

Data Protection Policy

V 3 December 2025

Contents

Document Version Control	3
Scope and Purpose	4
Accountability	4
Policy Statement.....	6
Processes and Principals.....	6
General Guidelines	6
Implementation	8
Data Retention Statement.....	8
Data Sharing of Apprentice Assessment Materials	8
Policy Review.....	8
Appendix A - Information the AO may collect and hold.....	9
Appendix B – Data Retention Schedule	11

Document Version Control

Document Details	
Document Name	Data Protection Policy
Document Version Number	V 3 December 2025
Document Status	Published on ACE360 and website
Document Owner	HoQA
Date Approved	December 2025
Next Scheduled Review Date	December 2026

Version History		
Version Number	Date Approved	Change/Reasons for Change/Comments
V 2	October 2023	Addition to Appendix A of sensitive, personal information data collection.
V 3	December 2025	Addition of data retention schedule and data sharing for assessor qualification purposes.

Scope and Purpose

This policy sets out the principles by which the OR Society Awarding Organisation (AO) collects, handles and stores personal data in accordance with its standards and to comply with the General Data Protection Regulation (GDPR) legislation.

The OR Society only collects, handles and stores the personal data it needs to conduct its operations or where it is required to do so by government agencies.

The policy applies to all OR Society staff based at any site or operation. Everyone has some level of responsibility for ensuring that personal data is collected, handled and stored appropriately and in compliance with the law.

The policy applies to all data it holds relating to identifiable individuals. The OR Society online privacy statement can be accessed [here](#).

Personal data is any information relating to a living, identifiable person **who can be identified by** reference to an identifier or in conjunction with other information that is held. It includes things such as name, address, email address (including email addresses of individuals in companies), IP address and also more sensitive types of data, called Special categories of personal data.

Special categories of personal data – this is personal data that gives a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, physical or mental health, sexual life, sexual orientation and criminal record. Special Categories of personal data are subject to additional controls.

The purpose of the policy is to set out how the OR Society:

- Complies with data protection law and follows good practice
- Protects the rights of its staff, students, partners and any organisation or individual with which it does business
- Is open about how it stores and processes individual's data
- Protects itself from the risks of a data breach

Accountability

All staff are responsible for compliance with this policy. The policy helps to protect the AO from data security risks including:

- Breaches of confidentiality
- Processing personal data for which active consent has not been obtained

- Reputational damage as a result of poor data protection practice or data breaches

Everyone who handles personal data must ensure that it is handled and processed in line with this policy and data protection principles, but the following people or groups have key areas of responsibility:

- The Governing Board is the ultimate decision-making authority of the OR Society and is responsible for its overall strategic direction and its legal compliance. It ensures that appropriate processes and procedures are in place to achieve such compliance. Board members conduct themselves in accordance with accepted standards of behaviour in public life.
- The OR Society Data Protection Officer¹ is responsible to the Board for data protection compliance. He has knowledge and experience of compliance, knowledge of the organisation and the authority to carry out the role.
- The Responsible Officer is responsible for day-to-day management and has responsibility for the structure for data processing in the AO, to ensure that appropriate resources are provided to enable good data protection and that staff comply with this policy. They are responsible to the AO Management Team for data protection and control. The post-holder is responsible for maintaining a record of all categories of personal data processing activities carried out on behalf of the OR Society as a data controller and processor.
- The Responsible Officer is responsible for the main assessment activities of the AO and the organisational systems which support these activities including the handling of personal data as part of these.
- The OR Society IT Technician is responsible for the technology provided by the Society to achieve data protection by design.
- The EPA Operations Manager is responsible for personal data processing of all EPA customers' details and also for the framework and content of the OR Society website and ACE360 which is the main means of communication to the public and to users of information about data protection.
- The EPA Operations Manager has day to day responsibility for maintaining the record of personal data processing and also for tracking responses to subject access requests.

¹ The role holder is the OR Society Executive Director who reports directly to the Governing Board.

Policy Statement

The OR Society will process personal data lawfully, fairly and transparently. It will collect data for specified, explicit and legitimate purposes and will process it in line with those purposes.

Personal data collection will be adequate, relevant, limited to what is necessary for the purposes intended and only kept for as long as is required for these purposes. It aims to ensure that personal data held is accurate and is kept up to date and to take every reasonable step to ensure that where the information held is inaccurate that it is removed or put right without delay.

