THE INSTITUTE OF CONSERVATION

Data Protection Policy

1	**Introduction**
1.1	The Institute of Conservation ('Icon', or 'The Institute') is committed to the protection of the privacy of individuals in compliance with good practice, the General Data Protection Regulation (GDPR) and related data protection and privacy legislation.
1.2	Icon relies on the use of personal data to provide services to Icon members and stakeholders, to achieve core objectives underpinning Icon's charitable status, and to ensure members of the public can identify and access quality-assured conservation professionals. To provide these services and achieve these objectives, Icon processes personal data from members, staff, Trustees, contractors, members of the public and representatives from allied organisations, for purposes including legal and regulatory compliance, and routine business functions of the organisation. Please see Icon's Privacy Notice for information about how Icon processes personal data.
1.3	This policy sets out what we do to protect individuals' personal data. It also explains the key rules on data protection and the legal conditions that must be satisfied when Icon processes (for example, obtain, handle, store and/or transfer) personal data
1.4	The policy applies to all staff, contractors, and volunteers acting on behalf of the organisation or serving Icon in any capacity. Anyone who handles personal data in any way on behalf of Icon must ensure that they comply with this policy, to ensure that Icon is not in breach of data protection law. Any breach of this policy will be taken seriously and may result in disciplinary action or more serious sanctions.
1.5	This policy has been approved by Icon's Board of Trustees. It may be amended from time to time to reflect any changes in legislation, regulatory guidance or internal policy decisions.
2	**Terms and definitions**
2.1	The GDPR applies to **personal data**, which means any information relating to a living person who can be identified directly from that information and other information in our possession. For Icon's purposes, for example, this definition therefore includes name, contact details, membership number, bank or credit card details, and online identifiers such as IP addresses.
2.2	The GDPR also applies to **sensitive personal data (known as "special categories of personal data" under the GDPR),** which includes personal information indicating: (a) racial or ethnic origin; (b) political opinions; (c) religious, philosophical or similar beliefs; (d) trade union membership;

	(e) physical or mental health or condition; (f) sexual life or orientation; (g) genetic data; (h) biometric data; and (i) such other categories of personal data as may be designated as "special categories of personal data" under legislation. This policy also refers to personal data relating to criminal convictions and offences as sensitive personal data. In some cases, in order to process sensitive personal data, we must obtain explicit consent from the individuals involved. As with any other type of information we will also have to be absolutely clear with people about how we are going to use their information. It is not always necessary to obtain explicit consent. There are a limited number of other circumstances in which the GDPR permits organisations to process sensitive personal data.
2.3	Icon is a **data controller**, as the organisation which determines the purposes and means of processing personal data in connection with its work and activities. Icon also works with **data processors** who are responsible for processing personal data on behalf of a controller. This does not include Icon's employees, who are regarded as part of the controller; processors include the publishers of Icon's membership magazine, for example.
2.4	Data Subjects include all living individuals about whom Icon holds personal data; for instance, a volunteer or a member of Icon. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.
2.5	Processing is any activity that involves use of personal data, whether or not by automated means. It includes but is not limited to: (a) collecting; (b) recording; (c) organising; (d) structuring; (e) storing; (f) adapting or altering; (g) retrieving; (h) disclosing by transmission; (i) disseminating or otherwise making available; (j) alignment or combination; (k) restricting; (l) erasing; or (m) destruction of personal data.
3	**Principles**
3.1	Article 5 of the GDPR requires that personal data shall be: *a) processed lawfully, fairly and in a transparent manner in relation to individuals;* *b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;*

	c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; *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;* *e) kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the personal data are processed; and* *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.*
3.2	Article 5.2 of the GDPR requires that: *the controller shall be responsible for, and be able to demonstrate, compliance with the principles.*
3.3	This document sets out the means of compliance with these principles and specifies policies and procedures in place governing the use of personal data across the organisation. We have sought to identify the Icon's main processing activities, and the lawful basis for processing is identified along with the justification for this basis. The GDPR sets out the following lawful bases for processing personal data: (i) The data subject has given their consent to processing (consent must relate to a particular purpose/particular purposes). (ii) The processing is necessary in order to perform a contract to which the data subject is party, or in order to take steps at the data subject's request prior to entering into a contract. (iii) The processing is necessary so that Icon can comply with a legal obligation to which it is subject. (iv) The processing is necessary to protect the "vital interests" of a data subjects or other living individual. In this regard, "vital" means essential for the data subject's life – it is likely to cover, for example, emergency medical situations. (v) The processing is necessary for the performance of a task carried out in the public interest or exercising official authority vested in Icon. Whether processing is in the public interest needs to be carefully considered on a case-by-case basis – please consult the Membership Manager for information as to whether this lawful basis is available. (vi) The processing is necessary for purposes of legitimate interests pursued by Icon or a third party, unless those interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data (in particular where the data subject is a child).
3.4	Where Icon works with data processors, Icon obtains details on the means by which the processors comply with the provisions of the GDPR. Data processors are contractually obligated to comply with Icon's Data Protection Policy, and to regularly furnish relevant details to demonstrate this to Icon's satisfaction.
3.5	Icon communicates the purpose of collection and use of personal data at point of

