International Community Organisation of Sunderland (ICOS)

Data Protection & Information Security Policy

Document Control

Field	Details
Policy Title	Data Protection & Information Security Policy
Policy Owner	Development and Service Manager (Michal Chantkowski)
Approved By	Board of Trustees
Version Number	2.0
Effective Date	June 2026
Review Frequency	Annual
Next Review Date	June 2027
ICO Registration Number	**ZA125982**

Field	Details
ICO Renewal Date	**28 June annually**
Replaces Version	Version 1.0 (2018)

1 Introduction

International Community Organisation of Sunderland (ICOS) is required by law to comply with data protection legislation, including the Data Protection Act 2018 (DPA 2018), the UK General Data Protection Regulation (UK GDPR), and the Data (Use and Access) Act (DUAA). These legal frameworks regulate the holding and processing of personal information relating to living individuals.

ICOS needs to collect, hold, and use personal information about individuals—such as employees, trustees, volunteers, service users, members, and supporters—to fulfill its charitable objectives, deliver services, and meet legal obligations. To comply with the law, all data must be collected lawfully and fairly, stored safely, and not disclosed unlawfully. All individuals who handle personal data on behalf of ICOS must abide by the data protection principles, follow this policy, and maintain effective internal complaints-handling mechanisms.

2 Data Protection Principles

ICOS is committed to processing personal data in accordance with the seven core data protection principles set out under Article 5 of the UK GDPR. Personal data shall be:

1. **Lawfulness, Fairness, and Transparency:** Processed lawfully, fairly, and in a transparent manner in relation to individuals.
2. **Purpose Limitation:** Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. **Data Minimisation:** Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
4. **Accuracy:** Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay.
5. **Storage Limitation:** 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.
6. **Integrity and Confidentiality (Security):** 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.

7. **Accountability:** ICOS shall be responsible for, and be able to demonstrate compliance with, all the principles listed above. ICOS demonstrates accountability through maintaining records of processing activities, implementing privacy notices, conducting data protection impact assessments, delivering staff training, maintaining breach logs, and establishing clear data retention schedules.

Any breach of this policy, whether deliberate or through negligence, may lead to formal disciplinary action or the termination of an individual's association with ICOS.

3 Definitions

- **Processing:** Any operation performed on personal data, whether or not by automated means. This includes collecting, recording, organising, structuring, storing, adapting, retrieving, consulting, using, disclosing, aligning, restricting, erasing, or destroying data.
- **Personal Data:** Any information relating to an identified or identifiable living individual ('Data Subject'). An identifiable individual is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier, or factors specific to their physical, physiological, genetic, mental, economic, cultural, or social identity. Personal data includes confidential items such as home addresses, salaries, and bank financial details; however, these items are classed as confidential personal data rather than legally defined special-category data.
- **Special-Category Data:** A sub-category of sensitive personal data that requires higher levels of protection. This includes information revealing race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used for unique identification, health data (physical or mental), and data concerning a natural person's sex life or sexual orientation.
- **Criminal-Offence Data:** Information relating to criminal convictions, alleged offences, proceedings, cautions, or Disclosure and Barring Service (DBS) checks. Criminal-offence data is not legally defined as special-category data but is subject to distinct, strict legal protections under section 10 of the DPA 2018.
- **Data Controller:** The natural or legal person or corporate body which (alone or jointly with others) determines the purposes and means of processing personal data. **ICOS as a corporate body is the sole Data Controller**. Employees, trustees, and volunteers are not individual data controllers; they process data on behalf of ICOS and must follow ICOS instructions.
- **Data Processor:** Any natural or legal person (other than an employee of the Data Controller) who processes personal data on behalf of the Data Controller. This includes third-party suppliers, IT providers, or outsourced payroll services.
- **Data Subject:** The living individual to whom personal data relates (e.g., employees, volunteers, trustees, service users, members, and job applicants).