The OR Society takes the security of personal data seriously and will take steps to protect it against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Processes and Principals

General Guidelines

- *Access* – Personal data will only be available to staff who are entitled to access it for lawful and legitimate work purposes.
- *Data protection by design* – we will seek to build in data protection by design in all its practices. It recognises that privacy by design is a requirement.
- *Lawful purpose for processing*– we will only collect, hold and process personal data where it has a lawful purpose for doing so. Where the basis for lawful processing is consent, we will only hold and process personal data where it has confirmed the active consent of an individual to do this. A list of lawful purposes for processing has been identified, which is given as an appendix to this policy.
- *Training* – General training will be provided to all staff in relation to data protection and participation is mandatory. This will be addressed in the induction of all staff and training will be given to enable all staff to understand their responsibilities when handling personal data. Where a member of staff's role may require specific training, this will be provided.
- *Assistance and guidance*- Staff should request help from their line manager in the first instance if they are unsure of any aspect of data protection. Where required, staff and line managers will have access to the IT Lead for organisational support and the EPA Operations Manager where general guidance is required.
- *Resources* – A programme of resources to support data protection will be introduced and maintained by us.

Consent – Where consent is required from an individual to handle their personal data, this will be clear and recorded. This consent can be withdrawn at any time and is made clear to individuals. Care will be taken to ensure that records are kept accurately to show consent. Individuals are entitled to have their data deleted if they request this. Where data is provided by consent, an individual has a right to be forgotten.

Data Storage – We are committed to keeping all data stored securely. Features to protect personal data by technology design will be used by us such as password protection and data encryption. Physical measures will be used where appropriate such as locked filing cabinets, locked rooms. We will review and update our arrangements for the storage of personal data regularly.

Data Usage and grounds for data processing – Personal data will only be used and kept where is needed for OR Society lawful purposes as a regulated awarding organisation.

Data accuracy – we take care to ensure that all data it holds is accurate. If an apprentice or client believe that their personal information held is not accurate or requires change, they should notify the Data Protection Officer. Staff and contractors should notify HR or the Data Protection Officer.

The OR Society will take action immediately to correct personal data when it has been informed that it is not accurate.

Data disclosure – we will only disclose personal data to other organisations where data sharing agreements with those organisations are in place. Apprentices must be informed as part of their enrolment with a training provider that we will share data as described above for lawful purposes when completing its duties as a regulated awarding organisation.

Privacy impact assessments – The circumstances where an impact assessment is required will be kept carefully under review. These will explicitly cover aspects such as how the data is retained securely and for what period.

Subject Access requests – we fully recognise and support the rights of individuals to make a subject access request. Requests should be emailed to the Data Protection Officer by contacting dpo@theorsociety.com where we expect to answer all subject access requests within the 28-day deadline.

Reporting data security breaches – we view data protection of great importance and will treat any data security breach as a matter of urgency. The risks associated with a breach are included in the OR Society' Corporate Risk Register.

When it becomes aware of a breach, we will notify the Information Commissioner and identified affected individuals within 72 hours and sooner wherever possible. AO staff, apprentices and clients must notify the EPA Operations Manager immediately if they suspect that a data breach has taken place.

Implementation

The Data Protection Policy is a key policy to be acknowledged by all AO staff and contractors. This policy will be implemented through training, publicity to staff and through the website.

It will be supported through the use of spot checks and audits and there will be regular reporting across the business. Board members will receive an annual report on data processing compliance and activity as well as other reports from time to time where there are particular developments to be reported or decisions required.

Data Retention Statement

The OR Society is committed to ensure the data it collects, and holds is in line with the ICO's guidance and meets data protection law. Please see Appendix B.

Data Sharing of Apprentice Assessment Materials

Apprentice assessment materials, including assessment recordings, may occasionally be shared for the limited purpose of supporting assessors in achieving their own assessor qualification.

Such sharing will only occur where it is strictly necessary, proportionate, and aligned with the awarding organisation's quality assurance processes.

In all cases, explicit consent will be sought from the apprentice prior to any sharing of their assessment materials, and no materials will be disclosed without this consent. Shared materials will be handled securely, used solely for the stated qualification purpose, and retained only for as long as required under applicable data protection legislation.

Policy Review

Ofqual may require the OR Society to change this policy at any time to ensure compliance with its requirements.

This policy is reviewed as part of the OR Society's continuous improvement monitoring through its annual self-assessment arrangements. It may be reviewed earlier should any feedback or concern be brought to the attention of the OR Society to ensure it remains fit for purpose and the process and its outcomes are deliverable.

