

GOVERNANCE & POLICIES



POLICY

Privacy, Data Protection and GDPR Policy

Adopted by the Board of Directors

25th May 2026

KENT WITH UKRAINE LTD

www.kentwithukraine.co.uk

Privacy, Data Protection and GDPR Policy

Kent With Ukraine's Data Protection and GDPR Policy applies to: Trustees, directors, staff, volunteers, advisers, secondees, contractors, consultants, delivery partners and anyone processing personal data on behalf of Kent With Ukraine

Review date: This policy shall be reviewed annually, or sooner following any serious incident, data breach, change in law, funder requirement or material change in operations.

Kent With Ukraine's Data Protection and GDPR Policy was updated and approved by our Board of Directors on 25th May 2026.

1. Who We Are and Purpose

Kent With Ukraine is committed to handling personal data lawfully, fairly, securely and transparently.

As a UK-based not-for-profit non-governmental organisation [NGO] working in support of Ukraine's resilience, recovery, humanitarian needs, veterans, civic partnerships and community links, Kent With Ukraine may process personal data relating to volunteers, donors, supporters, beneficiaries, partners, public officials, contractors, employees, secondees, veterans, displaced people, children, families, vulnerable adults and website users.

This policy sets out how Kent With Ukraine collects, uses, stores, shares, transfers, protects and deletes personal data in accordance with the UK General Data Protection Regulation, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations and relevant guidance issued by the Information Commissioner's Office.

Company Information:

We are a company limited by guarantee that is registered in England and Wales: 17220633

Our Registered Office is: Kent With Ukraine Ltd, 128 City Road, London. EC1V 2NX

Our mailing address is: Kent With Ukraine, Suite 2025, Fleet House, Springhead Road, Northfleet, Gravesend, DA11 8HU

Our Directors are: Mrs Iris Smith and Mrs Helen Ashenden

Policy Statement

Kent With Ukraine will:

- process personal data lawfully, fairly and transparently;
- collect personal data only for clear, legitimate and specific purposes;
- collect only the data needed for those purposes;
- keep personal data accurate and up to date where necessary;
- retain personal data only for as long as needed;
- protect personal data against unauthorised access, loss, misuse, alteration or disclosure;
- respect the rights of individuals whose data we hold;
- take particular care with sensitive, safeguarding-related, medical, disability, veterans, children's and conflict-affected data;
- ensure that data shared with partners in Ukraine or elsewhere is appropriately protected;
- maintain accountability records showing how we comply with data protection law.

2. ICO Registration

Kent With Ukraine will register with the Information Commissioner's Office and will maintain its registration for as long as it processes personal data in a way that requires registration or payment of the data protection fee.

Kent With Ukraine will:

- complete and maintain ICO registration as a data controller;
- pay the relevant data protection fee where required;
- renew ICO registration annually or as otherwise required;
- keep a copy of its ICO registration certificate on file;
- record the renewal date in the organisation's compliance calendar;
- update the ICO where the organisation's details, contact details or data protection contact change.

Even where a legal exemption may arguably apply, Kent With Ukraine's policy position is to maintain ICO registration as a matter of transparency, accountability and funder confidence unless formally advised otherwise.

3. Roles and Responsibilities

4.1 Board of Directors

The Board has overall responsibility for ensuring that Kent With Ukraine complies with data protection law and this policy.

The Board will ensure that:

- data protection risks are considered as part of organisational governance;
- adequate policies, procedures and controls are in place;
- data protection risks are reviewed where projects involve vulnerable people, children, veterans, displaced persons, medical information or cross-border data sharing;
- serious breaches are escalated appropriately;
- funder and regulatory reporting obligations are met.

4.2 Data Protection Lead

Kent With Ukraine will appoint a named Data Protection Lead responsible for day-to-day oversight of data protection compliance. At the publication of this Policy this role will be undertaken by the Head of Mission, who is responsible to the Directors for data protection and security.

The Data Protection Lead will:

- maintain the data protection policy and associated procedures;
- keep a record of processing activities;
- advise staff and volunteers on data protection matters;
- review privacy notices and consent forms;
- assess data sharing and international transfer risks;
- coordinate responses to data subject rights requests;
- maintain breach records;
- support breach reporting to the ICO where required;
- keep retention schedules under review.

