Data Protection Policy

Voluntary and Community Action Sunderland

Contents

Definitions 2

1. Purpose, scope and principles 3
2. Governance and accountability 3
3. Lawful, fair and transparent processing 3
4. Individual rights and complaints 4
5. Data minimisation, accuracy and retention 4
6. Security and acceptable handling 4
7. Data sharing, processors and international transfers 5
8. Direct marketing, cookies and new technology 5
9. Personal data breaches 5
10. Training, monitoring and review 5

Definitions

Charity	means Voluntary and Community Action Sunderland (VCAS).
Data protection law	means the UK GDPR, the Data Protection Act 2018, the Data (Use and Access) Act 2025, the Privacy and Electronic Communications Regulations 2003 (PECR), and other applicable legislation and regulatory guidance, as amended.
Personal data	means information relating to an identified or identifiable living person.
Special category data	includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic data, biometric data used for identification, health data, and data concerning a person's sex life or sexual orientation.
Responsible Person	means the person appointed by VCAS to oversee data protection compliance; the current postholder and contact details shall be recorded internally and in relevant privacy notices.
Record of Processing Activities	means VCAS's documented record of personal-data processing, including purposes, lawful bases, categories, recipients, retention periods and safeguards.

1. Purpose, scope and principles

This policy applies to all trustees, employees, volunteers, contractors and third parties who process personal data for or on behalf of VCAS. It covers personal data in electronic, paper, audio-visual and other forms, wherever processed.

VCAS shall comply with the seven UK GDPR principles:

a. lawfulness, fairness and transparency;
b. purpose limitation;
c. data minimisation;
d. accuracy;
e. storage limitation;
f. integrity and confidentiality; and
g. accountability, including keeping evidence of compliance.

2. Governance and accountability

3. Lawful, fair and transparent processing

a. Before processing begins, VCAS shall identify and document its purpose, UK GDPR lawful basis and, where relevant, an Article 9 condition and Data Protection Act 2018 Schedule 1 condition.
b. Recognised legitimate interests introduced by the Data (Use and Access) Act 2025 may be used only where the statutory conditions apply; other legitimate-interests processing requires a documented balancing assessment.

c. Privacy information shall be concise, accessible, accurate and provided at the appropriate time. It shall explain purposes, lawful bases, sharing, retention, rights, complaints and any material automated decision-making.
d. Consent shall be freely given, specific, informed, unambiguous, recorded and as easy to withdraw as to give. VCAS shall not rely on consent where another basis is more appropriate.

4. Individual rights and complaints

a. VCAS shall recognise requests for access, rectification, erasure, restriction, portability, objection and rights concerning automated decision-making, regardless of the wording or channel used.
b. Requests shall be logged, identity verified proportionately, relevant systems searched, exemptions considered and responses issued without undue delay and within the applicable statutory time limit. The period may be paused where permitted while necessary clarification or identity evidence is awaited.
c. Individuals have an absolute right to object to direct marketing. Suppression records shall be maintained so that opt-outs are respected.
d. VCAS shall operate an accessible data-protection complaints process, acknowledge complaints promptly and provide an outcome without undue delay and within the period required by law. Individuals shall be told of their right to complain to the ICO.
e. Fees shall be charged or requests refused only where permitted by law, with reasons and information about complaint rights.

5. Data minimisation, accuracy and retention

a. VCAS shall collect and use only personal data that is adequate, relevant and necessary for the documented purpose.
b. Personal data shall be checked and corrected where appropriate, with reasonable steps taken to notify recipients of material corrections.
c. A documented retention schedule shall set retention periods or review criteria for each record category. Data shall be securely deleted, anonymised or archived when no longer required, subject to legal, safeguarding, funding and evidential needs.
d. Regular data-quality and disposal reviews shall be completed and recorded.

6. Security and acceptable handling

a. VCAS shall use risk-based technical and organisational measures, including least-privilege access, strong authentication, timely patching, supported software, encryption where appropriate, secure configuration, logging, tested backups and secure disposal.
b. Access shall be reviewed regularly and removed promptly when roles change or end. Personal data shall not be stored on unauthorised devices, personal accounts or unapproved services.
c. Staff and volunteers shall follow clear rules for email, remote working, cloud services, removable media, paper records and sharing. Suspected phishing, loss or unauthorised access must be reported immediately.

d. VCAS shall maintain and rehearse incident response and business-continuity arrangements, taking account of current NCSC guidance for charities and small organisations.

7. Data sharing, processors and international transfers

a. Personal data shall be shared only where lawful, necessary, proportionate and secure. Routine or high-risk sharing shall be documented in an agreement or protocol.
b. Processors shall be selected through due diligence and bound by a written contract containing the terms required by UK GDPR. Their security and compliance shall be monitored.
c. Before transferring personal data outside the United Kingdom, VCAS shall confirm that a lawful transfer mechanism applies, complete any required transfer risk assessment and implement supplementary safeguards.
d. Requests from police, regulators or other authorities shall be verified and documented; only necessary information shall be disclosed unless disclosure is legally required.

8. Direct marketing, cookies and new technology

a. Direct marketing shall comply with UK GDPR, PECR and ICO guidance. Every message shall identify VCAS and provide a simple opt-out.
b. The charitable-purposes soft opt-in may be used only where all statutory conditions are met, the person expressed interest in or offered support for VCAS's charitable purposes, contact details were obtained in the permitted context, and an opt-out was offered when details were collected and in every message.
c. Non-essential cookies and similar storage or access technologies shall be used only with valid consent unless a statutory exception applies. Choices must be clear, granular and easy to change or withdraw.
d. Artificial intelligence, profiling and automated tools shall undergo documented necessity, fairness, transparency, security and human-oversight assessment before use. High-risk processing requires a DPIA.

9. Personal data breaches

Every suspected personal data breach must be reported immediately to the Responsible Person. VCAS shall contain the incident, preserve evidence, assess risks to individuals, document decisions and notify affected processors or controllers as required. Where a breach is likely to risk people's rights and freedoms, VCAS shall notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware. Where the risk is high, affected individuals shall also be informed without undue delay, unless a legal exception applies. All breaches, including those not reported externally, shall be recorded and reviewed for lessons learned.

10. Training, monitoring and review

a. All trustees, employees and volunteers handling personal data shall receive induction and refresher training appropriate to their responsibilities and shall confirm that they understand this policy.
b. Compliance shall be monitored through periodic reviews of access, processing records, privacy information, contracts, retention, security, rights requests,

complaints and incidents.

c. Breaches of this policy may result in access removal, disciplinary action, contract action or referral to an authority, as appropriate.
d. This policy takes effect on 3 September 2026 and shall be reviewed at least annually, and sooner following material legal, regulatory, technological or organisational change. Because some ICO guidance is being updated following the Data (Use and Access) Act 2025, the Responsible Person shall monitor ICO publications and revise procedures promptly where needed.