4 Individual Rights & Subject Access Requests (SARs)

4.1 Summary of Rights

Under UK data protection law, Data Subjects have several rights regarding their personal data:

- **Right to be Informed:** The right to clear, transparent information about how their data is processed via Privacy Notices.
- **Right of Access:** The right to request copies of their personal data (Subject Access Requests).
- **Right to Rectification:** The right to request that inaccurate or incomplete data be corrected without delay.
- **Right to Erasure ('Right to be Forgotten'):** The right to request the deletion of personal data where there is no compelling legal reason for its continued processing.
- **Right to Restrict Processing:** The right to block or suppress the processing of personal data under certain conditions.
- **Right to Data Portability:** The right to obtain and reuse their personal data for their own purposes across different services.
- **Right to Object:** The right to object to processing based on legitimate interests, public task, direct marketing, or research purposes.
- **Rights Regarding Automated Decision-Making & Profiling:** The right not to be subject to decisions based solely on automated processing that produce legal or significantly similar effects.

Note: These rights are not absolute and apply only under specific legal circumstances.

4.2 Subject Access Requests (SARs)

- **Making a Request:** A Subject Access Request does **not** need to be in writing. A valid SAR may be made verbally, by email, in writing, via social media, or through any other communication channel.
- **Handling Requests:** Any trustee, employee, or volunteer who receives a verbal or written request for personal data must immediately forward it to the Responsible Person.
- **Identity Verification:** ICOS will take reasonable steps to verify the identity of the applicant before releasing any personal information.
- **Fees:** SARs are provided **free of charge**. A reasonable administrative fee may only be charged if a request is manifestly unfounded, excessive, or repetitive.
- **Timeframe:** ICOS must respond to a SAR without delay and **within one calendar month** of receiving the request and verifying identity. Where a request is complex, or where an individual has made multiple requests, ICOS may extend the response period by up to a further **two months**. If an extension is required, ICOS will inform the applicant within the first month, explaining the reasons for the delay.

5 Lawful Basis for Processing & Special Categories

5.1 Default Lawful Basis

Consent is **not** the default lawful basis for processing personal data. ICOS must identify, establish, and document at least one valid lawful basis under Article 6 of the UK GDPR before collecting or processing any personal data:

1. **Consent:** The individual has given clear, affirmative consent for a specific purpose.
2. **Contract:** Processing is necessary to perform a contract with the individual (e.g., employment or service contracts).

3. **Legal Obligation:** Processing is necessary for ICOS to comply with the law (e.g., HMRC tax reporting, safeguarding law).
4. **Vital Interests:** Processing is necessary to protect someone's life or physical well-being.
5. **Public Task:** Processing is necessary to perform a task in the public interest with a clear basis in law.
6. **Legitimate Interests:** Processing is necessary for the legitimate interests of ICOS or a third party, except where overridden by the individual's data protection rights and freedoms.

5.2 Special-Category Data

Explicit consent is **not** the only condition for processing special-category data. To process special-category data, ICOS must identify **both** an Article 6 lawful basis **and** a specific Article 9 condition under the UK GDPR (such as explicit consent, employment/social security law, vital interests, or processing carried out in the course of legitimate activities by a non-profit body).

5.3 Criminal-Offence and DBS Information

Criminal-offence data, including information derived from Disclosure and Barring Service (DBS) checks, allegations, convictions, and cautions, requires a valid Article 6 lawful basis alongside an explicit condition under Schedule 1 of the Data Protection Act 2018 (e.g., safeguarding or employment requirements).

- **Access:** Access to criminal-offence data is strictly restricted to authorised personnel who require it for recruitment, suitability checks, or safeguarding purposes.
- **Retention and Destruction:** DBS certificate details and criminal-offence records must not be retained for longer than necessary for the purpose for which they were obtained (typically no longer than six months post-recruitment, unless specific regulatory retention applies) and must be securely destroyed via shredded confidential waste or permanent electronic purge.