Kent With Ukraine may review the need to appoint a formal Data Protection Officer if required by law or if the scale, sensitivity or risk profile of its activities makes this appropriate.

4.3 Staff, Volunteers and Representatives

Everyone processing personal data for Kent With Ukraine must:

- follow this policy;
- complete any required data protection training;
- collect only the data they are authorised to collect;
- use personal data only for approved purposes;
- keep personal data secure;
- report any suspected data breach immediately;
- avoid sharing personal data through personal devices, private email accounts or informal messaging channels unless specifically authorised and risk assessed.

5. Types of Personal Data We May Collect

Kent With Ukraine may collect and process the following categories of personal data:

5.1 Volunteers, Staff and Advisers

- legal names;
- contact details;
- emergency contact details;
- role details;
- availability;
- identity verification information including personal photographic ID and national documents;
- references;
- skills, training and qualifications;
- safeguarding, DBS, Vetting checks where required;
- travel documents where needed for missions;
- expenses and payment information including bank account details;
- health or accessibility information where necessary for duty of care;
- records of conduct, training, incidents or complaints.

5.2 Donors, Supporters and Fundraisers

- name;
- contact details;
- donation history;
- Gift Aid information where applicable;
- communication preferences;
- fundraising activity;
- event attendance;
- bank or payment details where required;
- correspondence and supporter engagement records.

5.3 Beneficiaries and Project Participation

Depending on the project, Kent With Ukraine may process:

- name;
- contact details;
- location or community information;
- age or date of birth where necessary;
- family or household information;
- vulnerability or support needs;
- disability or accessibility information;
- veteran status;
- displacement status;
- service access needs;
- case notes;
- consent records;
- photographs, videos or testimonies;
- monitoring and evaluation data.

Kent With Ukraine will collect beneficiary data only where necessary, proportionate and justified by the project purpose.

5.4 Partners, Public Officials and Institutional Contacts

- name;
- role/title;
- organisation;
- work contact details;

- meeting records;
- correspondence;
- project responsibilities;
- due diligence information;
- conflict of interest declarations where relevant.

5.5 Website Users

Kent With Ukraine may collect:

- contact form submissions;
- newsletter sign-ups;
- donation form information;
- event registration details;
- website analytics data;
- cookie preferences;
- IP address and device/browser information where collected by website systems.

6. Special Category and Sensitive Data

Kent With Ukraine recognises that some personal data is more sensitive and requires additional protection.

This may include:

- health information;
- disability information;
- medical or rehabilitation needs;
- psychological trauma information;
- safeguarding information;
- information about children;
- biometric data where relevant;
- racial or ethnic origin;
- religious or philosophical beliefs;
- political opinions where incidentally collected;
- information about sex life or sexual orientation;
- criminal offence data;
- veteran, military, captivity, injury or conflict-related information.

Where Kent With Ukraine processes special category data, it will identify both a lawful basis under Article 6 UK GDPR and a separate condition under Article 9 UK GDPR. The ICO confirms that special category data requires this additional protection and that an Article 9 condition is required alongside a lawful basis.

Kent With Ukraine will only process sensitive data where it is necessary, proportionate and subject to suitable safeguards.

7. Lawful Bases for Processing Information

Kent With Ukraine will identify and record a lawful basis before processing personal data.

Depending on the activity, the lawful basis may include:

7.1 Consent

Used where an individual has freely given clear permission, for example:

- receiving newsletters;
- appearing in photographs or case studies;
- sharing a personal testimony;
- participating in optional surveys;
- receiving certain communications.

Consent must be specific, informed, recorded and capable of being withdrawn.

7.2 Contract

Used where processing is necessary for a contract or pre-contractual steps, for example:

- engaging contractors;
- arranging volunteer agreements;
- booking services;
- processing expenses or payments.

7.3 Legal Obligation

Used where Kent With Ukraine must comply with the law, for example:

- accounting records;
- employment records;
- tax requirements;
- safeguarding referrals and security vetting where legally required;
- regulatory or funder obligations.

7.4 Vital Interests

Used only where processing is necessary to protect someone's life or immediate physical safety, for example during a medical emergency, evacuation, accident or urgent welfare situation.

7.5 Public Task

Normally this will not apply to Kent With Ukraine unless it is specifically carrying out a function in the public interest under lawful authority.

