[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.

Confidentiality Policy

The rules for keeping the organisation's information confidential, how it is classified, and what happens if it is 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] | Effective: [Date this policy takes effect] | Review: [Date of the next review] | Version: [Version number]

1. Purpose and scope

This policy sets out how [Name of the organisation] protects information that is not public: what counts as confidential, how to handle it, and what to do if it is shared or lost. It applies to all staff, including employees, temporary staff, contractors and volunteers, and to anyone else who receives confidential information from [Name of the organisation], in any form, including paper, electronic files, emails, messages and conversation. The duty continues after a person leaves, for information received while they worked here.

2. What counts as confidential

Confidential information is information that is not public and that a reasonable person would understand should be kept private, including personal and financial information, business plans, pricing, supplier and customer lists, and anything marked confidential. It is not confidential if it is already public through no fault of the person who holds it, or if it was received from a person not bound to keep it confidential. Classify all information at the level below, using the higher level when unsure and asking [Job title of the policy owner]: **Public:** published material, may be shared freely. **Internal:** staff-only material, share only with staff who need it. **Confidential:** harmful if shared, share only on a need-to-know basis, store securely, never by personal email or messaging. **Strictly confidential:** serious harm if shared, such as [Example of strictly confidential information], share only with people named by [Job title of the senior manager] and store only in the agreed secure place, recording who has access.

3. Access, handling, sharing and breach reporting

Access: on a need-to-know basis only. Access is approved by [Job title of the person who approves access] and reviewed at least [How often access is reviewed, for example, once a year]. When a person changes role or leaves, remove their access promptly; [Job title of the person who removes access] is responsible. Never share a password, login or access card, and never use another person's login.

Handling and sharing: store it only in systems and places approved by [Name of the organisation], never on personal devices, personal email or personal cloud storage unless [Job title of the senior manager] has approved it in writing. Lock your screen and paper records away when not in use, do not discuss confidential information where you can be overheard, collect printing promptly, and dispose of it under the Document Retention Policy, shredding paper and verifiably deleting electronic records. Share with a third party only where needed for the work of [Name of the organisation], where you have authority, and where the third party has agreed in writing to keep it confidential; check with [Job title of the policy owner] whether a written agreement is needed. Never share it with family or friends or on social media. Where sharing is required by law, by a court or by a regulator, tell [Job title of the senior manager] promptly where lawful and practicable and share only the part required.

A breach includes sharing confidential information without permission, losing a device or document holding it, sending it to the wrong person, or unauthorised access. Report any breach, or suspected breach, to [Job title of the policy owner] as soon as possible and no later than [Number of working days] working day(s) after you become aware of it. Do not hide a breach and do not delete anything that may help to understand what happened. [Job title of the policy owner] will record the breach, assess what information is affected and decide what action is needed, including telling the people affected where required.

4. Consequences, acknowledgement and review

A breach may lead to disciplinary action under the disciplinary process of [Name of the organisation], up to and including dismissal for a serious breach, and to legal action where it causes loss or harm. The action taken depends on the seriousness of the breach, whether it was deliberate or repeated, and whether it was reported promptly. Everyone covered by this policy must read it and sign the Confidentiality Acknowledgement Form, confirming they have read and understood it and agree to follow it. New staff sign at induction; the signed form is kept on their file by [Job title of the person who keeps the signed forms]. [ ] I have read and understood this Confidentiality Policy. Name: _____ Date: _____

This policy is reviewed at least [How often this policy is reviewed, for example, once a year], and whenever the work of [Name of the organisation] changes in a way that affects how information is handled. The review is carried out by [Job title of the policy owner] 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]