

ORCHARD FUNERAL SERVICES LTD

DATA PROTECTION POLICY

Document Owner: Orchard Funeral Services Ltd

Version: 3.0

Effective Date: 01/07/2026

****Review Date:** **01/06/2027

1. Purpose

Orchard Funeral Services Ltd recognises the importance of protecting personal and confidential information.

This policy establishes the standards that all directors, employees, contractors, temporary workers and other authorised persons must follow when handling information on behalf of Orchard Funeral Services.

2. Scope

This policy applies to information held in:

- paper files;
 - computers;
 - mobile phones;
 - tablets;
 - email accounts;
 - cloud systems;
 - databases;
 - funeral-management systems;
 - photographs;
 - audio and video recordings;
 - backup systems;
 - removable media; and
 - any other storage medium.
-

3. Data protection principles

Orchard Funeral Services will seek to ensure that personal information is:

- processed lawfully, fairly and transparently;
- collected for specified purposes;
- adequate, relevant and limited;

- accurate and kept up to date where necessary;
 - retained only for appropriate periods;
 - kept secure; and
 - handled in a manner that allows the company to demonstrate compliance.
-

4. Staff responsibilities

All staff must:

- only access information necessary for their duties;
 - keep passwords confidential;
 - not share client information unnecessarily;
 - not discuss funeral arrangements in public areas;
 - secure paper files when unattended;
 - lock computers when away from their workstation;
 - report suspected data breaches immediately;
 - use company-approved systems where available;
 - dispose of confidential documents securely;
 - verify recipients before sending sensitive information; and
 - follow Orchard Funeral Services procedures.
-

5. Confidentiality

Funeral arrangements are highly personal.

Staff must not disclose information about a client, deceased person, family member or funeral arrangement to anyone who is not authorised to receive it.

Particular care must be taken when:

- speaking on the telephone;
 - dealing with unexpected callers;
 - responding to emails;
 - discussing funerals in shared areas;
 - transporting documents;
 - handling personal effects; and
 - dealing with family disputes.
-

6. Accuracy

Staff should take reasonable steps to ensure information is accurate.

Particular care must be taken with:

- names;
 - dates of birth;
 - dates of death;
 - addresses;
 - family relationships;
 - burial plots;
 - funeral times;
 - crematorium details;
 - cemetery details; and
 - financial information.
-

7. Access control

Access to systems and records should be restricted according to role.

Staff must not use another person's account unless expressly authorised under an appropriate procedure.

Access should be removed when staff leave the business or no longer require access.

8. Paper records

Paper records containing confidential information must:

- be stored securely;
 - not be left unattended in public areas;
 - not be removed from company premises without authorisation where avoidable;
 - be transported securely when necessary; and
 - be destroyed securely when no longer required.
-

9. Electronic records

Electronic information must be protected using appropriate:

- passwords;
- access controls;
- software updates;
- security measures;

- backups; and
- secure storage.

Sensitive information should not be sent to an incorrect recipient.

Before sending an email containing sensitive information, staff should verify the recipient and attachments.

10. Photographs and recordings

Photographs, videos and recordings associated with a funeral must only be taken, stored or used where there is an appropriate lawful basis and, where required, appropriate permission or consent.

Staff must not publish funeral-related photographs or information on personal social-media accounts.

11. Personal devices

Staff must not store confidential client information on personal devices unless expressly authorised by Orchard Funeral Services and appropriate security measures are in place.

12. Data breaches

A suspected breach must be reported immediately to the person responsible for data protection.

Examples include:

- sending an email to the wrong person;
- losing a funeral file;
- losing a company phone;
- unauthorised access;
- accidentally publishing confidential information;
- losing personal effects records;
- sending the wrong family's documents;
- a stolen laptop;
- compromised passwords; or
- unauthorised disclosure of client information.

All suspected incidents must be recorded.

13. Training

Staff should receive appropriate data-protection and confidentiality training.

Training should be refreshed periodically and whenever significant changes are made to procedures.

14. Breach of this policy

Failure to comply with this policy may result in disciplinary action and, where appropriate, legal or regulatory action.

15. Review

This policy will be reviewed periodically and whenever there is a significant change to relevant legislation, guidance, technology or business processes.