	collection. This document sets out the means by which these purposes are communicated, along with retention rates.
4	**Purposes of Data Collection and bases for processing**
4.1	Icon collects personal data for specified, explicit and legitimate purposes. The Institute will not collect more personal data than is necessary for the purpose, nor will it retain data for longer than necessary.
4.2	***Governance*** Icon collects personal data to ensure legal and regulatory compliance. This includes **contact details of Icon Trustees**, who are required to be Icon members, and to be added to the corporate Register at Companies House as required by law. Timeframes for retention of these personal details are set out below as part of 4.1.2 – Membership. It is a legal requirement for personal contact details of Trustees to be registered at Companies House, and it is impossible for Trustees to withhold such details and remain a serving Trustee of the organisation. Therefore, the basis for the collection and processing of these personal details is *Necessary to fulfil legal obligations*.
4.3.1	***Membership*** Icon collects personal data **to provide services to paying members of the organisation**. Data collected include names, email and home or work addresses, and phone numbers. These details are required in order to deliver membership benefits, including Icon's membership magazine and scholarly journal, dispatched through the post; and regular email bulletins, sent to the member's registered email address. Phone numbers are required to resolve routine membership issues such as returned post or email bounce backs. Icon also collects bank details of members who wish to pay membership fees by Direct Debit, in order to provide these members with a direct debit payment collection service where they have so requested. In order to ensure the Institute is always able to confirm the past or present membership status of an individual, and to facilitate the resumption of past membership by returning members who may wish to do so, these details are retained on file for a period of five years after last contact. As members decide to join the organisation and pay the fee to receive advertised services – and are required to agree in writing to abide by the Institute's Code of Conduct and Professional Standards as a condition of membership – the basis for the collection and processing of these personal details is their necessity for the *performance of a contract with the subject*.
4.3.2	Icon collects personal data to **administrate the concessionary membership rate and provide discounts on membership fees to those on low incomes**. Members applying for the concessionary rate are required to provide proof that their total annual income is below the given threshold to qualify for the rate. Documentary evidence could include

	• HMRC self-assessment income calculation showing total income for the previous year • Proof of receipt of Jobseeker's Allowance or Housing Benefit • Copy of employment contract signed within the last year • Confirmation from your employer on business letterhead certifying your salary • P45 or P60 Upon receipt of this information to confirm entitlement, Icon allocates charitable funds to subsidise the memberships of conservations on low incomes. It is in the Institute's legitimate interest to ensure those accessing the concessionary rates are entitled to do so, and therefore provide a measure to safeguard fairness in the allocation of Icon's charitable funds. The Institute needs documentary evidence to achieve this aim, and seeks the minimum necessary to be satisfied of eligibility. The Institute does not consider that requiring this evidence causes any undue prejudice to the rights of the applicants seeking concessionary rates (and to the extent that there is any prejudice, that this can be justified by the need to safeguard Icon's charitable funds). As those applying for new memberships or renewing existing memberships do so on the concessionary rate only upon their request, and as it is necessary to determine whether they are eligible in order to safeguard the use of charitable funds, the basis for processing this data is the *necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.* Icon also accepts proof of receipt of disability-related benefits to evidence entitlement for the concessionary rate – and thus will occasionally process special categories of personal data. As members are under no obligation to provide these types of evidence to access the concessionary rate, pursuant to Article 9 of the GDPR and Data Protection Bill, the basis for processing this data is *explicit consent to the processing of those personal data for one or more specified purposes.* Some of the documentary evidence required to obtain concessionary membership may be particularly private (and could be distressing to members if lost or misused), so greater care is taken to ensure that it is kept safe. Data collected for this exercise remains confidential to the Institute and is not disclosed to any third parties, excepting Auditors who may have sight of the documents submitted as part of the annual auditing process. The benefit achieved by the processing will be to ensure that those members who are able to access lower membership fees will be entitled to do so, and therefore to ensure that the Institute's charitable funds are allocated fairly to achieve this purpose. This will in turn reflect the ongoing relationship between the organisation and the individual, as processing will cease if the individual opts to renew on the standard rate, or leaves the organisation. Documents submitted will remain on confidential file for a period of seven years, as statutory financial records evidencing a payment to the organisation alongside the allocation of charitable funds to subsidise that payment.
4.4.1	***Professional Development*** Icon collects personal data to assess the professional skills of **individuals who apply to become Accredited members** of the Institute. This includes employment context,

