

Data Protection and GDPR Policy

Introduction

InterAct is committed to protecting the privacy, confidentiality, integrity, and security of the personal information it processes. The Charity recognises that individuals entrust us with personal information in order for us to deliver services, support beneficiaries, employ staff, engage volunteers, work with partners, and fulfil our charitable objectives.

Protecting personal information is essential to maintaining the trust and confidence of our service users, families, carers, employees, volunteers, trustees, funders, donors, partners, and the wider community.

InterAct processes personal information lawfully, fairly, transparently, and securely in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Data (Use and Access) Act 2025, and other applicable legislation.

The Charity recognises that good data protection is not solely about legal compliance. It is also fundamental to safeguarding, protecting confidentiality, managing information securely, maintaining public confidence, and supporting effective governance.

Purpose

The purpose of this policy is to:

- ensure that personal information is processed lawfully, fairly, and transparently;
- protect the privacy and rights of individuals whose information is held by the Charity;
- ensure compliance with UK GDPR, the Data Protection Act 2018, the Data (Use and Access) Act 2025, and other relevant legislation;
- establish clear responsibilities for the collection, use, storage, sharing, retention, and disposal of personal information;
- promote good information governance and accountability throughout the Charity;
- support the secure handling of personal information in both paper and electronic formats;
- ensure personal information is only accessed where there is a legitimate business need;
- support appropriate information sharing for safeguarding, legal, regulatory, and operational purposes;
- minimise the risk of personal data breaches; and
- maintain the confidence of service users, families, staff, volunteers, trustees, funders, donors, and partner organisations.

Scope

This policy applies to anyone processing personal information on behalf of InterAct and to all personal, special category and criminal record information processed by the Charity regardless of format.

This policy applies throughout the entire information lifecycle, including the collection, recording, use, storage, sharing, retention, archiving, and secure disposal of personal information.

Definitions

Personal Data

Any information relating to an identified or identifiable living individual.

Special Category Data

Personal information requiring additional protection under UK GDPR, including information relating to:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data used for identification;
- health;
- sex life; or
- sexual orientation.

Criminal Offence Data

Information relating to criminal convictions, offences, allegations, or related safeguarding checks, including Disclosure and Barring Service (DBS) information, where processed in accordance with applicable legislation.

Data Subject

The individual to whom the personal information relates.

Processing

Any operation performed on personal information, including collecting, recording, organising, storing, accessing, using, sharing, disclosing, updating, archiving, deleting, or destroying information.

Personal Data Breach

A security incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information.

Legal and Regulatory Framework

This policy has been developed with reference to:

- UK General Data Protection Regulation (UK GDPR);
- Data Protection Act 2018;
- Data (Use and Access) Act 2025;
- Privacy and Electronic Communications Regulations (PECR), where applicable;
- Human Rights Act 1998;
- Freedom of Information Act 2000 (where applicable);
- Common Law Duty of Confidentiality;
- Children Act 1989;
- Children Act 2004;
- Care Act 2014;
- Safeguarding Vulnerable Groups Act 2006;
- Equality Act 2010;
- Charity Commission guidance;
- Information Commissioner's Office (ICO) guidance; and
- other relevant legislation and statutory guidance relating to information governance, safeguarding, and confidentiality.

Roles and Responsibilities

Board of Trustees

The Board of Trustees has overall responsibility for ensuring that InterAct complies with its legal and regulatory obligations relating to data protection and information governance, and will:

- promote a culture of confidentiality, accountability, and good information governance;
- ensure appropriate policies, procedures, and controls are in place;
- oversee significant data protection risks and compliance issues;
- ensure sufficient resources are available to support effective data protection arrangements; and
- review significant personal data breaches and lessons learned where appropriate.

Chief Executive Officer

The CEO is responsible for the day-to-day implementation of this policy and will:

- promote good information governance throughout the Charity;
- ensure appropriate policies and procedures are implemented;
- ensure personal data breaches are managed appropriately;
- support staff and volunteers in understanding their responsibilities;
- ensure appropriate records relating to data protection compliance are maintained; and
- seek specialist advice where necessary.

Managers

Managers are responsible for:

- implementing this policy within their areas of responsibility;
- ensuring staff and volunteers understand their responsibilities;
- ensuring personal information is collected, used, shared, retained, and disposed of appropriately;
- reporting actual or suspected personal data breaches promptly; and

Staff and Volunteers

Everyone working for or on behalf of InterAct has a responsibility to protect personal information.

