Information Technology and Acceptable Use Policy

1. Purpose

Durkin and Sons Ltd relies upon information technology to support the safe, secure and efficient delivery of its operations. This policy sets out the principles for the acceptable use of company information technology systems, equipment and digital services while protecting company information, client data and business operations from misuse, cyber threats and unauthorised access. The company is committed to complying with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and other applicable legal and contractual requirements relating to information security.

2. Scope

This policy applies to all employees, directors, agency workers, subcontractors, consultants and any other authorised users of Durkin and Sons Ltd information technology systems.
It applies to all company-owned or authorised devices including, but not limited to:

- Desktop computers
- Laptop computers
- Tablets
- Mobile telephones and smartphones
- Servers and network infrastructure
- Cloud-based applications
- Email systems
- Internet services
- Company software
- Portable storage devices

The requirements of this policy also apply where personal devices are authorised for business use.

3. Acceptable Use

Company IT systems are provided primarily for business purposes.
Limited personal use is permitted provided it:

- Does not interfere with work duties.
- Does not affect system performance or security.
- Does not incur unreasonable cost.
- Does not breach company policies or legal requirements.
- Does not damage the reputation of Durkin and Sons Ltd.

Users are responsible for using company systems professionally and responsibly at all times.

4. Information Security

All users are responsible for protecting company information.
Users must:

- Keep usernames and passwords secure.
- Never share login credentials.
- Use multi-factor authentication where provided.
- Lock devices when unattended.
- Store company information only within approved company systems.
- Report suspected cyber security incidents immediately.
- Ensure confidential information is protected against unauthorised access.

Confidential company, client and employee information must only be accessed where there is a legitimate business need.

5. Cyber Security

To reduce cyber security risks, users must not:

- Install unauthorised software.
- Disable security software or system updates.
- Attempt to bypass security controls.
- Open suspicious emails or attachments.
- Click unknown links without appropriate verification.
- Download files from untrusted websites.
- Connect unauthorised devices to the company network.
- Share company information using unauthorised applications or cloud storage.

Users should remain alert to phishing attempts and other cyber security threats and report any suspected incidents immediately.

6. Email, Internet and Communications

Electronic communications must be professional, respectful and appropriate.

Users must not use company systems to:

- Access unlawful or inappropriate material.
- Send offensive, discriminatory or abusive communications.
- Harass, intimidate or bully others.
- Conduct personal commercial activities.
- Distribute malicious software.
- Breach copyright or intellectual property rights.
- Represent personal opinions as those of Durkin and Sons Ltd without authorisation.

All electronic communications should reflect the professional standards expected of the company.

7. Company Equipment

Users are responsible for taking reasonable care of company equipment issued to them.

Equipment should be protected from theft, loss and damage and should not be loaned or transferred to another individual without authorisation.

Any loss, theft, damage or suspected compromise of equipment or information must be reported immediately.

8. Monitoring

Durkin and Sons Ltd reserves the right to monitor the use of company IT systems, email, internet access and electronic communications where permitted by law.

Monitoring may be undertaken to:

- Protect company information.
- Maintain cyber security.
- Investigate suspected misconduct.
- Ensure compliance with legal obligations.
- Support business continuity.

Monitoring will be carried out proportionately and in accordance with applicable legislation.

9. Responsibilities

All users are responsible for complying with this policy and protecting company information.
Managers are responsible for ensuring employees understand the requirements of this policy.
Those responsible for managing the company's IT systems will implement appropriate technical controls to protect information, maintain system availability and support users.

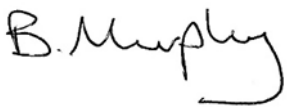
10. Breaches

Failure to comply with this policy may result in disciplinary action and, where appropriate, civil or criminal proceedings.
Any suspected cyber security incident, loss of information or breach of this policy must be reported immediately.

11. Monitoring and Review

This policy will be reviewed annually or sooner where changes in legislation, technology or business operations require.

Signed



Ben Murphy, Managing Director	Date 1st July 2026	Review by date 30th June 2027