	professional specialism, details on any disabilities required to facilitate reasonable adjustments to the Accreditation process in line with the Institute's Reasonable Adjustments Policy, employment history, educational background, examples past previous work, and details on individual professional development forward plans. These details are required to enable an assessment to be made to determine whether the applicant has reached the 'proficient' level against Icon's Professional Standards. To ensure the Institute retains sufficient documentation to address questions of feedback, or to respond to a potential challenge of the outcome of an Accreditation assessment or other dispute, these details are retained on file for 6 years from expiry of membership. As applicants apply to become Accredited and are under no obligation to do so, the basis for collection and processing of this data is *Consent.* As the Institute may process data related to special categories of personal data in order to facilitate the enaction of reasonable adjustments, pursuant to Article 9 of the GDPR and Data Protection Bill, the basis for processing this data is *explicit consent to the processing of those personal data for one or more specified purposes.* If consent were to be withdrawn by a subject, the subject's application for Accreditation would be invalidated.
4.4.2	Icon collects personal data **to administrate the Accredited standard**. This includes detail provided in the course of the submission of Continuing Professional Development returns where requested, including the professional development plans of the Accredited members; details on recent training courses or qualifications; and reflections on career progress from individuals. These details are then shared with a designated Accredited peer, who will comment on the submission and provide supportive feedback. This process is required to ensure Accredited members continue to work to the highest professional standards, and are up-to-date with the latest advances and technical approaches in the sector. This is necessary for Institute to guarantee these professionals as "quality assured conservators", indicated by their Accredited status. To ensure the Institute retains sufficient documentation to address questions of feedback, particularly where a CPD return does not meet the required standard, and to retain evidence in the event of a complaint, these documents are retained on file for 6 years following termination of membership. As the Accredited standard cannot be maintained without the requirement for Accredited members to submit evidence of their continuing adherence to quality standards, it is in the legitimate interest of the organisation to ensure Accredited members are doing so. The basis for collection and processing of this data is therefore *Legitimate Interest.* *Privacy Impact Assessment.* A key function of the Institute underpinning its charitable status is to provide public access to quality assured conservators. This cannot be achieved without measures of regular assessment to confirm Accredited individuals are working to the highest professional standards and are keeping up-to-date with the latest advances and technical approaches in the sector. If the assessments were not compulsory, it would not be possible to provide this measure of quality assurance. Those who are Accredited therefore expect some measure of compulsory regular

	reassessment to maintain and defend the high standards of professional practice they have reached. It therefore adds clear value to their memberships, as they can demonstrate to clients, employers, funders and elsewhere that they are senior professionals with a conspicuous mark of quality assurance: as a condition of this it also points to the ongoing relationship between the organisation and the individual. If the scope of this processing were to be modified, the quality assurance provided as a key objective of the organisation could not be verified. Some of the accreditation data processed may be confidential and/or could cause detriment to members if lost or misused (eg by giving an advantage to competitors). As such, Icon takes particular care to ensure this data is kept confidential and safe. *Assessment of risk to data subjects and measures to address those risks.* Icon recognises that sensitive details will likely be included in CPD returns – ranging from personal development plans to self-assessment of skills areas requiring refreshment – and that these details could, for example, provide an unfair advantage to competitors or dissuade potential clients from commissioning certain conservators if leaked or disclosed. The CPD readers appointed to read the CPD return are not from the same conservation specialism as the member being reviewed or are known to them personally – limiting risk of competition. CPD readers indicate those they are unable to read to address any conflict of interest. For these reasons CPD returns are not anonymised at point of reception by a member of Icon staff, but once the conflict issue has been processed, the reviews are anonymised and therefore CPD readers possess no information about the identity of those submitting this sensitive information. The identity of those submitting CPD returns is therefore strictly limited to members of Icon staff and not disclosed to other conservation professionals whatever their roles in the support of Icon's Professional Development programmes. Once this processing has ended, CPD records are held by the Icon office with appropriate measures so as to ensure their security and confidentiality for the statutory period in which they are retained.
4.4.3	Icon processes personal data **to publish details of those conservators who have achieved the Accredited standard (ACR)**. This includes the name and an additional secondary identifier, such city of residence, along with the year in which they achieved their Accreditation. These details are published in a publicly-accessible online directory to ensure members of the public have direct means to confirm the veracity of accounts given by potential conservation service providers – and to ward against confusion between any two Accredited conservators who may share the same name ('*Mary Smith'*). It is a key charitable objective of the organisation to provide the means for members of the public to identify which professionals are Accredited and which not, and therefore to deliver public benefits in quality assurance for those seeking to commission conservation services. Icon publishes only the minimal details necessary for this purpose, and does not consider that doing so causes any prejudice to Accredited members. As it is in legitimate interests of the Institute to ensure no one is able to profess to be Icon-Accredited unless this were verifiably true, the basis for the processing of this data is therefore *Legitimate Interest.* *Privacy Impact Assessment.* A key function of the Institute underpinning its charitable status is to provide public access to quality assured conservators, and so there are regular compulsory checks of Continuing Professional Development returns to confirm Accredited