6 Responsibilities of the Data Controller, Staff, & Volunteers

6.1 Role of the Responsible Person

Primary operational responsibility for data protection compliance within ICOS is assigned to:

- **Lead Responsible Person:**

  Michal Chantkowski (Development and Service Manager)

  Email: `michal@icos.org.uk` | *Phone:* 0759 653 84 82

- **Deputy Responsible Person (acting in absence):**

  Daniel Krzyszczak (Engagement and Operations Manager)

  Email: `daniel@icos.org.uk` | *Phone:* 0759 653 84 82

Data protection queries, subject access requests, and data breach notifications must be directed to Michal Chantkowski, or in his absence, escalated immediately to Daniel Krzyszczak.

6.2 Board of Trustees Oversight

The Board of Trustees holds ultimate legal responsibility for governance and compliance. The Board shall receive regular updates and reports regarding:

- Serious personal data breaches and notifications made to the ICO;
- Formal data protection complaints;
- Compliance risks and Data Protection Impact Assessments (DPIAs);
- Staff and volunteer training completion rates.

6.3 Employee, Trustee, and Volunteer Responsibilities

- **Need-to-Know Access:** Access to personal data is restricted to individuals who require access to perform their specific role. Access permissions will be reviewed periodically and removed immediately upon termination of employment, volunteering, or change of duties.
- **Data Accuracy:** Data subjects and staff must ensure that any personal data provided to ICOS is accurate and updated when changes occur (e.g., address updates).
- **Personal Devices & Email Accounts (BYOD):** Unauthorised personal phones, personal laptops, personal email accounts, or unapproved consumer cloud storage and messaging applications must **not** be used to store, transmit, or process ICOS personal data. All processing must occur through approved, secure ICOS infrastructure unless formally authorized by the Lead Responsible Person under a written policy.
- **Password & Technical Guidance:** Passwords must be strong, unique, and kept confidential. Passwords must never be openly shared or stored insecurely. ICOS mandates multi-factor authentication (MFA) on all business accounts where supported and recommends the use of approved enterprise password management systems.
- **Artificial Intelligence (AI) Tools:** Personal, confidential, or sensitive information must **not** be entered into unapproved artificial intelligence tools, public chatbots, or external online platforms. Any proposed use of AI involving personal data must be reviewed and approved in advance via a Data Protection Impact Assessment (DPIA).

6.4 Training Requirements

- Mandatory data protection induction training must be completed by all new trustees, staff, and volunteers prior to being granted access to personal data.
- Refresher training must be completed annually by all personnel.
- Enhanced, role-specific training will be provided to personnel handling sensitive personal data, service-user casework, safeguarding matters, human resources, or recruitment.

7 Data Retention & Disposal

Personal data must only be retained for as long as necessary to fulfill the purposes for which it was collected, or to satisfy legal, statutory, accounting, or reporting obligations.

ICOS Delivery Data Retention Rule (6-Year Limitation Rule)

- **General Rule:** All project and delivery data (including service-user casework records, delivery evidence, attendance registers, and project-specific personal data) will be retained for a **maximum of 6 years** from the formal end date of the respective project.
- **Legal Justification:** This 6-year retention timeframe explicitly aligns with Section 5 of the **Limitation Act 1980** (statutory limitation period for actions founded on simple contracts and civil claims in England and Wales), as well as general HMRC audit requirements. Retaining project records for 6 years post-completion ensures that ICOS maintains defensive evidence should contractual or legal disputes arise.
- **Exceptions:** Delivery data will be retained beyond 6 years **only** where there is an explicit statutory or regulatory requirement (e.g., specific child safeguarding records requiring longer retention, or grant terms requiring 12-year retention under contracts executed as deeds).

When personal data reaches the end of its designated retention period, it must be permanently erased from electronic systems or physically destroyed via cross-cut shredding or certified confidential waste disposal.

8 Data Protection Complaints Procedure

Individuals have a statutory right under the Data (Use and Access) Act (DUAA) to submit a formal data protection complaint directly to ICOS if they believe their personal data has been mishandled or that their rights have been infringed.

