Data Protection Policy

Policy · UK · Updated 2026-07-11 · Square brackets are placeholders to replace with your own details.

A data protection policy is the internal rulebook that tells your staff how personal data must be handled inside the organisation — the principles you follow, who is responsible for what, and the day-to-day rules for storing, sharing, and disposing of information. Where a privacy policy speaks to the outside world, this document speaks to your team.

Most data protection failures are not sophisticated attacks. They are an email sent to the wrong recipient, a spreadsheet copied to a personal drive, records kept for no reason anyone can name. A clear internal policy, trained into staff, is the control that prevents them.

This template gives you a complete policy: the data protection principles in practical terms, named responsibilities, staff handling rules, how rights requests and suspected breaches are routed, and the training and review arrangements that keep it live.

Purpose and scope

This policy sets out how [Your company] protects the personal data it holds and the rules everyone must follow when handling it. It applies to all employees, workers, contractors, and volunteers; to all personal data we process, whether about customers, staff, suppliers, or anyone else; and to all formats, digital and paper.

Policy statement

[Your company] is committed to handling personal data lawfully, fairly, and transparently, collecting only what we need, keeping it accurate and secure, and deleting it when it is no longer required. Deliberate or careless breaches of this policy may be dealt with under our disciplinary procedure.

Definitions

- Personal data: any information relating to an identifiable living person — a name, email address, photo, CCTV image, or an ID number.
- Special category data: data about health, racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetics, biometrics, sex life, or sexual orientation. It needs extra protection.
- Processing: anything done with personal data — collecting, storing, reading, sharing, or deleting it.
- Personal data breach: a security failure leading to loss, destruction, alteration, unauthorised disclosure of, or access to personal data.

Responsibilities

- Senior owner ([name/role]): accountable for this policy and for resourcing data protection properly.
-

Data protection lead ([name/role]): first point of contact for questions, rights requests, and breach reports; maintains training and processing records. [If a Data Protection Officer is appointed, name them here.]

- Managers: ensure their teams are trained and that new tools or processes involving personal data are approved before use.
- All staff: follow the handling rules below and report concerns or mistakes immediately.

The data protection principles in practice

- Lawfulness, fairness, and transparency: we identify a lawful basis before processing and tell people what we do through our privacy notices.
- Purpose limitation: data collected for one purpose is not quietly reused for another.
- Data minimisation: we collect what the task needs, not what might someday be useful.
- Accuracy: records are corrected promptly when we learn they are wrong.
- Storage limitation: data is kept for the periods in our retention schedule, then securely disposed of.
- Integrity and confidentiality: data is protected against loss and unauthorised access.
- Accountability: we keep the records — policies, training logs, breach log — that show all of the above.

Day-to-day handling rules for staff

- Access only the personal data your role requires, and never share logins.
- Check the recipient and attachments before sending any personal data; use [BCC/secure share method] for group messages to external contacts.
- Never forward personal data to personal email accounts or copy it to personal devices or drives.
- Lock your screen when away from your desk; keep paper records in [locked storage] and off desks overnight.
- Use only systems approved by [name/role] for personal data — no new apps, spreadsheets, or AI tools holding customer or staff data without approval.
- Handle special category data only where your role is authorised to, and store it in [restricted location/system].

Rights requests and breaches

Anyone can ask for a copy of their data or exercise other rights, in any words, through any channel. Pass any such request to [name/role] the same working day — the one-calendar-month response clock starts when the organisation receives it, not when the right person sees it.

Report any suspected personal data breach to [name/role] immediately, however small it seems. Notifiable breaches must reach the ICO within 72 hours of us becoming aware, so speed matters more than certainty. The data breach response procedure sets out what happens next.

Training, records, and review

Every new starter completes data protection training before handling personal data, with refreshers [frequency]. Training records, the breach log, and processing records are kept in [system/location].

This policy is reviewed [frequency, e.g. annually], after any breach or near miss, and whenever our systems or processing change materially. Owner: [name/role]. Next review due: [date].

How to use this template

1. Name a real data protection lead and a deputy before publishing — a policy with an empty role box routes nothing.
2. Walk the handling rules against how staff actually work; if everyone uses personal phones for rotas, write the rule you can enforce or change the practice first.
3. List the systems that genuinely hold personal data and get them into the approved list.
4. Check the ICO's guidance on whether you must appoint a DPO or keep formal processing records, and record your conclusion.
5. Train the policy into current staff — not just new starters — and keep the sign-off records.
6. Set the review date and owner before you publish.

Official guidance

› ICO — UK GDPR guidance and resources