	individuals are working to the highest professional standards and are keeping up-to-date with the latest advances and technical approaches in the sector. This quality assurance is of no use to the wider public unless members of the public are able to access the means to confirm who is accredited and who is not – but equally, there is no reason members of the public would need data beyond the surname, first name and a general third identifier such as location or city of home base to confirm the status of a potential contractor, employee or grant funding recipient already known to them. For this reason, those seeking this information will first need to know the surname of the individual concerned. Accredited individuals have long asked for a public directory to be deployed in such a way, and so they expect their information to be so processed and published. Icon appreciates there may be a risk to conservators who are obliged to disclose their general location – particularly where this may be the location where priceless artefacts and artworks are stored during the course of conservation work. The risk is intensified by the potential for this general locator to be paired with other information gleaned from alternate sources that could pinpoint the location of such valuables. Icon considers this risk unacceptable. For this reason, the listing will provide a flexible basis to ensure the Accredited conservator themselves can select an additional personal identifier to ensure clarity – ranging from general location, to headshot or middle name. By this means conservators will not be obliged to publicly disclose their location, while ensuring members of the public can distinguish between two Accredited conservators who may share the same name.
4.4.4	Icon processes personal data **to enable members of the public to contact and commission the services of quality-assured conservators** – but only where these conservators have so requested for their details to be provided in this way. In this case, details provided by the Institute include names, email address, and year of Accreditation, provided as part of a searchable 'Enhanced Listing' on Icon's public directory of ACRs – in accordance with the processing pursued in accordance with the *Legitimate Interest* of the organisation. As details are provided beyond what is published in accordance with the legitimate interest of the organisation, and only at the discretion of the Accredited member who must first apply to the Institute to be so listed, the basis for the processing of this 'Enhanced Listing' data is *Consent.* If consent for the provision of an Enhanced Listing were to be withdrawn by a subject, the subject's Enhanced Listing would be invalidated; leaving them with a Standard listing only.
4.4.5	Icon processes personal data **to facilitate the assessment of CPD returns**. This includes the name, email address and telephone numbers of CPD readers, which are shared with each co-reader to enable collaboration as they assess the CPD return for which they are paired as assessors. As individuals are under no obligation to serve as CPD readers, and consent in writing to perform this role where requested by Icon management, the basis for the processing of

	this data is *Consent.* If consent for the processing of contact details in this way were withdrawn by a subject, they would be removed from the register of CPD readers – although the Institute would need to retain the CPD assessments that had previously been submitted by the Reader. The basis for retaining and processing this data is therefore *Legitimate Interest.*
4.4.6	Icon collects personal data **to administrate the Icon Internships programme**. At the application stage, this includes current employment context, employment history, examples of past previous work, educational background, and details on any disabilities required to facilitate reasonable adjustments in line with the Institute's Reasonable Adjustments Policy. These details are required to enable an assessment to be made to determine if the applicant possesses sufficient experience to be selected for the internship. To ensure the Institute retains sufficient documentation to address questions of feedback, these documents are retained on file for 3 years. Applicants must apply to become Icon Interns and have no choice but to provide this information, and they might not be able to reasonably withhold consent from processing if they view the internship as a necessary step in their professional career. As it is in the legitimate interest of the organisation to ensure a fair assessment of those who wish to apply for a limited number of internship places, the basis for retaining and processing this data is therefore *Legitimate Interest*. *Privacy Impact Assessment.* This processing activity is compliant with prevailing standards for the management of interns, and those who have successfully applied, interviewed and won an internship would expect their data to be used this way. There is unlikely to be any significant prejudice to the rights and freedoms of the interns in relation to this processing. The basis for processing special category data to facilitate reasonable adjustments for those with disabilities is its *necessity in connection with employment.*
4.4.7	Icon collects personal data where this has been issued **to facilitate the management of interns in their workplaces**. This includes essays and reports submitted by Interns as part the programme, in order to support their professional development. As some external funders require lengthy retention periods in compliance with rigorous auditing guidelines – particularly where public money has been invested – these documents are retained on file to a maximum of 20 years. As it is in the legitimate interest of the Institute to comply with requirements of external funders, and to manage staff effectively, the basis for the collection and processing of this data is *Legitimate Interest.* *Privacy Impact Assessment.* This processing activity is compliant with prevailing standards for the management of interns, and those who have successfully applied, interviewed and won an internship would expect their data to be used this way. There is unlikely to be any significant prejudice to the rights and freedoms of the interns in relation to this processing.