- **Submission Channel:** Complaints should be sent directly via email to **office@icos.org.uk**. Complaints do not require formal legal terminology and will be accepted through any communication method.
- **30-Day Acknowledgment Rule:** ICOS will log and formally acknowledge receipt of any data protection complaint within **30 days of receipt**. (A separate acknowledgment is not required if the substantive investigation and response are completed within those initial 30 days).
- **Investigation Workflow:** Complaints will be investigated by the Lead Responsible Person **without undue delay**.
- **Outcomes & Regulatory Rights:** Complainants will be kept informed of progress. Upon completion, ICOS will provide a written response setting out the outcome and any remedial actions taken. While individuals are expected to utilize this internal complaints procedure first, they retain the right to lodge a complaint directly with the UK Information Commissioner's Office (ICO) at any point.

9 Internal Personal Data Breach Procedure

9.1 Immediate Reporting Requirement

All trustees, employees, volunteers, contractors, and processors must report any suspected or confirmed personal data breach to the Lead Responsible Person (or Deputy) **immediately** upon discovery. Staff must not attempt to evaluate the severity of a breach independently before reporting it.

9.2 Breach Containment and Assessment Process

Upon receiving a breach notification, the Responsible Person shall execute the following internal steps:

1. **Containment & Recovery:** Take immediate technical and operational steps to contain the breach, prevent further loss or disclosure, and recover compromised data.
2. **Risk Assessment:** Assess the likelihood and severity of potential adverse impacts on affected individuals' rights and freedoms (e.g., identity theft, financial loss, discrimination, reputational damage, or distress).
3. **ICO Notification (72-Hour Rule):** If the breach presents a risk to individuals' rights and freedoms, ICOS must notify the Information Commissioner's Office (ICO) without undue delay and **within 72 hours** of becoming aware of the breach.
4. **Individual Notification:** If the breach is likely to result in a **high risk** to the rights and freedoms of individuals, ICOS must inform the affected Data Subjects directly, clearly, and without undue delay.
5. **Documentation & Review:** All breaches, incidents, and near-misses—regardless of whether they were reportable to the ICO—must be recorded in the internal ICOS Data Breach Log, detailing facts, effects, and remedial actions taken.

10 Privacy Notices, DPIAs, & Third-Party Management

10.1 Privacy Notices

At the point of collecting personal data, ICOS must provide clear, accessible, and plain-language Privacy Notices. Privacy notices must explain: the identity of ICOS as Data Controller; what data is collected; the purposes and lawful bases for processing; who the data will be shared with; retention periods; how to exercise data subject rights; and how to submit a complaint.

10.2 Data Protection Impact Assessments (DPIAs)

A DPIA must be carried out prior to initiating any project, system, or processing activity that is likely to result in a high risk to individuals' privacy (e.g., introducing new software platforms, large-scale processing of special-category/vulnerable user data, or systematic monitoring). The DPIA must evaluate necessity, proportionality, privacy risks, and mitigation measures.

10.3 Third-Party Suppliers & Data Processors

Before engaging any third-party supplier or Data Processor to handle personal data, ICOS must conduct due diligence to verify that appropriate technical and organizational security measures are implemented. ICOS must enter into a formal written contract containing standard data processing clauses that require the processor to:

- Process data only on written instructions from ICOS;
- Ensure confidentiality obligations for personnel;
- Implement technical and organizational security;
- Refrain from engaging sub-processors without written authorization;
- Assist ICOS in responding to SARs and managing breaches;

- Delete or return all personal data at the termination of the contract.

10.4 Data-Sharing Arrangements

When sharing personal data with partner agencies, local authorities, funders, or service providers, ICOS must establish a formal Data Sharing Agreement (or confirm written terms) detailing the specific purpose, lawful basis, minimum necessary dataset, security controls, and individual responsibilities of each organisation prior to transfer.

11 International Data Transfers

Restricted transfers of personal data outside the United Kingdom must satisfy specific legal safeguards. ICOS will not transfer personal data outside the UK unless:

- The recipient country is covered by UK Adequacy Regulations;
- Appropriate legal safeguards are in place, such as the UK International Data Transfer Agreement (IDTA) or the UK Addendum to the EU Standard Contractual Clauses; or
- A specific statutory exception applies under Article 49 of the UK GDPR (e.g., explicit consent, performance of a contract, or vital interests).