7.6 Legitimate Interests

Used where Kent With Ukraine has a legitimate organisational interest, provided this does not override the rights and freedoms of the individual. This may include:

- managing volunteers;
- maintaining donor relationships;
- preventing fraud;
- protecting organisational security;
- maintaining project records;
- evaluating programme effectiveness;
- communicating with institutional partners;
- responding to enquiries.

Where legitimate interests is used, Kent With Ukraine will consider and document the balance between its interests and the rights of the individual.

8. Our Data Protection Principles

Kent With Ukraine will apply the following principles to all personal data.

8.1 Lawfulness, Fairness and Transparency

Individuals must be told how their data will be used. Privacy notices, consent forms and project information must be clear and accessible.

8.2 Purpose Limitation

Personal data must only be collected for specified, explicit and legitimate purposes. It must not be reused for unrelated purposes unless there is a lawful basis to do so.

8.3 Data Minimisation

Kent With Ukraine will collect only the personal data required for the relevant activity. Staff and volunteers must avoid collecting excessive, speculative or unnecessary information.

8.4 Accuracy

Reasonable steps must be taken to keep personal data accurate and up to date.

8.5 Storage Limitation

Personal data must not be kept longer than necessary. Retention periods must be documented and followed.

8.6 Security, Integrity and Confidentiality

Personal data must be protected against unauthorised access, accidental loss, destruction, damage, misuse or disclosure.

8.7 Accountability

Kent With Ukraine must be able to demonstrate compliance through policies, records, training, risk assessments, contracts, privacy notices and governance oversight.

9. Collecting and Processing Data in Ukraine

Kent With Ukraine's work in Ukraine may involve humanitarian aid, veterans' support, civic partnerships, monitoring and evaluation, institutional engagement, education links, mobility support, rehabilitation pathways, case studies, delegation visits and partnership projects.

Because this work may involve people affected by war, displacement, injury, trauma, bereavement, disability or military service, Kent With Ukraine will apply enhanced safeguards when collecting or processing data in Ukraine.

9.1 Core Requirements for Ukraine-Based Data Collection

Kent With Ukraine will ensure that:

- data collection has a clear and documented purpose;
- only necessary information is collected;
- participation is voluntary wherever possible;
- individuals understand who is collecting the data and why;
- interpreters or local partners explain consent clearly where needed;
- data is not collected in a coercive or pressurised environment;
- people are not denied aid solely because they refuse optional publicity, photography or testimonial consent;
- safeguarding concerns are escalated through agreed procedures;
- data collection is trauma-informed and conflict-sensitive.

9.2 Beneficiary and Veteran Data

Where Kent With Ukraine collects data from veterans, injured persons, displaced families, children, disabled people or other vulnerable groups, it will:

- explain the purpose of data collection in plain language;
- collect the minimum data necessary;
- avoid intrusive questioning about trauma, military service, captivity, bereavement or injury unless essential;
- avoid collecting medical or psychological information unless needed for the project;
- separate service delivery data from publicity and communications consent;
- anonymise or pseudonymise monitoring data wherever possible;
- restrict access to sensitive information to authorised personnel only;
- avoid publishing names, locations or identifying details that may create safety or security risks.

9.3 Working with Ukrainian Partners

Kent With Ukraine may share data with Ukrainian ministries, regional administrations, municipalities, hospitals, schools, veteran centres, civil society organisations, delivery partners or professional advisers where necessary for project delivery.

Before sharing personal data with a Ukrainian partner, Kent With Ukraine will consider:

- the purpose of the sharing;
- whether the partner needs identifiable data or whether anonymised data is sufficient;
- whether there is a lawful basis for sharing;
- whether a data sharing agreement or processor agreement is required;
- whether the transfer is a restricted international transfer;
- whether the recipient can protect the data appropriately;
- whether special category data is involved;
- whether the data could place individuals at risk if misused, lost or disclosed.

9.4 International Transfers to Ukraine

Where Kent With Ukraine transfers personal data from the UK to Ukraine, or makes UK-held personal data accessible to a separate organisation in Ukraine, it will assess whether this is a restricted international transfer under UK GDPR.

Where required, Kent With Ukraine will ensure that the transfer is covered by one of the following:

- UK adequacy regulations, where applicable;
- appropriate safeguards, such as an International Data Transfer Agreement or approved contractual clauses;
- a valid exception under UK GDPR, where appropriate and documented.