4.5.1	***Business and Finance*** Icon collects the personal data **to reimburse the organisation's volunteers for expenses incurred** in the course of their work on behalf of the organisation. This includes names, address, bank details to facilitate expenses payments, and evidence of personal activities such as receipts for train travel, sustenance and hotel stays needed to verify the expenses claim. As financial documents, these are retained on file for seven years in compliance with auditing guidelines. As it is in the legitimate interests of the organisation to reimburse the expenses of volunteers, the basis for the collection and processing of this personal data is *Legitimate Interest.* *Privacy Impact Assessment.* Those submitting expenses claims would expect these claims to be settled in the fastest way possible, and the provision of this data in the course of processing such data is a prevailing standard at similar organisations elsewhere. There is unlikely to be any significant prejudice to the rights and freedoms of the interns in relation to this processing.
4.5.2	Icon may sometimes collect personal data to **facilitate payment of external contractors**, particularly where the contractors may be individual sole traders who use their home contact details to administrate their business. These details are then used to raise and pay invoices submitted by the contractor. As financial documents, these are retained on file for seven years in compliance with auditing guidelines. As collection and processing of this data is necessary to pay contractors for their services, the basis for collection and processing of this data is the *necessity for the performance of a contract with the subject.*
4.5.3	Icon processes personal data to complete the annual audit, in compliance with regulatory guidelines. This will include the sharing of a sample of personal and financial data relating to payments to the Institute, which will be reviewed by Icon's external auditors to test internal financial procedures. As it is a legal requirement for the Institute to comply with regulatory guidelines and complete with annual audit, the basis for the processing of this data is *the necessity to fulfil legal obligations.*
4.6.1	***Human Resources*** Icon collects personal data **to recruit staff**. This includes name, addresses, employment history, and educational background. This data is then assessed and measured against a set of defined published criteria in order to select applicants for a paid position. In order to administrate the recruitment of staff, and to ensure hiring decisions can be justified in the event of any request for feedback, these details are retained on file until

	the recruitment cycle has been completed – and therefore to a maximum of 1 year. As applicants are under no obligation to apply for a role at Icon, and are free to share as much personal information as they wish in their applications, the basis for collecting and processing this data is its *necessity in order to take steps at the request of the data subject prior to entering into a contract.*
4.6.2	Icon collects personal data **to pay staff and administrate staff contracts**, in compliance with employment regulations. This includes names, addresses, bank details and emergency next of kin contact details. To justify expenditure for auditing purposes, and to retain sufficient documentation to confirm the past employment status of individuals, these records are retained on file for 7 years after the departure of the member of staff in question. As these details are required to administrate staff contracts, the basis for collecting and processing this data is the *necessity for the performance of a contract with the subject.*
4.6.3	Icon collects personal data **to manage staff**, comprised of performance records where applicable. To ensure Icon can account for staff performance, facilitate the provision of staff references where requested, and defend any legal claims, these records are retained on file for 7 years after the departure of the member of staff in question. As it is in the legitimate interests of the organisation to manage staff effectively, the basis for collecting and processing this data is *Legitimate Interest*. Although occasionally this processing may detrimentally affect individuals (for example, where disciplinary action is taken), any detriment is outweighed by Icon's legitimate interest in managing its staff effectively and holding the information necessary to defend itself against any future legal claims.
4.7	***Fundraising and Marketing*** Icon collects the personal data of non-members to enable the pursuit of fundraising and marketing objectives. This includes names, addresses and email addresses of people the Institute might wish to influence, from whom the Institute might wish to obtain feedback, or invite to an event. These communications are sent within the data subjects' reasonable expectations, and data subjects are provided with transparency information required via the Institute's privacy notice. The Institute only sends this information where it has been requested by non-members, and so the basis for collecting and processing this data is *Consent* *Retainment of records of consent.* To ensure the Institute can manage consent, and particularly to retain an awareness of individuals who have previously refused or withdrawn their consent to be contacted, this data will be stored on Icon's CRM system for a period of 20 years. Icon will refresh consents biennially to ensure the maintenance of up-to-date details. If consent were to be withdrawn by a subject, the Institute would cease to contact them,