Where required, a Transfer Risk Assessment (TRA) must be completed and documented prior to executing the transfer.

12 ICO Registration & Related Policies

12.1 Regulatory Fee & Registration Status

ICOS maintains its corporate registration with the UK Information Commissioner's Office (ICO) under registration reference **ZA125982**.

- **Registered Data Controller:** International Community Organisation of Sunderland (ICOS)
- **Registration Reference:** ZA125982
- **Renewal Cycle:** The Data Protection Fee must be renewed **by 28 June each year**.
- **Responsibility:** The Lead Responsible Person (Michal Chantkowski) is responsible for ensuring the annual fee is paid and that registration details are updated prior to the 28 June deadline.

12.2 Related Policies

This policy operates alongside other ICOS organizational policies, including:

- IT & Acceptable Use Policy
- Information Security Policy
- Safeguarding Policy
- Data Breach Procedure & Retention Schedule
- Complaints Policy
- Homeworking & Mobile Device Policy
- Recruitment & HR Policies

Appendix – Operational Guidelines

I. General Responsibilities & Daily Practice

Staff and volunteers must process data fairly, store it securely, and dispose of it when no longer required. Always review the **Checklist for Processing Data** prior to initiating new activities.

II. Dealing with Subject Access Requests (SARs)

Requests may be received verbally or in writing via any channel. Forward SARs immediately to Michal Chantkowski (or Daniel Krzyszczak in his absence). Responses must be provided within **one calendar month** free of charge. Verification of identity is required before releasing information.

III. Handling Confidential, Health, & Employment Information

- **Sickness and Health Information:** Authorised managers or HR staff may access employee sick notes or medical data where necessary for lawful employment, health and safety, or reasonable-adjustment purposes. Only the minimum health information required for the specific management purpose must be shared.
- **Disciplinary and Grievance Information:** Absolute secrecy or complete disclosure regarding outcomes must not be assumed. Disclosure depends on balancing the rights of all individuals involved, employment duties, safeguarding requirements, and legal obligations. Share only what is necessary, lawful, and fair.
- **References:** Confidential employment or educational references may be exempt from disclosure under SARs under specific statutory exemptions. Decisions to disclose or redact references will be based on applicable legal exemptions rather than solely on referee consent.

IV. Images, Photography, & Media

- **General & Crowd Shots:** Photography notices must be displayed at public events. While crowd photographs may not always single out individuals, identifiable persons in public shots remain protected by data protection principles. Objections to image usage will be reviewed fairly on a case-by-case basis.
- **Photographs of Children:** Data protection principles apply alongside ICOS safeguarding policies. Formal written parental or legal guardian consent must be secured prior to photographing or publishing images of children under 13 years of age, detailing specific platforms, storage security, and retention limits.

V. Direct Marketing & Electronic Communications

A clear distinction must be maintained between **essential service updates** (e.g., changes to casework appointments) and **direct marketing or fundraising communications**. Direct marketing via email, SMS, or automated call systems requires prior opt-in consent under the Privacy and Electronic Communications Regulations (PECR), unless a soft opt-in applies. All marketing messages must contain an explicit, clear opt-out mechanism.

VI. Emergency Data Sharing

Personal data may be disclosed to emergency services or medical personnel where necessary to protect an individual's vital interests (life or health).

- **Action Steps:** Staff must confirm that the disclosure is necessary and proportionate, verify the identity of the recipient agency, share only the minimum necessary information, and log the incident details and rationale in writing immediately afterward.

Policy Adoption & Sign-off

This Data Protection & Information Security Policy was formally approved and adopted by the Board of Trustees of the International Community Organisation of Sunderland (ICOS).

- **Approved by the board**
- **Date:** __31/07/206_____
- **Next Scheduled Review Date:** 31/07/2029