Staff and volunteers must:

- comply with this policy and associated procedures;
- protect personal information from unauthorised access, disclosure, alteration, loss, or destruction;
- report actual or suspected personal data breaches immediately;
- complete required data protection training; and
- seek advice whenever they are unsure how personal information should be handled.

Policy

Data Protection Principles

InterAct will ensure that personal information is processed in accordance with the principles set out in Article 5 of UK GDPR.

Personal information will be:

- processed lawfully, fairly, and transparently;
- collected only for specified, explicit, and legitimate purposes;
- adequate, relevant, and limited to what is necessary;
- accurate and, where necessary, kept up to date;
- retained only for as long as necessary;
- processed securely using appropriate technical and organisational measures; and
- processed in a manner that enables the Charity to demonstrate compliance with these principles.

The Charity recognises the principle of accountability and will be able to demonstrate compliance with its data protection obligations through appropriate governance, policies, procedures, training, monitoring, and record-keeping.

Lawful Processing of Personal Information

InterAct will only process personal information where there is a lawful basis for doing so under UK GDPR. Depending upon the purpose of processing, lawful bases may include:

- consent;
- performance of a contract;
- compliance with a legal obligation;
- protection of vital interests;
- performance of a task carried out in the public interest; or
- legitimate interests pursued by the Charity or a third party.

The lawful basis for processing will be identified before personal information is collected wherever reasonably practicable.

Where the Charity processes Special Category Data or Criminal Offence Data, an additional condition for processing under the Data Protection Act 2018 and UK GDPR will also be identified and documented where required.

Consent

Where consent is relied upon as the lawful basis for processing personal information, InterAct will ensure that consent is:

- freely given;
- specific;
- informed;
- unambiguous; and
- capable of being withdrawn at any time.

The Charity recognises that consent is only one of several lawful bases for processing personal information and will not rely on consent where another lawful basis is more appropriate.

Consent relating to photographs, videos, marketing communications, and similar activities will normally be obtained separately where appropriate.

Individuals may withdraw their consent at any time unless another lawful basis permits continued processing.

Special Category and Criminal Offence Data

InterAct recognises that much of the information it processes is particularly sensitive and requires a higher level of protection. This may include information relating to:

- physical or mental health;
- disabilities and neurodivergence;
- safeguarding concerns;
- racial or ethnic origin;
- religious or philosophical beliefs;
- sexual orientation;
- criminal convictions or allegations;
- Disclosure and Barring Service (DBS) checks;
- financial hardship; and
- information relating to children and vulnerable adults.

Such information will only be processed where:

- there is a lawful basis for doing so;
- an appropriate condition for processing exists where required;
- access is restricted to those with a legitimate need to know;
- appropriate security measures are in place; and
- the information is handled with the highest levels of confidentiality.

Confidentiality

Everyone working for or on behalf of InterAct has a duty to maintain the confidentiality of personal information obtained through their work.

Personal information must only be:

- accessed where there is a legitimate business need;
- shared with authorised individuals (see below);
- discussed in appropriate settings*;
- stored securely; and
- used only for authorised purposes.

*Staff and volunteers should take particular care when discussing confidential matters in public places, using mobile devices, working remotely, or communicating electronically.

The duty of confidentiality continues after employment, volunteering, or other involvement with the Charity has ended.

Information Sharing

InterAct recognises that appropriate information sharing is essential to delivering safe, effective, and lawful services.

Personal information will only be shared where there is a lawful basis for doing so.

Information may be shared with:

- individuals themselves;
- parents, carers, or advocates where appropriate;
- partner organisations;
- commissioners;
- health and social care professionals;
- schools, colleges, or other education providers;
- local authorities;
- the Police;
- regulators; or
- other organisations where required or permitted by law.

When sharing information, staff should ensure that:

- there is a lawful basis for sharing the information;
- only the minimum information necessary is shared;
- the information is accurate, relevant, and up to date;
- information is shared only with individuals or organisations that have a legitimate need to know;
- appropriate steps are taken to verify the identity of the recipient;
- secure methods of communication are used wherever possible;
- the reasons for sharing the information are appropriately recorded where required; and
- advice is sought from a manager where there is any uncertainty.

InterAct recognises that data protection legislation does **not** prevent the sharing of information where this is necessary to safeguard a child, vulnerable adult, or another individual at risk of harm.

Where safeguarding concerns arise, information may be shared without consent where this is lawful, necessary, and proportionate. Staff should refer to the Charity's safeguarding policies for further guidance.

Information Security

InterAct is committed to protecting personal information against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or unauthorised access.