	and delete their personal data (except retaining a record that they have asked not to be contacted in this way).
5	**Systems for documenting and managing consent**
5.1	Consent for the processing of personal data related **to the assessment of applications for Accreditation** will be documented on the application form submitted. In accordance with retention guidelines (Appendix 3), this consent is then stored on file for 6 years from expiry of membership. The stipulated lifetime of the consent will not extend beyond the processing timeframes required to assess the application. As processing of the data will usually end with the decision to Accredit the individual or not, there is no circumstance under which the consent for collection and processing of this data will need to be refreshed.
5.2	Consent for the processing of personal data of CPD assessors **to facilitate the assessment of CPD returns** will be documented in explicit written correspondence at the time of each annual agreement to serve as a CPD assessor. To facilitate the process, this consent is then stored on file for the duration of the assessment year in question – after which it is deleted. The stipulated lifetime of the consent will not extend beyond the assessment activity of the assessment year in question. Readers are asked afresh every year if they would be willing to perform the assessment role, at which time relevant consents will be renewed and documented as applicable.
5.3	Consent for the processing of personal data **related to communication with non-members for the purposes of fundraising and marketing** will be documented in explicit written correspondence at the time of each individual agrees to receive free communications from Icon. In a technical sense, these contacts will be managed via Icon's existing CRM system, where the date of consent will also be stored. Correspondence relating to the consent will be stored in on Icon's computer systems, organised annually. To ensure the consent is organic and ongoing, Icon will refresh consents every two years – writing to the individual in question with a comprehensive look at activities over the duration of their consent and requesting permission to continue writing to them for a further two years – in accordance with procedures in place to restrict processing of personal data where requested.
6	**Transparency**
	Every time the Institute receives personal data about an individual directly from that individual, which it is intended to keep, the Institute provides that individual with **"fair processing information"**: a. the type of information we will be collecting (categories of personal data concerned); b. who will be holding their information, including contact details of the relevant

	member of staff c. why we are collecting their information and what we intend to do with it for instance to process donations or send them mailing updates about our activities; d. the legal basis for collecting their information (for example, are we relying on their consent, or on our legitimate interests or on another legal basis); e. if we are relying on legitimate interests as a basis for processing, detail on what those legitimate interests are; f. whether the provision of their personal data is part of a statutory or contractual obligation and details of the consequences of the data subject not providing that data; g. the period for which their personal data will be stored or, where that is not possible, the criteria that will be used to decide that period; h. details of people or organisations with whom we will be sharing their personal data; i. if relevant, the fact that we will be transferring their personal data outside the EEA and details of relevant safeguards; and j. the existence of any automated decision-making including profiling in relation to that personal data. Where we obtain personal data about a person from a source other than the person his or her self, we must provide that individual with the following information *in addition to that listed above:* a. the categories of personal data that we hold; and b. the source of the personal data and whether this is a public source In addition, in both scenarios, (where personal data is obtained both directly and indirectly) we must also inform individuals of their rights outlined below, including the right to lodge a complaint with the ICO and, the right to withdraw consent to the processing of their personal data. This fair processing information can be provided in a number of places including on web pages, in mailings or on application forms. We must ensure that the fair processing information is concise, transparent, intelligible and easily accessible.
7	**Processing data for the original purpose**
	The second data protection principle requires that personal data is only processed for the specific, explicit and legitimate purposes that the individual was told about when we first obtained their information. This means that we should not collect personal data for one purpose and then use it for another. If it becomes necessary to process a person's information for a new purpose, the individual should be informed of the new purpose beforehand. For example, if we collect personal data such as a contact number or email address, in order to update a person about our activities it should not then be used for any new purpose, for example to share it with other organisations for marketing purposes, without first getting the individual's consent.
8	**Personal data should be adequate and accurate**

	The third and fourth data protection principles require that personal data that we keep should be accurate, adequate and relevant. Data should be limited to what is necessary in relation to the purposes for which it is processed. Inaccurate or out-of-date data should be destroyed securely, and we must take every reasonable step to ensure that personal data which is inaccurate is corrected.
9	**Not retaining data longer than necessary**
	The fifth data protection principle requires that we should not keep personal data for longer than we need to for the purpose it was collected for. This means that the personal data that we hold should be destroyed or erased from our systems when it is no longer needed. If you believe the Institute is holding out-of-date or inaccurate personal data, please speak to the Membership Manager. For guidance on how long particular types of personal data that we collect should be kept before being destroyed or erased, please see Appendix 3 below or contact the Membership Manager.
10	**Procedures to protect the rights of individuals**
10.1	***Subject Access Requests*** Individuals have the right to request a copy of any personal data that Icon hold about them, as well as a description of the type of information that we are processing, the uses that are being made of the information, details of anyone to whom their personal data has been disclosed, and how long the data will be stored (known as subject access rights). There will be no charge for fulfilling this request. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject. Those wishing to lodge such a request should do so by writing by email to membership@icon.org.uk. Information must be provided within one month of receipt of the request, though we must first ensure we are satisfied as to the identity of the person making the request for the data.
10.2	***Ensuring accuracy of personal data*** Individuals have the right to have personal data rectified if it is inaccurate or incomplete. In cases where the Institute has provided data to third parties, the Institute will inform them of the rectification, unless this is impossible or would involve disproportionate effort. Individuals wishing to update their personal details should do so in writing by email to membership@icon.org.uk. The Institute will normally amend relevant records within 7 days of receipt of the request.
10.3	***Erasure of personal data*** Individuals have the right to have personal data erased and to prevent processing in specific circumstances – although there exist grounds upon which this request may be refused, including circumstances where the personal data in question is processed for a

