

Institute of Conservation

04.03 Data Protection Policy

Policy number	04.03 Data Protection Policy
Summary	This Policy details Icon's approach towards the management of personal data and its compliance with UK GDPR
Who this policy applies to	All staff, volunteers and third party processors with access to personal data
Author / policy contact	Patrick Whife, Policy and Programmes Director
Approved by / approved level	Board of Trustees
Date effective	19.09.2018
Date last reviewed	23.09.2026
Frequency of Review	Annual

1.0	Introduction
1.1	The Institute of Conservation is committed to ensuring that personal data is managed lawfully, fairly, transparently and securely, and that it meets its obligations under UK GDPR, the Data Protection Act 2018 and other applicable legislation.
2.0	Definitions
2.1	GDPR: General Data Protection Regulation (GDPR), the EU's agreed standards for data protection that are also written into UK law through the Data Protection Act 2018 (DPA 2018). ICO: The Information Commissioner's Office (ICO) is the independent public body responsible for upholding information rights and enforcing data protection laws. Personal data: Information which can be used to identify an individual as a data subject. This could include names, addresses, photographs, financial information. Special Category Information: Personal data that is particularly sensitive and given extra protection under data protection law, such as information about health, race or ethnicity, religion, or sexual orientation. Data subject: An individual who can be identified from personal data. Processing: Any operation performed on personal data, including collation, recording, organising, storing, altering, retrieving, using, disclosing or deleting it. Data controller: The organisation which has responsibility for deciding how data is processed and protected. Data processor: An organisation or individual that processes personal data on behalf of a data controller. Individual rights: A data subject's right to control how their personal data is used. There are eight individual rights. Right to be informed: The data subject's right to be informed about how their personal data is used. Right to access: The data subject's right to access personal data held by a data controller.

	3. Right to rectification: The right to request that personal data be corrected if it is inaccurate. 4. Right to erasure: The right to request that personal data be deleted when there is no valid reason to continue holding it. 5. Right to restrict processing: The data subject's right to request the restriction or suppression of their personal data 6. Right to data portability: The data subject's right to obtain or reuse their personal data for their own purposes across different services. 7. Right to object: The data subject's right to object to the processing of their personal data, unless there is a legitimate reason for the processing to continue. 8. Rights related to automated decision making including profiling: The data subject's right not to be subject to a decision based solely on automated processing, including profiling, where that decision produces legal effects or similarly significantly affects them. Individuals have the right to request human intervention, express their view, and challenge the decision. Lawful basis: the valid reason for collecting or using personal data. There are six lawful bases, consent, contract, legal obligation, vital interests, public task, and legitimate interest. Icon relies on four lawful bases for the collection and processing of personal data. 1. Consent: When a data subject is offered a real choice and control over how their personal data is used. It should be freely given, not a precondition of a service, specific and informed (relating to a particular activity), indicated by a positive action to opt-in, separate from other terms and conditions. 2. Contract: When personal data is used to deliver a contractual service. 3. Legal obligation: Collection of personal data to comply with the law, such as employment, and health and safety legislation. 4. Vital interest: where the processing is necessary to protect someone's life. 5. Public task: The processing is necessary to perform a task in the public interests or where official functions and the task of function has a clear basis in the law. 6. Legitimate interests: Where processing is necessary for the legitimate interests of Icon, the data subject, or another party, provided those interests are not overridden by the rights and freedoms of the individual. 7. Recognised legitimate interest: Where the processing of personal data is necessary for one of the following pre-approved purposes: safeguarding vulnerable people; responding to emergencies; preventing or investigating crime; national or public security and defence; sharing personal information with an organisation that needs it for their public task or function of their request. Stakeholder: Any individual or organisation with an interest in Icon's activities, including members, volunteers, donors, employers, training providers, funders, sector partners, government bodies, suppliers and supporters. Personal data breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. Third Party Processor: an individual or organisation who handles personal data on behalf of a data processor.
3.0	Principles of data protection
3.1	Article 5(1) requires that personal data shall be:

	(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency'). (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation'). (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'). (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy'). (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation'); (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')." Article 5(2) adds that: The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').
4.0	Data collected and basis for collection
4.1	We collect and process personal data only where necessary to deliver our services, support our charitable and professional objectives, meet regulatory requirements, and operate the organisation effectively. Depending on the activity, we rely on one or more lawful bases under UK GDPR.
4.2	Membership, Professional Assessment and CPD Data required to administer membership applications, renewals and member services; manage professional accreditation and continuing professional development (CPD), maintain professional registers and directories, complaints and professional standards processes. <u>Data types we may collect</u> • Name and contact details • Personal preferences such as title and pronouns • Membership information • Financial records • Qualifications, training and employment history • Assessment submissions, portfolios and CPD records • Accreditation and assessment outcomes • Assessor and quality assurance records • Appeals and complaints records