The Charity will implement appropriate technical and organisational measures to protect personal information, taking into account the nature of the information processed, the risks involved, and available resources.

InterAct will seek to ensure that:

- access to personal information is restricted to those with a legitimate business need and appropriate authorisation;
- appropriate access controls are implemented and reviewed periodically;
- paper records are stored securely and protected from unauthorised access, loss, damage, or theft;
- electronic records are stored using approved systems and protected by appropriate technical security measures;
- appropriate backup, recovery, and business continuity arrangements are maintained for electronic information;
- systems and devices used to process personal information are maintained appropriately and kept up to date with security patches where reasonably practicable;
- confidential information is transmitted securely using approved methods where appropriate;
- personal information is retained and securely disposed of in accordance with the relevant legislation and best practice; and
- information security risks are monitored and managed as part of the Charity's wider governance and risk management arrangements.

Staff and volunteers must:

- store personal information only within approved Charity systems, databases, and storage locations appropriate to the type and sensitivity of the information;
- use only authorised devices, software, and cloud-based systems when processing personal information;
- create and maintain strong, unique passwords and never share passwords with others;
- use multi-factor authentication where available or required by the Charity;
- lock computers, mobile devices, and other equipment whenever left unattended;
- ensure paper records containing personal or confidential information are stored securely and are not left unattended or accessible to unauthorised individuals;
- take appropriate precautions when working remotely or from community venues to prevent unauthorised access to personal information;
- verify the identity of recipients and check email addresses carefully before sending personal or confidential information;
- collect confidential documents promptly from printers and photocopiers;
- not store personal information on personal devices or personal cloud storage services unless specifically authorised by the Charity;
- report lost or stolen devices, suspected cyber security incidents, and actual or suspected personal data breaches immediately; and
- comply with the Charity's Information Security Policy and associated procedures.

Artificial Intelligence (AI)

InterAct recognises that artificial intelligence (AI) technologies may support productivity and administrative tasks. However, they also present potential risks to confidentiality and data protection. Staff, volunteers, and others working on behalf of the Charity must not enter confidential, personal, or special category data into publicly available AI systems unless:

- the use of the system has been authorised by the Charity;
- appropriate contractual and security safeguards are in place;
- the processing complies with UK GDPR and the Data Protection Act 2018; and
- doing so is consistent with the Charity's policies and procedures.

Any proposed use of AI involving personal information should be discussed with the CEO before implementation.

Data Retention and Secure Disposal

InterAct will retain personal information only for as long as necessary to fulfil the purposes for which it was collected, to comply with legal and regulatory requirements, or to establish, exercise, or defend legal claims.

The Charity maintains a separate Data Retention Schedule (Appendix A) which specifies how long different categories of records will normally be retained.

When information is no longer required, it will be disposed of securely.

Secure disposal may include:

- confidential shredding of paper records;
- secure deletion of electronic files;
- secure destruction of storage media; or
- other appropriate disposal methods.

Staff and volunteers must not retain personal information for longer than necessary or dispose of confidential information using ordinary waste disposal methods.

Personal Data Breaches

A personal data breach is any security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information.

Examples include:

- sending personal information to the wrong recipient;
- losing paper records;
- losing laptops, mobile phones, or portable storage devices containing personal information;
- unauthorised access to records;
- cyber attacks or malware;
- accidental deletion of personal information; or
- disclosure of confidential information to an unauthorised person.

All actual or suspected personal data breaches must be reported to the Chief Executive Officer immediately upon discovery.

InterAct will:

- assess the nature and impact of the breach;
- take immediate steps to contain and recover information where possible;
- investigate the cause of the breach;
- maintain appropriate records;
- notify the Information Commissioner's Office (ICO) where legally required;
- notify affected individuals where required; and
- implement measures to reduce the likelihood of similar incidents occurring again.

No member of staff or volunteer should attempt to conceal a personal data breach.

Individual Rights

InterAct is committed to respecting the rights of individuals under UK GDPR. Subject to applicable legal exemptions, individuals have the right to:

- be informed about how their personal information is used;
- request access to their personal information;
- request correction of inaccurate or incomplete information;
- request erasure of personal information in certain circumstances;
- request restriction of processing;
- object to certain types of processing;
- request transfer of personal information where applicable; and
- not be subject solely to automated decision-making where UK GDPR provides such protection.

Requests will be handled promptly and in accordance with statutory timescales (see the next section).