	number of purposes: (a) So that Icon can exercise the right of freedom of expression and information. (b) So that Icon can comply with a legal obligation for the performance of a task in the public interest or in the exercise of official authority. (c) For archiving purposes in the public interest; scientific or historical research or statistical purposes; or (e) For the exercise or defence of legal claims. Individuals wishing to lodge such requests should do so in writing by email to membership@icon.org.uk. The Institute will acknowledge to such requests within 7 days of receipt, and normally respond within one month.
10.4	***Objection to the processing of personal data*** Individuals have the right to object to the processing of personal data where this processing is based on *Legitimate Interests.* In some circumstances, the Institute may need to continue to process the data anyway, where there are important reasons to do so which override the rights of the individual. However, Icon will always respect requests to opt-out of direct marketing. The Institute will inform individuals of their right to object at the first point of communication, and in the published privacy notice. Individuals wishing to lodge such an objection should do so in writing by email to membership@icon.org.uk. The Institute will acknowledge such requests within 7 days of receipt, and normally respond within one month.
10.5	***Restriction of processing*** Individuals have the right to request that Icon restricts the processing of their data in certain circumstances (for example, if they say their data is inaccurate, the processing will be restricted while we check the accuracy of the data).
10.6	***Safeguards against automated decision making and profiling*** The Institute of Conservation does not employ any methods of automated decision making or profiling with reference to the processing of personal data, and so no safeguards specific to this aspect are required.
11	**Security**
11.1	***Access to Personal Data*** The Institute has a responsibility to ensure that appropriate organisational measures are in place to prevent the unlawful processing of personal data and to protect against accidental disclosure, loss or destruction of data. Access to personal data processed and stored by the Institute is restricted to specific members of staff responsible for processing the data, and to applicable external service providers contracted as data processors by Icon's Senior Management.

	These external providers are contractually obligated to act in accordance with Icon's Data Protection Policy as a condition of their engagement, and the contract with them is compliant with the requirements of the GDPR. This contract must set out (i) the subject matter, duration, nature and purpose(s) of the processing; (ii) the type(s) of personal data (iii) the categories of data subjects which will be processed, and (iv) the obligations and rights of the controller. The data processing agreement must provide: (i) that the data processor will not engage another data processor without the prior specific or general written authorisation of Icon; (ii) that the data processor will only process personal data based on documented instructions from Icon; (iii) that the person(s) authorised to process the personal data on Icon's behalf commit to the confidentiality of the personal data; (iv) that the data processor will take organisational and technical security measures appropriate to the nature, scope, context and purposes of processing, the type(s) of personal data involved and the associated risks to data subjects; (v) that the data processor will facilitate Icon's obligations to comply with data subjects' request to exercise their rights; (vi) that, bearing in mind the nature of the processing and information available to the data processor, the data processor will assist Icon in complying with the its security obligations, its obligations to report data breaches obligations, and its obligations in relation to data privacy impact assessments. (vii) that the data processor is obliged, at the choice of Icon, to delete or return all the personal data concerned to Icon at the end of the provision of data processing services; and (viii) makes available to Icon all information necessary to demonstrate compliance with obligations under GDPR and related legislation. Compliance is reviewed annually as part of the broader organisational annual reporting cycle.
11.2	***Technical means of ensuring data security*** The Institute has a responsibility to ensure that appropriate technical measures are in place to prevent the unlawful processing of personal data and to protect against accidental disclosure, loss or destruction of data. Icon's membership database is encrypted and stored on a secure server and backed up nightly. Access to the database is via log-in and password, and log-ins are restricted to the specific members of staff responsible for collecting and processing the data. No further access to Icon's membership records is permitted.
11.3	***Staff responsibility*** The Controller's Representatives, who have access to and responsibility for processing and collecting personal data, are set out in the Institute's Privacy Notice, which is updated annually as part of the broader organisational annual reporting cycle and published on the Icon website.

