[Company name]

How to use this document: delete this paragraph before saving, sharing, or circulating it. Every part shown in blue is yours to replace: type your own details over each blue [field] until no blue remains. Then select all (Ctrl+A) and set the font colour to the same dark colour throughout. What is left is your finished document.

Data Protection Policy

How the organisation handles personal data, the rights of data subjects, and what happens if personal data is lost or shared without permission. General wording only, not legal advice. Check it fits your situation and seek professional advice before relying on it; adapt every [bracketed] item to your organisation. Organisation: [Name of the organisation] | Policy owner: [Full name of the policy owner], [Job title of the policy owner] | Data protection lead: [Full name of the person responsible for data protection] | Effective: [Date this policy takes effect] | Review: [Date of the next review] | Version: [Version number]

1. Purpose, scope, law and roles

This policy sets out how [Name of the organisation] handles personal data, meaning information about an identifiable person, such as a name, address, contact details or an identification number. It applies to all personal data held by [Name of the organisation], in any format, and to all staff who handle personal data, including employees, temporary staff, contractors and volunteers. The law that applies to [Name of the organisation] is [Name of the applicable data protection law], and the person responsible for data protection is [Full name of the person responsible for data protection]. Where that law sets a stricter rule than this policy, the law prevails.

[Job title of the senior manager]: has overall responsibility for this policy and for how personal data is handled. **[Full name of the person responsible for data protection]:** advises on this policy, handles requests from data subjects, leads the breach response, and keeps the record of how personal data is used. **Managers:** make sure their team follows this policy and report any problem to the data protection lead. **All staff:** handle personal data only as this policy allows, keep it secure, and report any problem promptly.

2. Principles for handling personal data

Handle personal data in line with these principles: **1.** Collect and use it only for a clear, recorded purpose, and not for a different purpose without a lawful basis under [Name of the applicable data protection law]. **2.** Collect only the data needed for that purpose, and no more. **3.** Keep it accurate and up to date, and correct or delete it promptly where it is wrong. **4.** Keep it only as long as needed, as set out in the Document Retention Schedule, then dispose of it securely. **5.** Keep it secure, using the measures in section 4 and in the Confidentiality Policy. **6.** Be open about how it is used, telling the people the data is about the purpose, how long it will be kept, and who it may be shared with. **7.** Do not transfer it outside [Name of the country or region] unless the law allows it and the transfer has been approved by the data protection lead.

3. Rights and requests

A data subject is a person whose personal data is held by [Name of the organisation], with rights under [Name of the applicable data protection law]: **Access:** ask what personal data is held about them and receive a copy within [Number of days] days. **Correction:** ask for wrong data to be corrected promptly and be told when done. **Deletion:** ask for data to be deleted where the law allows it, checked against the retention schedule, and be told the outcome. **Restriction:** ask for use of data to be limited while a question about it is checked. **Objection:** object to a use of data where the law allows it; the objection is recorded and the use reviewed.

A request may be made in writing to [Email address or postal address for requests] or in person to the data protection lead. Check identity before sharing any personal data, using [Method used to check identity, for example, a form of identification]. Record each request with the date received, what was asked for, and the date answered. If a request is refused in whole or in part, tell the person why and how to complain or ask for a review, as the law requires. No fee is charged unless the law allows a fee for a request that is repeated or excessive, in which case the fee is [Amount of the fee, if any].

4. Breach response, retention, training and review

A personal data breach is any loss, sharing of, or access to personal data without permission, including a lost device, data sent to the wrong person, or unauthorised access to a system. **1.** Report it to the data protection lead as soon as possible and no later than [Number of hours] hour(s) after you become aware of it. Do not hide a breach and do not delete anything that may help to understand what happened. **2.** The data protection lead will record the breach and assess the data and people affected and how serious it is. **3.** Where the breach is likely to cause harm, tell the people affected promptly, in clear language, what has been done and what they can do. **4.** Where the law requires a report to [Name of the regulator or authority], make it within the time the law requires. **5.** Afterwards, record what was learned and what will change, so it does not happen again.

Keep personal data only as long as needed, as set out in the Document Retention Schedule, then dispose of it securely, shredding paper and verifiably deleting electronic records. Do not keep personal data in personal email, on personal devices, or in personal cloud storage unless the data protection lead has approved it in writing. All staff who handle personal data must be trained on this policy when they join [Name of the organisation] and at least [How often training is repeated, for example, once a year] after that; training is arranged by [Job title of the person who arranges training] and attendance recorded by [Job title of the person who records training]. This policy is reviewed at least [How often this policy is reviewed, for example, once a year], and whenever the applicable law changes or the way personal data is handled changes. The review is carried out by the data protection lead and approved by [Job title of the senior manager].

Approved: [Job title of the approver], [Full name of the approver], [Date of approval] | [Job title of the second approver], [Full name of the second approver], [Date of approval]