



Latest Policy Review Date: Sept. 2025

Next Policy Review Date: Sept. 2026

## Data Protection & Confidentiality Policy

### 1. Policy Aims

Oaks Rise aims to ensure that all personal data collected about staff, pupils, parents, directors, visitors and other individuals is collected, stored and processed in accordance with the [General Data Protection Regulation \(EU\) 2016/679 \(GDPR\)](#) 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 [UK-GDPR](#) and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the UK-GDPR. It also reflects the [ICO's code of practice](#) for the use of 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.

Oaks Rise has a responsibility and obligation to consistently maintain its records and record keeping systems to the highest standards. When doing this, the organisation will take account of the following seven Data Protection Principles. Data must:

- Be processed fairly, lawfully and transparently
- Be collected and processed only for specified, explicit and legitimate purposes
- Be adequate, relevant and limited to what is necessary for the purposes for which it is processed
- Be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay
- Not be kept for longer than is necessary for the purposes for which it is processed
- Be processed securely
- Oaks Rise must be accountable for how personal data is processed and ensure that compliance can be demonstrated.

This policy reflects Oaks Rise's current practice, the requirements of current legislation and best practice and guidance. Oaks Rise may vary any parts of this procedure, including any time limits, as appropriate in any case.

### 3. Definitions

Term	Definition
Personal Data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: <ul style="list-style-type: none"><li>• Name (including initials)</li><li>• Identification number</li><li>• Location data</li><li>• Online identifier, such as a username</li></ul> 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: <ul style="list-style-type: none"><li>• Racial or ethnic origin</li><li>• Political opinions</li><li>• Religious or philosophical beliefs</li><li>• Trade union membership</li><li>• Genetics</li><li>• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes</li><li>• Health– physical or mental</li><li>• Sexual orientation</li></ul>
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.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

### 4. Roles and Responsibilities

#### 4.1 The Data Controller

Oaks Rise processes personal data relating to parents, pupils, staff, directors, visitors and others, and therefore is a data controller. Oaks Rise is registered with the ICO, as legally required.

This policy applies to all staff employed by Oaks Rise, to directors and to external organisations or individuals working on our behalf. Staff and directors who do not comply with this policy may face disciplinary action.

## 4.2 Data Protection Officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. They will provide an annual report of their activities directly to the Senior Leadership Team (SLT) and, where relevant, report to the SLT their advice and recommendations on Oaks Rise's data protection issues. The DPO is also the first point of contact for individuals whose data Oaks Rise processes, and for the ICO. Full details of the DPO's responsibilities are set out in their job description. Our DPO is Georgia Rowe and is contactable via email at: [Info@oaksrise.org](mailto:Info@oaksrise.org).

## 4.3. All staff and Directors

Staff and directors are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing Oaks Rise of any changes to their personal data, such as a change of address
- 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 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
  - 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

## 5. Collecting personal data

### 5.1 Lawfulness, fairness, and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that Oaks Rise can fulfil a contract with the individual, or the individual has asked Oaks Rise to take specific steps before entering into a contract
- The data needs to be processed so that Oaks Rise 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 Oaks Rise can perform a task in the public interest or exercise its official authority

- The data needs to be processed for the legitimate interests of Oaks Rise (where the processing is not for any tasks Oaks Rise 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 one 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 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.

## 5.2 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 Oaks Rise's record retention schedule which is available on request.

### 5.3 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 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 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 data protection law. The UK-GDPR is only concerned with restricted transfers. These are transfers of personal data that are being sent, or being made accessible, to:

- A receiver to which the UK-GDPR does not apply (e.g. countries outside of the European Economic Area); and
- A receiver that's a separate organisation or individual, and not someone employed by Oaks Rise.

If we're making a restricted transfer, we:

- Ensure there's an adequacy decision in place from the European Commission; or
- Have an appropriate safeguard in place (usually a contract or agreement with standard data protection clauses included); or
- Ensure the transfer is covered under an exemption

### 5.4 Subject access requests and other rights of individuals

#### 5.4.1 Subject access requests

Individuals have a right to make a subject access request to gain access to personal information that Oaks Rise 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.

#### 5.4.2 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. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

#### 5.4.3 Responding to subject access requests

Subject access requests will be immediately passed to a nominated member of the SLT, to ensure that no potential conflicts of interest occur, and that no member of staff who undertakes data processing is involved in the collation of material for the response. 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.

#### 5.4.4 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, 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 which 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.

## 6. Parental requests to see the educational record

As Oaks Rise is an independent provision, there is no automatic parental right of access to the educational records of children within our setting. However, we feel that transparency is key to good relationships with parents so have therefore chosen to provide parents access to their child's educational record (which includes most information about a pupil) within 15 days of receipt of a written request.

If the request is for a copy of the educational record, Oaks Rise will charge a fee to cover the cost of supplying it. We will also withhold information that could cause serious harm to the physical or mental health of the pupil or another individual, or if releasing the information would mean disclosing exam results before they are officially announced.