	• Reasonable adjustment information and, where necessary, special category data <u>Lawful basis</u> • Performance of a Contract • Legitimate Interests • Explicit Consent for special category personal data where required
4.3	Events and training Data required to organise and deliver conferences, events, training, webinars and learning activities; to manage bookings, registrations and attendance, and communicate information relating to events and learning activities <u>Data types we may collect</u> • Name and contact details • Organisation and job title • Registration and attendance records • Accessibility, dietary and adjustment requirements where necessary • Photographs, video recordings and related media content <u>Lawful basis</u> • Performance of a Contract • Consent (where marketing communications are involved) • Legitimate Interests
4.4	Apprenticeship assessment Data required to administer, deliver and quality assure apprenticeship assessment; comply with regulatory requirements; manage certification, appeals, complaints, malpractice investigations, and external quality assurance activities. <u>Data types we may collect</u> • Name and contact details • Learner, employer and training provider information • Assessment evidence, submissions and records • Assessment outcomes and certification records • Appeals, complaints and quality assurance records • Reasonable adjustment and special category data where required <u>Lawful basis</u> • Performance of a Contract • Legal Obligation • Legitimate Interests • Explicit Consent for special category personal data where required

4.5	Marketing, communication and digital services Data required to communicate with members, subscribers and stakeholder; distribute newsletters, publications and service updates; respond to enquiries; promote events, services, campaigns and charitable objectives, and manage websites, online resources and digital engagement activities. <u>Data types we may collect</u> • Name and contact details • Communication preferences • Subscription records • Enquiry records • Website usage information • Technical data such as IP addresses or online identifiers <u>Lawful basis</u> • Consent • Legitimate Interests
4.6	Research activities Data required to conduct research, surveys and consultations; produce reports, statistics and sector insights, and to support policy development and advancement of professional practice. Where possible research outputs are anonymised or aggregated so that individuals cannot be identified. <u>Data types we may collect</u> • Survey and consultation responses • Research participant information • Demographic information • Membership and service usage data • Statistical and analytical data <u>Lawful Basis</u> • Legitimate Interests • Consent (where individuals actively participate in research activities)
4.7	Fundraising, Donations and Supporter Engagement Data required to administer donations, grants, sponsorships, Gift Aid claims, fundraising activities, legacy giving enquiries and supporter communications. <u>Data types we may collect</u> • Name and contact details • Donation and payment records • Gift Aid declarations • Funding applications and correspondence • Records of supporter engagement

	- Information relating to legacy giving intentions where voluntarily provided <u>Lawful Basis</u> - Consent - Legitimate Interests - Contract (where relevant)
4.8	People management Data is collected to recruit, engage and manage employees, volunteers, interns, assessors, trustees and contractors; to administer contracts, payroll and expenses; manage performance, training and professional development, and to ensure health, safety and wellbeing. <u>Data types we may collect</u> - Name and contact details - Recruitment and employment records - Qualifications and experience - Payroll and payment information - Bank details - Performance and training records - Emergency contact details - Health or other special category data where required - Criminal conviction or DBS information where required for a particular role, activity or legal requirement <u>Lawful Basis</u> - Performance of a Contract - Legal Obligation - Legitimate Interests - Employment-related processing conditions for special category data where applicable
4.9	Governance, Finance and Regulatory Compliance Data is collected to meet legal, regulatory, financial and governance obligations; maintain accurate financial and organisational records; conduct audits and assurance activities; prevent fraud and manage risk, and to investigate complaints and support legal proceedings where necessary. <u>Data types we may collect</u> - Trustee and governance records - Financial and payment records - Audit records - Compliance and regulatory information - Identity and contact information - Correspondence