The ICO states that restricted transfers must be covered by adequacy regulations, appropriate safeguards or an exception, and that the organisation initiating the transfer is responsible for compliance with the transfer rules.

9.5 Security in Ukraine

Where data is collected during visits, aid missions, meetings or field activity in Ukraine, Kent With Ukraine will:

- avoid carrying unnecessary paper records;
- keep paper forms secure and transfer them to secure storage as soon as possible;
- use encrypted or password-protected devices where possible;
- avoid storing sensitive data only on personal phones;
- avoid sending beneficiary lists through unsecured messaging apps;
- limit access to data during travel;
- delete temporary copies once uploaded to approved secure systems;
- ensure photographs and videos are stored securely;
- avoid publishing precise locations of vulnerable individuals, veterans, families, shelters, schools, medical facilities or aid routes where this could create a security risk.

9.6 Monitoring, Evaluation and Reporting

Kent With Ukraine may collect data to evidence project delivery, measure impact, report to funders, improve services and inform policy. Where possible, monitoring and evaluation data will be:

- anonymised;
- aggregated;
- pseudonymised;
- limited to what is necessary;
- stored separately from direct identifiers;
- presented in a way that avoids identifying vulnerable individuals or exposing them to harm,

Personal stories, photographs and case studies must not be used for publicity or funder reporting unless the appropriate consent and safeguards are in place.

10. Website, Cookies and Online Data

Kent With Ukraine will ensure that its website complies with data protection and privacy requirements.

10.1 Website Privacy Notice

Kent With Ukraine will maintain a clear and accessible website privacy notice explaining:

- who Kent With Ukraine is;
- what personal data is collected through the website;
- why the data is collected;
- the lawful basis for processing;
- how long data is kept;
- who data may be shared with;
- whether data may be transferred outside the UK;
- how individuals can exercise their rights;
- how to contact Kent With Ukraine about data protection;
- how to complain to the ICO.

The privacy notice should be linked clearly from the website footer and from any form that collects personal data.

10.2 Contact Forms

Where users submit information through website contact forms, Kent With Ukraine will:

- collect only necessary information;
- explain how the information will be used;
- avoid requesting sensitive information unless necessary;
- store submissions securely;
- restrict access to authorised personnel;
- delete enquiries once they are no longer needed.

10.3 Newsletter and Marketing Sign-Ups

Kent With Ukraine will only send newsletters, fundraising updates or marketing-style communications where there is an appropriate lawful basis and, where required, valid consent.

Individuals must be able to unsubscribe easily from electronic communications.

10.4 Donations and Fundraising

Where donations are made through the website, Kent With Ukraine will ensure that:

- payment processing is handled securely;
- payment providers are subject to appropriate contractual safeguards;
- donor information is used only for legitimate fundraising, accounting, Gift Aid, stewardship and reporting purposes;
- restricted donations are recorded accurately;
- donor preferences are respected;
- donor personal data is not sold or shared for unrelated purposes.

10.5 Cookies and Analytics

Kent With Ukraine will use cookies and similar technologies lawfully and transparently. The website will:

- explain what cookies are used and why;
- distinguish between strictly necessary cookies and optional cookies;
- obtain valid consent for non-essential cookies, including analytics, advertising or tracking cookies where required;
- allow users to reject non-essential cookies as easily as accepting them;
- avoid setting non-essential cookies before consent is obtained;
- maintain a cookie notice or cookie policy.

ICO guidance states that consent for cookies must be freely given, specific and informed, and must involve clear positive action; consent cannot be demonstrated merely by placing information in a privacy policy that is hard to find.

10.6 Website Security

Kent With Ukraine will take reasonable steps to secure its website, including:

- using HTTPS;
- maintaining strong administrator passwords;
- limiting administrator access;
- enabling multi-factor authentication where available;
- keeping website software and plugins updated;
- removing unused accounts;
- monitoring suspicious activity;
- ensuring website suppliers provide appropriate data protection safeguards.

11. Photographs, Videos, Case Studies and Testimonies

Kent With Ukraine may use photographs, videos, personal stories and testimonies to demonstrate impact, support fundraising, report to donors and raise awareness.