## 7. Photographs and videos

As part of Oaks Rise activities, we may take photographs and record images of individuals within Oaks Rise. We will obtain written consent from parents/carers and pupils for photographs and videos to be taken of pupils for communication, marketing and promotional materials. Consent will be obtained for recording from all participants at the start of any lesson. Students who have not given consent for photographs or videos to be taken will be clearly marked on the Contact list.

## 8. Assessment materials

Pupils taking part in assessments with a practical element may be required to submit photographic or video evidence of work done or attainments met. This evidence will be shared with relevant learning facilitators, the examinations officer and the examination board's allocated moderator.

Any such video or photographic evidence will be securely destroyed after the EAR period has elapsed following the relevant examination series, in line with our retention schedule which is available on request.

### *Other use of photographs and videos*

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and 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 Oaks Rise 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 Oaks Rise takes photographs and videos, uses may include:

- Within Oaks Rise on notice boards and in Oaks Rise brochures, newsletters, etc.
- Outside of Oaks Rise by external agencies such as, newspapers or fundraising campaigns
- Online on our Oaks Rise 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.

Photographs and videos for promotional purposes will only be taken of children who are fully dressed (not in swimwear) to reduce the likelihood of inappropriate use.

## 9. 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
- Completing data protection impact assessments where Oaks Rise'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 European Economic Area (EEA), where different data protection laws will apply
- Maintaining records of our processing activities, including:
  - For the benefit of data subjects, making available the name and contact details of the Oaks Rise DPO 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, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the EEA and the safeguards for those, retention periods and how we are keeping the data secure.

## **10. Data security and storage of records**

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

- Paper-based records are kept under lock and key when not in use. Portable electronic devices, such as laptops will not contain personal data on their hard drives. All personal data will be stored on a secure cloud based drive that can only be accessed using two step authentication.
- 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
- Passwords to access Oaks Rise computers, laptops and other electronic devices should be at least 8 characters long and contain upper and lower case letters, numbers & special characters. Staff and pupils are reminded that they should not reuse passwords from other sites

Documents stored on our secure cloud are only shared with the members of staff who need access to them - this minimises the likelihood of accidental editing or deletion of records, and prevents anyone not granted access from viewing the document.

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. Where it

is necessary to share information about a child with a third party, such as a commissioning borough or medical professional, the child will only be referred to by their initials in any covering email.

## **11. 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, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to dispose of records on Oaks Rise's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

## **12. Personal data breaches**

Oaks Rise will make all reasonable endeavours to ensure that there are no personal data breaches. When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches in an Oaks Rise context may include, but are not limited to:

- Oaks Rise safeguarding information being made available to an unauthorised person.
- The theft of an Oaks Rise laptop containing personal data about pupils on the hard drive.

## **13. Training**

All staff and directors will be provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or Oaks Rise's processes make it necessary.

## **14. Monitoring arrangements**

The DPO is responsible for monitoring and reviewing this policy. This policy will be reviewed at least every 2 years and shared with the Senior Leadership Team and staff.

## **15. Types of Data that we hold**

### **15.1 Student data**

This may include:

- Name; Address; Emergency contact details; Previous Oaks Rise(s) attended; Date of birth; Prior educational attainment; EHCP information; Reports from other professionals; Photos of students completing activities; Notes of any safeguarding concerns; Medical information including diagnoses and allergies.

### **15.2 Students' parents/legal guardians data that we hold**

This may include:

- Name; Address; Phone number(s); Email address

### 15.3 Contractor/Employee data that we hold.

These may include:

- Qualifications/references; Eligibility to work documentation, for example photocopies of passport, visas etc. job history; Annual assessment reports; resignation, termination and/or retirement letters; Disciplinary matters; Grievance procedures; Travel and subsistence; contract hours; timesheets/invoices; health assessment records; DBS records.

### 15.4 Recruitment records

Oaks Rise will ensure that no recruitment record is held beyond the statutory period in which a claim arising from the recruitment process may be brought. Unless there is a clear business reason for exceeding this period.

Oaks Rise will carefully consider what information contained on an application form is to be transferred to the employee's employment record and we will not retain information that has no bearing on the ongoing employment relationship.

Oaks Rise may keep an unsuccessful applicant's data on file in case there are future employment opportunities for which they may be suited. We will ask for consent before we keep data for this purpose and such consent, if given, may be withdrawn at any time. Most records will be held in electronic format. We ask that you keep us informed of your personal information, such as your home address or contact details, changes during your working relationship with us.

### 15.5 Payroll and wage records

These may include:

- Overtime details; Rate of pay; Expenses incurred; Court orders; Student loan repayment plan; Banking details; Insurance details for motor and travel; Pension and enrolment details.