	<u>Lawful Basis</u> • Legal Obligation • Legitimate Interests • Contract
5.0	Data retention
5.1	Icon only retains personal data for as long as it is necessary. Icon typically adheres to the following retention periods. Apprenticeship assessment: Assessment and quality assurance records are retained for a minimum of 7 years following completion of the apprenticeship, or longer where required to meet regulatory, legal, audit, appeals, complaints, or malpractice investigation requirements. Records are securely destroyed when no longer required. Events and training: For up to 7 years after the event. After this period, limited archival information may be retained where necessary to record attendance at previous events. Fundraising and donor records: Retained for up to 7 years after the last financial transaction or engagement, unless a longer period is required for financial, legal or tax purposes. Governance, Finance and Regulatory Compliance: Finance records are retained for years 7 years from the end of the relevant financial year. Marketing, communication and digital services: Until consent is withdrawn or an individual objects to receiving communications, and for up to 3 years thereafter to maintain suppression lists where required. Website and analytics data are retained in accordance with our cookie settings and retention periods, typically no longer than 26 months. Membership, Professional Assessment and CPD: Full membership records are retained for the duration of membership and for up to 7 years after membership ceases. After this period, limited archival information may be retained where necessary to maintain a record of historic membership, professional accreditation, qualifications, awards or other legitimate organisational interests. People management: Recruitment records for unsuccessful candidates are retained for up to 12 months after completion of the recruitment process. Employee records are retained for the duration of employment and up to 7 years after employment ends, unless a longer retention period is required by law. Research activities: For 5 years following completion of research activity. Reports will be retained indefinitely.
5.2	Icon undertakes an annual audit of personal data held across the organisation to ensure that records remain accurate, relevant and necessary for the purposes for which they are processed. The audit also reviews compliance with retention periods, identifies records due for deletion, and confirms that appropriate technical and organisational measures remain in place to protect personal data.
6.0	Complying with individual rights
6.1	Data subjects have a right to control how their personal data is used. Icon recognises all UK GDPR rights and will respond to requests relating to any of these rights where applicable. There are eight individual rights, although Icon typically relies on five of these rights.

	Right to be informed: Data subjects are informed about how their personal data is collected, used, stored, and shared through Icon's Privacy Notice. As most personal data is provided online via the Icon website, the Privacy Notice is prominently displayed and easily accessible on the website. When registering for services or opting in to receive communications, individuals are required to review and acknowledge the Privacy Notice, confirming that they have been informed about how their personal data will be processed. <i>See Appendix B – Icon Privacy Notice</i> Right to access: Data subjects have the right to access the personal detail held by the data controller. This is done through a Subject Access Request. This request must be made in writing, either by post or email. Icon will review the request and respond in one month. Requests are typically accepted; however, they will be rejected in instances that releasing the data will impact the rights of another data subject. Right to rectification: Data subjects have the right to request the correction of inaccurate or incomplete personal data. In most cases, individuals can review and update their personal information directly through the Icon website. Alternatively, requests for amendments may be submitted by email or post. Icon will review and respond to such requests within one calendar month and will update the data where appropriate. Right to erasure: Data subjects have the right to request the erasure of their personal data. Requests for erasure must be submitted by email or post. Icon will acknowledge and respond to such requests within one calendar month of receipt. Erasure requests will generally be fulfilled unless Icon is required to retain the data to comply with a legal, regulatory, or statutory obligation, or where another lawful basis for retention applies. In such cases, the data subject will be informed of the reason why the request cannot be fully actioned. Right to object: The data subject's right to object to the processing of their personal data, unless there is a legitimate reason for the processing to continue.
7.0	Data storage and security
7.1	Icon primarily uses secure, cloud-based systems to store and manage personal data. These systems include the organisation's CRM platform, financial accounting software, assessment and learning management portals, video conferencing services, and donation management platforms. All key service providers maintain certified Information Security Management Systems, including ISO/IEC 27001 certification, providing assurance that appropriate security controls are in place to protect personal data. Multi-factor authentication (MFA) is enforced across all platforms containing personal or sensitive information to reduce the risk of unauthorised access.
7.2	Paper-based records are not routinely used or created by Icon. Exceptions are made only where records pre-date current operating practices or where hard-copy documentation must be retained to meet statutory, financial, legal, or regulatory requirements. Such records are retained only for the applicable retention period and are securely destroyed when that period expires. Any paper records that are retained are stored in locked and secure facilities with access restricted to authorised personnel, ensuring appropriate protection against loss, unauthorised access, disclosure, or damage.
7.3	The most significant risks to personal data typically arise from human error, unauthorised access, phishing attacks, and other malicious cyber threats. To mitigate these risks, Icon maintains appropriate technical and organisational security measures, including access