Subject Access Requests and Other Rights Requests

Requests do not need to refer specifically to UK GDPR or describe themselves as Subject Access Requests in order to be valid.

All requests should be forwarded to the Chief Executive Officer as soon as they are received.

InterAct will normally respond within one calendar month of receiving a valid request, although this period may be extended where permitted by law.

The Charity may request additional information to verify an individual's identity before releasing personal information.

Where a request cannot be fully complied with, the Charity will explain the reasons, together with any rights of complaint available to the individual.

Data Protection Impact Assessments (DPIAs)

When introducing new projects, systems, technologies, services, or ways of working, InterAct will consider data protection, privacy, confidentiality, and information security from the outset. The Charity will seek to collect and process only the minimum personal information necessary, ensure appropriate security measures are in place, and identify and manage any risks to individuals before processing begins.

InterAct recognises that certain processing activities may present higher risks to the rights and freedoms of individuals.

Where appropriate, the Charity will undertake a Data Protection Impact Assessment (DPIA) before introducing new systems, technologies, services, projects, or processing activities that are likely to involve high-risk processing.

A DPIA may consider:

- the purpose of the processing;
- the necessity and proportionality of the processing;
- potential risks to individuals;
- measures to reduce or eliminate those risks; and
- whether consultation with the Information Commissioner's Office (ICO) is required.

Data Processors and Third Parties

InterAct may engage third-party organisations to process personal information on its behalf, for example payroll providers, IT support providers, cloud service providers, accountants, or software suppliers.

Where third parties process personal information on behalf of the Charity, InterAct will seek to ensure that:

- appropriate written agreements are in place;
- processors provide appropriate security measures;
- personal information is processed only on the Charity's documented instructions;
- confidentiality is maintained; and
- UK GDPR requirements are met.

The Charity will undertake appropriate due diligence before engaging organisations that will process personal information on its behalf.

International Transfers

InterAct will not normally transfer personal information outside the United Kingdom unless there is a lawful basis for doing so and appropriate safeguards are in place.

Where international transfers are necessary, the Charity will ensure they comply with UK GDPR requirements, including the use of adequacy regulations or other approved transfer mechanisms where applicable.

Photography, Video Recordings and Marketing

Photographs and recordings may be taken for safeguarding, incident recording, service delivery, publicity and marketing, fundraising, training, celebrating achievements, and maintaining a historical record of the Charity's activities.

InterAct recognises that photographs, video recordings, audio recordings, and other images may constitute personal data and, in some circumstances, Special Category Data.

Where photographs or recordings are used for publicity, marketing, fundraising, social media, or publication, the Charity will ensure that an appropriate lawful basis applies and, where consent is relied upon, that valid consent has been obtained.

The Charity will:

- explain how photographs and recordings will be used;
- respect any restrictions placed on the use of images;
- store images securely;
- limit access to authorised individuals; and
- remove or archive images where appropriate and in accordance with the Charity's Data Retention Schedule.

Further guidance is contained within the Charity's Photography and Social Media Policies.

Staff Training and Awareness

InterAct recognises that effective data protection depends upon everyone understanding their responsibilities.

The Charity will seek to ensure that trustees, staff, volunteers, and others working on its behalf receive training and guidance appropriate to their role.

This may include:

- induction training;
- periodic refresher training;
- updates where legislation or guidance changes;
- role-specific training where appropriate;
- information security awareness;
- cyber security awareness;
- recognising and reporting personal data breaches;
- confidentiality; and
- safeguarding information sharing.

Managers are responsible for ensuring that staff and volunteers understand the requirements of this policy and receive appropriate support where necessary.

Monitoring and Compliance

InterAct is committed to maintaining high standards of information governance and continually improving its data protection arrangements.

The Charity will monitor compliance with this policy through a range of measures which may include:

- policy reviews;
- internal audits;
- management oversight;
- review of personal data breaches;
- review of complaints relating to personal information;
- monitoring of subject access requests;
- review of data retention practices;
- staff and volunteer feedback;
- lessons learned from incidents; and
- updates to procedures following changes in legislation or guidance.

The Charity will seek to identify opportunities for continual improvement and will take appropriate action where weaknesses or risks are identified.

Non-Compliance

InterAct expects everyone working for or on behalf of the Charity to comply with this policy.

Failure to comply may expose individuals, service users, the Charity, and others to significant legal, financial, safeguarding, and reputational risks.

Where breaches of this policy occur, the Charity will take appropriate and proportionate action.