### 15.6 Maternity records – if employed

These may include:

- Maternity payment schedules; Dates of maternity leave/ cover; Period of employment without maternity leave; Maternity certificates showing the expected week of confinement

## 16 Emails

Email accounts are not a case management tool in itself. Generally emails may need to fall under different retention periods (for example, an email regarding a health and safety report will be subject to a different time frame to an email which forms part of a pupil record). It is important to note that the retention period will depend on the content of the email and it is important that staff file those emails in the relevant areas to avoid the data becoming lost.

## 17 Lawful, Fair and Transparent Processing

### 17.1 Lawful processing

Personal Information must be processed lawfully. Under data protection laws, there are a number of grounds that make it lawful to process personal information. We will only process personal information if one or more of the following apply:

- The Data Subject has given his or her consent;
- The Processing is necessary for the performance of a contract with the Data Subject;
- The Processing is necessary to meet our legal obligations;
- The Processing is necessary to protect the Data Subject's vital interests;
- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority (often referred to as Public Task)

We recognise that some categories of Personal Information are more sensitive and further conditions must be satisfied if we are to Process this information (Special category and criminal conviction data). Where we Process these categories of Personal Information, we will ensure that we do so in accordance with the additional conditions for Processing set out under the GDPR and the DPA.

### 17.2 Consent

Where it is necessary for us to obtain consent to process personal Information, we will ensure that we do so in accordance with data protection laws. Generally, we will only obtain consent where there is not another lawful ground for processing. Some examples as to when we will obtain your consent is if we want to place a photograph of a pupil in the newspaper, on social media or in other publications to celebrate their achievements.

We recognise that under data protection laws, there are stricter rules as to how consent is obtained. We will ensure that when we obtain consent, we:

- Take steps to ensure that we make it clear to Data Subjects what they are being asked to consent to
- Ensure that the Data Subject, either by a statement or positive action, gives their consent. We will never assume that consent has been given simply because a Data Subject has not responded to a request for consent
- Never use pre-ticked boxes as a means of obtaining consent
- Ensure that a Data Subject is informed that they can withdraw their consent at any time and the means of doing so
- Keep appropriate records evidencing the consents we hold

### 17.3 Transparency

We are required to provide information to Data Subjects which sets out how we use their personal information as well as other information required by law. We will provide this information by issuing Privacy Notices which will be concise, transparent, intelligible, easily accessible, and in clear, plain language.

## 18 Data Retention

Oaks Rise will establish and adhere to standard retention times for categories of information held on the records of job applicants, existing and former employees, workers and contractors. The Organisation will ensure that records which are to be disposed of are securely and effectively destroyed and will keep under review the arrangements for dealing with old records to ensure they are securely disposed of and advise anyone holding records of these arrangements for disposal.

This policy sets out how long employment-related and pupil data will normally be held by us and when that information will be confidentially destroyed in compliance with the terms of the UK General Data Protection Regulation (UK GDPR) and the Freedom of Information Act 2000.

Data will be stored and processed to allow for the efficient operation of Oaks Rise. Oaks Rise Data Protection Policy outlines its duties and obligations under the UK GDPR.

Information (hard copy and electronic) will be retained for at least the period specified in the Oaks Rise Data Retention. Schedule which is available on request. When managing records, Oaks Rise will adhere to the standard retention times listed within that schedule.

Electronic and paper records will be regularly monitored by all individuals within their own area of responsibility.

The Data Retention Schedule lists the many types of records used by Oaks Rise and the applicable retention periods for each record type. The retention periods are based on business needs and legal requirements.

## 19 Data Disposal

Where records have been identified for destruction they will be disposed of in an appropriate way. All information must be reviewed before destruction to determine whether there are special factors that mean destruction should be delayed, such as potential litigation, complaints or grievances.

All paper records containing personal information, or sensitive policy information should be shredded before disposal where possible. All other paper records should be disposed of by an appropriate waste paper merchant. All electronic information will be deleted.

Oaks Rise will maintain a database of records which have been destroyed and who authorised their destruction. When destroying documents, the appropriate staff member should record in this list at least:

- File reference)
- File title/description;
- Number of files; and
- Name of the authorising officer
- Date destroyed or deleted from system
- Person(s) who undertook the destruction.

Any allegations made that are found to be malicious must not be part of the personnel records.

For any other allegations made, Oaks Rise must keep a comprehensive summary of the allegation made, details of how the investigation was looked into and resolved and any decisions reached. This should be kept on the personnel files of the accused.

Any allegations made of sexual abuse should be preserved by Oaks Rise for the term of an inquiry by the Independent Inquiry into Child Sexual Abuse. All other records (for example, the personnel file of the accused) should be retained until the accused has reached normal pension age or for a period of 10 years from the date of the allegation if that is longer. Guidance from the Independent Inquiry Child Sexual Abuse states that prolonged retention of personal data at the request of an Inquiry would not contravene data protection regulation provided the information is restricted to that necessary to fulfil potential legal duties that Oaks Rise may have in relation to an Inquiry.