12	**Transferring Data Outside the EEA**
	The GDPR requires that when organisations transfer personal data outside the EEA, they take steps to ensure that the data is properly protected. We may transfer personal data outside the EEA in the following circumstances: a) Where we use cloud storage to back up our servers b) Where we use service providers (for example, to run a survey) who are based outside the European Economic Area (EEA). The European Commission has determined that certain countries provide an adequate data protection regime. These countries currently include Andorra, Argentina, Canada, Guernsey, Isle of Man, Israel, New Zealand, Switzerland, Faroe Islands, Jersey and Uruguay. This list may be updated. As such, personal data may be transferred to people or organisations in these countries without the need to take additional steps beyond those you would take when sharing personal data with any other organisation. In transferring personal data to other countries outside the EEA (which are not on this approved list), it will be necessary to enter into an EC-approved agreement, seek the explicit consent of the individual, or rely on one of the other derogations under the GDPR that apply to the transfer of personal data outside the EEA. The EU-US Privacy Shield is an instrument that can be used as a legal basis for transferring personal data to organisations in the US, although specific advice should be sought from the Membership Manager before transferring personal data to organisations in the US. For more information, please speak to the Membership Manager.
13	**Notification**
	There is no obligation for us to make an annual notification to the ICO under the GDPR, but we will ensure we pay the annual licence fee to the ICO. We will also consult with the ICO where necessary when we are carrying out "high risk" processing. We must report breaches (other than those which are unlikely to be a risk to individuals) to the ICO where necessary, within 72 hours. We will also notify affected individuals where the breach is likely to result in a high risk to the rights and freedoms of these individuals.
14	**Record keeping**
	We must keep a record of our data processing activities, to demonstrate that we are complying with them. These records will include: • the purpose of processing • descriptions of categories of data subjects and categories of personal data • categories of recipients of data • evidence of consent where we are relying on an individual's consent to process their data

	• details of transfers to third countries • retention periods of personal data • a description of security measures.
15	**Reporting**
15.1	The Institute's Board of Trustees is responsible for reviewing the organisation's annual data audit, Data Protection Policy, and privacy notice annually. Ultimately, the responsibility for overseeing compliance with this Data Protection Policy rests with the Board. This includes the approval of the Data Protection Policy in each annual reporting cycle, and the management of risks associated with the implementation of the Policy.
15.2	To ensure the Board of Trustees are able to fulfil this responsibility, as part of the broader organisational annual reporting cycle an annual data protection report will be provided to the board which will include, but not be limited to, the following: • Results of the annual data flow audit, identifying external recipients of personal data collected by the Institute • Details on contractual arrangements with external recipients of personal data to ensure their full compliance with the Institute's Data Protection Policy • Details on any issues that arose with reference to the compliance of external contractors with this policy that arose within the reporting period • Updated Privacy Notices stipulating designated members of staff with responsibility for collecting and processing personal data

Michael Nelles
Membership Manager
June 2018

Appendix 1 –
Basis for collecting and processing personal data by activity

Activity	Basis for collecting and processing
Governance	
Trustee contact details	Necessary to fulfil legal obligations
Membership	
Membership records	Necessary for the performance of a contract
Professional Development	
Accreditation applications *Any related special category personal data*	Consent *Explicit consent for the processing for one or more specified purposes*
CPD returns	Legitimate Interest (submissions) Consent (assessors)
Public listing of ACRs	Legitimate Interest
Enhanced public listing of ACRs	Consent
Internship applications *Any related special category personal data*	Legitimate interest *Necessary in connection with employment*
Intern performance records	Legitimate Interest
Business and Finance	
Payment of expenses	Legitimate Interest
Payment of certain external contractors	Necessary for the performance of a contract
Auditing	Necessary to fulfil legal obligations
Human Resources	
Job applications	In order to take steps at the request of a data subject prior to entering into a contract
Pay staff	Necessary for the performance of a contract
Manage staff	Legitimate Interest

Marketing and Fundraising	
In pursuit of marketing and fundraising objectives	Consent

Appendix 2 –
Method of documentation of Consents where applicable

Activity	**Method of Documentation**
Accreditation applications	In application form submitted at time of application
CPD Readers	In explicit written correspondence at the time of each annual agreement to serve as a CPD assessor
Enhanced public listing of ACRs	In application form submitted at time of application
Internship applications	In application form submitted at time of application
Job applications	In application form submitted at time of application
Marketing and Fundraising	In explicit written correspondence at the time the individual agrees to receive communications from Icon

Means of central recording system – database

Appendix 3 –
Retention rates of personal data by activity

Data	Rate	Rationale
Membership		
Membership records	5 years after expiry of membership	To enable the Institute to confirm the past or present status of an individual To facilitate the resumption of membership by returning lapsed members
Professional Development		
Accreditation applications	6 years from expiry of membership	To justify decisions in light of potential requests for feedback
CPD returns	6 years following expiry of membership	To justify decisions in light of potential requests for feedback
Internship applications	3 years	To justify decisions in light of potential requests for feedback
Intern performance records	20 years	To comply with applicable funding and auditing guidelines
Business and Finance		
Payment of expenses	7 years	In compliance with auditing guidelines
Payment of certain external contractors	7 years	In compliance with auditing guidelines
Human Resources		
Job applications	1 year	To justify decisions in light of potential requests for feedback
Staff records	7 years after departure	To justify expenditure for auditing purposes, and retain sufficient documentation to confirm the past employment status of individuals and defend any potential legal claims.
Marketing and Fundraising		
Non-member contacts	20 years	To ensure the Institute can track who has withdrawn consent in order to ensure continued compliance.