For employees, volunteers, trustees, contractors, and others acting on behalf of the Charity, this may include:

- advice, guidance, or additional training;
- supervision or management action;
- disciplinary action;
- termination of volunteering arrangements;
- termination of contracts or service agreements;
- referral to professional or regulatory bodies where appropriate; or
- reporting matters to law enforcement agencies where required.

InterAct recognises that many personal data breaches arise through human error rather than deliberate misconduct. The Charity encourages individuals to report mistakes or concerns promptly so that appropriate action can be taken to minimise harm and identify learning opportunities.

Deliberate misuse of personal information, unauthorised access to records, unlawful disclosure of confidential information, or intentional breaches of this policy may be treated as gross misconduct and could result in dismissal or other appropriate action.

Policy Review

This policy will be reviewed periodically, or sooner where there are:

- changes in legislation or statutory guidance;
- changes to the Charity's activities or systems;
- significant personal data breaches;
- recommendations arising from audits or investigations; or
- organisational learning requiring amendments to policy or procedures.

Appendix A: Data Retention Schedule

Record Type	Minimum Retention Period	Disposal Method
Governing document, Constitution, Articles of Association and Charity Commission registration records	Permanent	Archive
Board and Committee minutes	Permanent	Archive
Policies (superseded versions)	7 years after being replaced	Secure destruction
Strategic plans	7 years	Secure destruction
Risk registers	7 years	Secure destruction
Insurance policies	7 years after expiry	Secure destruction
Insurance claims	7 years after settlement	Secure destruction
Financial accounts	6 years plus the current financial year	Secure destruction
Accounting records, invoices and receipts	6 years plus the current financial year	Secure destruction
Bank statements	6 years plus the current financial year	Secure destruction
Payroll records	6 years plus the current financial year	Secure destruction
HMRC records	6 years plus the current financial year	Secure destruction
Gift Aid records	6 years after the relevant claim	Secure destruction
Contracts and agreements	6 years after expiry or termination	Secure destruction
Procurement records	6 years after contract ends	Secure destruction
Donor records	6 years after the last contact unless consent is withdrawn earlier	Secure destruction
Fundraising consent records	Whilst consent remains valid, then 6 years	Secure destruction
Employee personnel files	6 years after employment ends	Secure destruction
Volunteer records	6 years after volunteering ends	Secure destruction
Trustee records (appointments, declarations and eligibility checks)	6 years after leaving office	Secure destruction
Recruitment records, successful applicants	Personnel file	As personnel file
Recruitment records, unsuccessful applicants	6 months	Secure destruction

Right to Work records	Employment plus 2 years	Secure destruction
DBS recruitment decision records	6 months unless there is a lawful reason to retain them for longer	Secure destruction
Occupational health records	Employment plus 6 years (or longer where legally required)	Secure destruction
Staff training records	Employment plus 6 years	Secure destruction
Service user records	7 years after support ends unless safeguarding or legal reasons require longer retention	Secure destruction
Children's safeguarding records	Until the child's 25th birthday (or longer where required)	Secure destruction
Adult safeguarding records	7 years after case closure unless safeguarding, legal or insurance reasons require longer retention	Secure destruction
Accident books	3 years after the last entry (or longer where children are involved)	Secure destruction
Accident reports involving children	Until the child's 21st birthday	Secure destruction
Incident reports	7 years	Secure destruction
Complaints records	7 years after closure	Secure destruction
Compliments and feedback	3 years	Secure destruction
Equality monitoring information	No longer than necessary and, where possible, anonymised	Secure deletion
Consent forms	Duration of the activity plus 6 years unless linked to safeguarding records	Secure destruction
Photography and media consent forms	Whilst images are retained plus 6 years	Secure destruction
Marketing mailing lists	Until consent is withdrawn or no longer required	Secure deletion
General correspondence	3 years unless incorporated into another record	Secure destruction
Subject Access Requests (SARs)	3 years after closure	Secure destruction
Data Protection Impact Assessments (DPIAs)	6 years after processing ends	Secure destruction
Personal data breach records	6 years after closure	Secure destruction
Information security incident records	6 years	Secure destruction
CCTV recordings (where applicable)	Normally 30 days unless required for investigation	Secure deletion

Version Control

Author: Policy Pros

Policy Owner/Contact Email:

Document classification: Internal

Version Number: 2

Change history

Version 1 [November 2021] Initial issue

Version 2 [September 2026] Reviewed and updated to align with legislation changes. Added more practical guidance for staff.

Approved Date: Sept 2026

Approved By: Vickie Perkins (CEO) and Caroline Clements (Chair)