	controls, staff awareness training, secure cloud services, and multi-factor authentication. In addition, Icon holds Cyber Essentials certification, demonstrating that fundamental cybersecurity controls are in place to protect systems and reduce the risk of data loss, compromise, or unauthorised disclosure.
8.0	International transfers
8.1	Icon primarily uses UK and internationally hosted cloud-based services to deliver its activities. Where personal data is transferred outside the United Kingdom, Icon will ensure that appropriate safeguards are in place in accordance with UK GDPR. Such safeguards may include adequacy regulations, the International Data Transfer Agreement (IDTA), International Data Transfer Addendum, or other approved transfer mechanisms.
9.0	Access to data
9.1	Access to personal data is limited to staff members who require access to the data in order to perform their role. Staff are provided with full training on data security upon appointment to ensure they have a full understanding of Icon's Data Protection policy.
9.2	Icon shares personal data with third parties where necessary to support its operations and deliver its services. Such third parties may include professional advisers, accountants, auditors, technology providers, and other suppliers acting on Icon's behalf. Personal data is shared only where there is a lawful basis for doing so and where appropriate safeguards are in place to protect the data.
9.3	Icon's volunteers may require access to personal data in order to carry out duties associated with their role. This may include conducting assessments, reviewing Continuing Professional Development (CPD) submissions, administering membership activities, and supporting the delivery of events. Access to personal data is granted on a need-to-know basis and is limited to the information required to perform the relevant function. All volunteers who have access to personal data are required to sign a confidentiality and data protection agreement confirming that they have read, understood, and will comply with Icon's Data Protection Policy, and any other relevant information security requirements. Volunteers are also expected to handle personal data in accordance with applicable data protection legislation and organisational procedures.
9.4	Icon is committed to responding promptly and effectively to any actual, suspected, or potential personal data breach. All incidents will be managed using a proportionate and risk-based approach, taking into account the nature of the breach, the sensitivity of the data involved, the number of individuals affected, and the potential impact on data subjects.
10.0	Data breach management and response
10.1	Icon is committed to responding promptly and effectively to any actual, suspected, or potential personal data breach. All incidents will be managed using a proportionate and risk-based approach, taking into account the nature of the breach, the sensitivity of the data involved, the number of individuals affected, and the potential impact on data subjects.
10.2	Any employee, volunteer, contractor, or third party who becomes aware of a potential data breach must report it immediately to the designated Data Protection Lead (or Chief Executive). Upon notification, the incident will be assessed and documented using Icon's

	Data Breach Assessment Form, which provides a structured method for recording the circumstances of the incident, assessing risks, and determining appropriate actions.
10.3	All data breaches, regardless of severity, will be recorded in Icon's breach log. Where an assessment identifies a risk to the rights and freedoms of individuals, Icon will consider whether notification to the ICO is required and, where applicable, will do so within the statutory timescales. Where a breach is likely to result in a high risk to affected individuals, Icon will also consider whether those individuals should be informed.
10.4	Following resolution of the incident, Icon will conduct a review to identify any corrective actions, training requirements, process improvements, or technical controls necessary to reduce the likelihood of similar incidents occurring in the future.
11.0	Key Roles and Responsibilities
11.1	Effective data protection requires all individuals involved in Icon's activities to understand and fulfil their responsibilities for the secure and lawful handling of personal data. The following key roles have specific responsibilities for ensuring compliance with data protection legislation and this policy.
11.2	Board of Trustees The Board of Trustees has overall accountability for ensuring that Icon complies with its legal, regulatory, and governance obligations relating to data protection. The Board is responsible for: • Providing oversight of data protection and information security risks. • Approving and supporting appropriate policies, procedures, and controls. • Ensuring sufficient resources are available to manage personal data securely. • Reviewing significant data protection issues, including serious data breaches where appropriate.
11.3	Data Protection Lead Icon's designated Data Protection Lead is the Policy and Programmes Director. They are responsible for coordinating data protection activities across the organisation – their responsibilities include: • Maintaining and reviewing data protection policies and procedures. • Providing guidance on data protection requirements and good practice. • Managing data subject rights requests. • Assessing and managing personal data breaches. • Maintaining records of processing activities where required. • Acting as the primary point of contact for data protection matters and regulatory enquiries.
11.4	Employees and Contractors All employees and contractors who handle personal data are responsible for: • Complying with this policy and any related procedures. • Processing personal data only where authorised and for legitimate business purposes.

	• Maintaining the confidentiality and security of personal data. • Reporting actual or suspected data breaches without delay. • Completing any required data protection and information security training.
11.5	Volunteers Volunteers who have access to personal data are responsible for: • Handling personal data only as required for their role. • Maintaining confidentiality at all times. • Following Icon's policies, procedures, and guidance relating to data protection and information security. • Reporting suspected breaches or security concerns immediately. • Signing the required confidentiality and data protection agreement before being granted access to personal data.
11.6	Third Party Processors Icon undertakes appropriate due diligence before appointing data processors and maintains written agreements containing required data protection provisions. Third Party Processors must: • Ensure access controls are implemented and maintained appropriately. • Apply security settings and controls in accordance with organisational requirements. • Review and remove access when no longer required. • Support the investigation and remediation of data protection incidents where necessary.
11.7	Every person acting on behalf of Icon has a responsibility to protect personal data and to contribute to a culture of privacy, security, and accountability. Failure to comply with this policy may result in disciplinary action, termination of engagement, or other appropriate measures depending on the circumstances.
12.0	Managing implementation and review
12.1	This Policy will be reviewed annually to ensure that it is reflective of current regulations and guidance and is responsive to local, national and international events.