However, these materials may create risks, especially for children, veterans, displaced people, injured persons, families in Ukraine, aid recipients and people living near conflict-affected areas. Kent With Ukraine will:

- obtain informed consent before using identifiable images or stories;
- explain where the image or story may be used;
- allow individuals to refuse without losing access to support;
- avoid using degrading, exploitative or sensationalist images;
- avoid identifying children without appropriate consent and safeguards;
- avoid publishing sensitive locations;
- remove images where consent is withdrawn, where practicable;
- use anonymised or non-identifying images where appropriate.

Separate consent should be obtained for:

- service delivery;
- monitoring and evaluation;
- publicity;
- social media;
- media use;
- funder reporting.

12. Children's Data

Kent With Ukraine will apply additional care when processing children's data.

Where children are involved in school partnerships, educational projects, aid work, case studies, events, safeguarding matters or family support, Kent With Ukraine will:

- collect only the data necessary;
- obtain appropriate parental, guardian, school or institutional consent where required;
- consider the child's own understanding and wishes;
- avoid publishing full names, precise locations or sensitive details;
- use child-friendly explanations where appropriate;
- ensure photographs and stories are dignified, safe and proportionate;
- comply with safeguarding requirements at all times.

Children's data must never be used in a way that places a child at risk of harm, exploitation, stigma, trafficking, targeting or unwanted identification.

12. Children's Data

Kent With Ukraine will apply additional care when processing children's data.

13. Data Sharing

Kent With Ukraine may share personal data with:

- delivery partners;
- Ukrainian authorities and institutions;
- UK public bodies;
- funders;
- professional advisers;
- payment processors;
- website and IT providers;
- insurers;
- safeguarding authorities;
- law enforcement agencies;
- auditors or evaluators;
- medical or emergency services where necessary.

Personal data will only be shared where there is a lawful basis and where sharing is necessary, proportionate and properly controlled.

Where appropriate, Kent With Ukraine will use:

- data sharing agreements;
- processor agreements;
- confidentiality clauses;
- due diligence checks;
- international transfer safeguards;
- role-based access controls;
- secure and encrypted transfer methods.

14. Data Processors and Suppliers

Where Kent With Ukraine uses third parties to process personal data on its behalf, it will ensure that appropriate contractual terms are in place. This may include:

- website providers;
- email platforms;
- cloud storage providers;
- payment processors;
- CRM systems;
- accountants;
- payroll providers;
- consultants;
- monitoring and evaluation partners;
- translators or interpreters;
- IT support providers.

Contracts with processors should require them to:

- process data only on Kent With Ukraine's instructions;
- keep data secure;
- restrict access to authorised personnel;
- assist with data rights requests;
- report breaches promptly;
- delete or return data at the end of the contract;
- obtain approval before using sub-processors.

15. Security Measures

Kent With Ukraine will apply appropriate technical and organisational security measures, including:

- password protection;
- multi-factor authentication where available;
- encrypted devices where appropriate;
- secure cloud storage;
- restricted access permissions;
- secure deletion;
- locked storage for paper records;
- clear desk practices where appropriate;
- secure disposal of printed material;
- staff and volunteer training;
- data breach reporting procedures;
- regular review of access rights.

Sensitive data should not be stored on personal devices unless authorised and protected.

Personal data must not be shared through informal channels where a secure alternative is available.

16. Data Retention

Kent With Ukraine will keep personal data only for as long as necessary for the purpose for which it was collected.

Retention periods may be extended where required for legal, safeguarding, audit, insurance, funder, regulatory or dispute-resolution purposes.

Data that is no longer needed will be securely deleted, anonymised or destroyed.

17. Data Subject Rights

Individuals have rights under data protection law. These may include:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object;
- rights relating to automated decision-making and profiling.

Kent With Ukraine will respond to rights requests in accordance with legal timescales.

Requests should be sent to the Data Protection Lead [[Click here to e-mail](#)]

Kent With Ukraine will verify identity where appropriate before disclosing personal data.

Some rights may be limited where exemptions apply, for example where disclosure would prejudice safeguarding, legal claims, crime prevention, regulatory obligations, security of our staff and volunteers, UK National Security or the National Security of Ukraine or the rights and freedoms of others.

18. Data Breaches

A personal data breach may include:

- sending personal data to the wrong person;
- losing a laptop, phone, USB drive or paper file;
- unauthorised access to email or cloud storage;
- accidental publication of personal information;
- ransomware, hacking or cyberattack;
- loss of beneficiary lists;
- disclosure of sensitive veteran, child, medical or safeguarding information;
- misuse of donor, volunteer or supporter data.

