPO provides independent advice and challenge.

6. Investigation and Risk Assessment

The investigation will establish, as far as reasonably possible:

- what happened and when;
- how the breach occurred;
- the categories of personal data involved;
- whether special category, safeguarding, medical or criminal-offence data was involved;
- the approximate number of people and records affected;
- who has accessed or received the information;
- whether the information can be recovered or secured;
- the possible consequences for affected individuals; and
- what action has already been taken.

The risk assessment will consider the likelihood and severity of harm, including:

- distress, anxiety or reputational harm;
- discrimination;
- identity theft or fraud;
- financial loss;
- risk to physical or emotional safety;
- safeguarding consequences;
- loss of confidentiality; and
- any particular vulnerability of the individuals affected.

7. Containment and Recovery

Depending on the circumstances, the school may:

- recall or delete information sent in error;
- request written confirmation that information has been deleted;
- recover paper records or devices;

- disable accounts or reset passwords;
- restrict access permissions;
- remove information published online;
- contact relevant suppliers or processors;
- notify safeguarding, clinical or professional leads;
- strengthen technical or organisational controls; or
- seek legal, insurance, police or specialist advice.

Where safeguarding information is involved, the Designated Safeguarding Lead must be informed without delay so that any risk to a pupil can be considered separately from the data protection response.

8. Notification to the ICO

Not every personal data breach must be reported to the ICO.

A breach must be reported where it is likely to result in a risk to the rights and freedoms of individuals. A notifiable breach must be reported without undue delay and, where feasible, within 72 hours of the school becoming aware of it. If reporting is delayed, the reason must be recorded and explained.

The report will include, where available:

- a description of the nature of the breach;
- the categories and approximate number of individuals affected;
- the categories and approximate number of records affected;
- the DPO's name and contact details;
- the likely consequences of the breach; and
- the measures taken or proposed to contain the breach and reduce harm.

Where all information is not yet available, an initial report may be submitted within the required timescale and further information supplied in phases.

The Data Protection Officer will advise on whether reporting is required and support the School in completing the notification.

9. Informing Affected Individuals

Where a breach is likely to result in a high risk to individuals' rights and freedoms, affected individuals will be informed without undue delay.

The communication will be clear and accessible and will include:

- a description of what happened;
- the name and contact details of the DPO;
- the likely consequences;
- the action taken or proposed by the school;
- steps the individual may take to protect themselves; and

- how to obtain further information or raise concerns.

The school will consider pupils' age, understanding, SEND and communication needs when deciding how information should be shared.

10. Recording Breaches

All actual or suspected personal data breaches must be recorded, including those that are not reported to the ICO.

The record will include:

- the date and time of discovery;
- the nature and cause of the breach;
- the information and individuals affected;
- the assessment of risk;
- containment and recovery action;
- advice received from the DPO;
- decisions about ICO and individual notification;
- reasons for those decisions;
- actions taken to prevent recurrence; and
- the date the matter was closed.

UK GDPR requires organisations to keep a record of personal data breaches, whether or not they are reportable.

Records will be stored securely in the school's designated confidential data protection records.

11. Review and Learning

Following any significant breach, Helen Carmel, the Headteacher and the Data Protection Officer will review:

- how and why the breach occurred;
- whether procedures were followed;
- whether the response was timely and effective;
- whether staff require further guidance or training;
- whether technical controls or access permissions require amendment;
- whether policies, contracts or privacy notices require updating; and
- whether similar incidents or patterns have occurred.

Actions will be allocated to named individuals and monitored to completion.

The purpose of the review is to strengthen practice and reduce the likelihood or impact of future breaches. Any separate concerns about misconduct or failure to follow procedures may be addressed under the school's appropriate staff procedures.

12. External Guidance and Reporting Links

External Guidance and Reporting Links

- ICO Personal Data Breach Guidance : [guidance on personal data breaches](#)
- ICO Personal Data Breach Self-Assessment Tool: [self-assessment tool](#)
- ICO Online Breach Reporting Form: [‘report a breach’ page](#)
- ICO Helpline: 0303 123 1113

13. Reporting Route

Suspected breach identified

Report immediately to Helen Carmel, Business Manager

↓

Also notify Craig Hunter where technology is involved

↓

Helen Carmel informs the Headteacher and refers without delay to Aanika Patel, DPO

↓

Contain, investigate and assess risk

↓

DPO advises on ICO and individual notification

↓

Record, review and implement learning

Further ICO Guidance

This procedure is based on [guidance on personal data breaches](#) produced by the Information Commissioner’s Office (ICO).

The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO’s [self-assessment tool](#)

The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored, on the school’s computer system, under EMS Private.

Where the ICO must be notified, the DPO will do this via the [‘report a breach’ page](#) of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school’s awareness of the breach.