Appendix A - Information the AO may collect and hold

The information we may collect	How we collect the information	Why we collect the information	How we use and may share the information
<p>Apprentice name, date of birth, gender, ethnic origin, nationality, OR Society apprentice number, unique apprentice number (ULN), contact details (i.e., address, home and mobile phone numbers, email address).</p> <p>Registration and completion dates; Details of assessments, assessment recordings, qualifications, components and standards achieved.</p> <p>Copy of an apprentice’s photographic ID i.e., passport or driving licence</p>	<p>From OR Society contracted employers/training providers.</p> <p>In some circumstances apprentices may contact us directly and provide this information.</p> <p>From an apprentice during the video recording of remote proctoring sessions or assessments</p>	<p>For the purpose of performing our functions as an Awarding Organisation.</p> <p>The identification of an apprentice.</p> <p>There is a legitimate interest -to maintain apprentice and customer records and to comply with legal, regulatory and corporate governance obligations and good practice.</p> <p>The identification of an apprentice prior to sitting an exam</p>	<p>For the purpose of performing our functions.</p> <p>Data may be shared with our regulators, other educational bodies where appropriate and our external contractors / professional advisers/IT suppliers.</p>
<p>Details of contracted training provider or employer staff, to include name, contact details i.e., home and mobile phone numbers, email address.</p>	<p>From contracted training providers/employers/ assessors/IQAs.</p>	<p>For the purpose of performing our function as an Awarding Organisation.</p>	<p>For the purpose of performing our functions.</p>

<p>All supporting documentation required to confirm staff competency to deliver our qualifications or assessments (i.e., CV, copy of qualification certificates)</p> <p>Sensitive personal information (Special Categories) i.e. information about health including any medical condition, health and sickness records, race or ethnicity, religious beliefs, sexual orientation</p>	<p>In some circumstances staff may contact us directly and provide this information.</p> <p>From contracted training providers and in some cases, apprentices</p>	<p>There is a legitimate interest -to maintain customer and assessor/IQA records and to comply with legal, regulatory and corporate governance obligations.</p> <p>For the purpose of complying with any legal obligation under the Equality Act 2010, such as to apply access arrangements and reasonable adjustments to an apprentices assessment.</p>	<p>Data may be shared with our regulators, other educational bodies where appropriate and our external contractors/professional advisers.</p> <p>We will process this data strictly for the purpose described and will disclose it only as necessary to ESFA or other regulator for the purposes of audit to evidence compliance with legal and regulatory obligations.</p>
--	---	--	---

You are required (by law, regulatory requirements or under the terms of your agreement with us, or in order to enter into an agreement with us) to provide the categories of information specified above to us where applicable, to enable us to provide you with the ability to deliver our qualifications and to administer our apprentice and customer records.

If you would like further details on how we handle sensitive personal information, please contact the Data Protection Officer by contacting dpo@theorsociety.com

Appendix B – Data Retention Schedule

The Society will not keep personal data in a form that permits identification of the subjects for a longer period than is necessary, in relation to the purposes for which it was originally collected.

We may store data for longer periods if the data in question is being archived for standardisation/quality assurance or for statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights of the data subject. Data is currently hosted in ACE360 and the Society's SharePoint with access restricted to members of the awarding organisation function.

The retention period is set out in the Data Retention Schedule below.

Subject	Subsets	Data Gathered	Retention Period
Learner/apprentice	Registration, Assessment completion, certificate production, responding to enquiries, complaints and appeals	Full Name / DOB/ Unique Learner Number, Centre Number, Date of assessment, Qualification Level / Results	Indefinite- will be stored electronically in the OR Society's SharePoint
	Other personal and sensitive Data	ID, Address, Contact information, ethnicity, gender	6 Years
	Accessibility Needs	Application documentation and medical evidence for Special Consideration or Reasonable Adjustment Applications.	3 Years
	Assessment Data	Assessment marking	Assessment marking and grading documents – 3 years

	Retained Assessment Footage	Video Footage (learners assessment retained in SharePoint)	18 months – manually destroyed
	Enquiries about Results and Appeals	All data pertaining to investigation / requests.	3 Years (Enquiry and Appeals log and Incident Log - 6 years)
Any	Malpractice / complaints	All data pertaining to investigations or allegations	3 years (Malpractice and complaints logs - 6 years)
Approved Centres and training providers	Centre Approval and/or point of contracting and ongoing monitoring.	Details of staff, to include name, contact details i.e., mobile phone numbers, email address.	Duration of Approval/contract + 6 Years
Assessors and freelance workers	Pre-Appointment	Application and Interview Documentation	Application (+6 Months if not appointed)
	Recruitment	Contact Info, Application form and CV. Qualifications evidence and references. DBS Records.	Duration of Services + 6 Years
	Standardisation / Training	Training and Assessment Results	Duration of Services + 6 years