All suspected or actual data breaches must be reported immediately to the Data Protection Lead. Kent With Ukraine will:

- contain the breach;
- assess what data is involved;
- assess the risk to individuals;
- decide whether the breach is reportable to the ICO;
- decide whether affected individuals must be informed;
- document the breach and response;
- review lessons learned and improve controls.

Where a breach is likely to result in a risk to individuals' rights and freedoms, Kent With Ukraine will report it to the ICO without undue delay and, where required, within 72 hours of becoming aware of it. ICO guidance confirms the 72-hour reporting expectation for notifiable personal data breaches.

19. Training and Awareness

Kent With Ukraine will provide proportionate data protection training to trustees, staff, volunteers and representatives. Training may cover:

- basic GDPR principles;
- handling beneficiary data;
- safeguarding-sensitive data;
- secure use of email and cloud storage;
- photography and consent;
- Ukraine-specific data risks;
- website and supporter data;
- breach reporting;
- data minimisation;
- secure deletion and retention.

Volunteers and staff working with sensitive data, children, veterans, displaced people or Ukrainian partners must receive enhanced guidance appropriate to their role.

20. Records of Processing

Kent With Ukraine will maintain appropriate records of processing activities. These records should include:

- categories of data processed;
- purposes of processing;
- lawful basis;
- categories of individuals;
- categories of recipients;
- retention periods;
- security measures;
- international transfers;
- processors and suppliers;
- special category data conditions where relevant.

21. Data Protection Impact Assessments

Kent With Ukraine will conduct a Data Protection Impact Assessment where processing is likely to create a high risk to individuals. This may include projects involving:

- vulnerable beneficiaries;
- children;
- veterans;
- health, disability or trauma data;
- large-scale monitoring;

- new digital systems;
- cross-border data sharing;
- location-sensitive data in Ukraine;
- new data-sharing arrangements with public authorities or partners;
- sensitive photographs, case studies or testimonies.

A DPIA will consider risks to individuals and identify safeguards before processing begins.

22. Funders, Government and Reporting Requirements

Where Kent With Ukraine receives funding from government, institutional donors or grant-making bodies, it may need to process data for due diligence, monitoring, evaluation, audit, fraud prevention and reporting. Kent With Ukraine will ensure that:

- only necessary personal data is shared with funders;
- reports use anonymised or aggregated data where possible;
- identifiable case studies are used only with appropriate consent;
- safeguarding and beneficiary data is protected;
- grant agreements are reviewed for data protection obligations;
- any onward transfer or publication risk is considered.

23. Complaints

Individuals who have concerns about how Kent With Ukraine handles their personal data should contact the Data Protection Lead in the first instance.

Kent With Ukraine will investigate complaints promptly and fairly.

Individuals also have the right to complain to the Information Commissioner's Office, and can do so by clicking [here](#) or by calling the ICO on: 0303 123 1113

24. Non-Compliance

Failure to comply with this policy may result in:

- retraining;
- restriction of access to data;
- removal from a project or activity;
- disciplinary action;
- termination of volunteering or contractual arrangements;
- referral to regulators, funders, safeguarding authorities or law enforcement where appropriate.

Serious breaches include unauthorised disclosure of sensitive data, misuse of beneficiary information, failure to report a breach, insecure sharing of personal data, unlawful publication of images, or deliberate misuse of organisational systems.

25. Review

This policy will be reviewed at least annually by the Board or delegated governance lead. It will also be reviewed following:

- a serious data breach;
- a safeguarding incident involving personal data;
- a major new project;
- a change in UK data protection law;
- a change in ICO guidance;
- a funder requirement;
- any significant expansion of operations in Ukraine.

Appendix A: Data Protection Rules for KWU People

All Directors, Staff, Advisors and volunteers must follow these rules:

- Do not collect personal data unless you have been authorised to do so.
- Do not collect more information than is necessary.
- Do not store beneficiary lists on personal phones unless authorised.
- Do not send sensitive information through WhatsApp or personal email unless approved and risk assessed.
- Do not publish photographs of children, veterans, injured people or displaced families without consent.
- Do not share aid recipient lists publicly.
- Do not identify vulnerable people's locations online.
- Do not use personal stories for publicity unless consent has been recorded.
- Do not keep paper forms longer than necessary.
- Report any suspected data breach immediately.