

Information Technology Policy

Introduction

The company ensures it meets the requirements of the Data Protection Act 2018 and the General Data Protection Regulations 2018 as well as other relevant legal requirements. Individuals must follow the contents in this policy to also meet these requirements.

1 The use of IT and the Internet

The company encourages its employees to expand their use of IT and electronic communications. They are vital tools to help us improve our efficiency, levels of service and effective communications.

However, there have been occasional incidents of abuse of these services and there are pitfalls that we all need to be aware of. This policy is both a reminder of what is good practice and a warning that you should regulate your own use of these services.

“IT” includes, but is not limited to:

- All company provided computers i.e. desktop, laptop, terminal, tablet or smart phone.
- All company provided communication equipment including mobile and fixed-line phones, fax, data enabled SIM card and satellite systems.
- All internet and fax services provided by the company, either via an on-site connection or via remote connections.
- All company provided software.

2 Care of IT Equipment & Services

You are responsible for the condition of equipment provided and could be held liable for any costs incurred by improper use. When using, storing or transporting any IT equipment it is important that you adhere to the following guidelines:

- IT hardware is fragile and electronic, it can be easily damaged by exposure to liquids and any extremes of temperature. Impacts from any height can cause serious damage too. Under no circumstances shall an employee attempt to undertake maintenance on any piece of electronic IT equipment without express instruction from the IT Administrator.
- IT software is provided according to the business needs of the user. Under no circumstances should any additional software be installed without permission from the IT Administrator. In addition, no person should ever attempt to alter the developed code or functional configuration of any software pre-installed on an IT device.
- Data services allowing access to the internet and the company’s Wide-Area-Network shall be provided by the IT Administrator according to business capacity need. Care should be taken to ensure that consumption of data does not breach pre-agreed contract levels.

3 Security

Correspondence via email is not guaranteed to be private within or outside the company and may be accessed by our designated IT Administrator. All computers will have up-to-date anti-virus software installed at the time they are issued. The anti-virus system’s database will be updated on a regular basis. In no circumstances should you delete or disable the anti-virus software.

4 Authority

Corporate email accounts, Internet and Web pages must only be used for communications sanctioned by the company.

5 Privacy

Use of email and Internet will be monitored for security, network management reasons and for irregular activity. All incoming and outgoing data will be screened via a secure firewall for computer viruses and access to certain external Internet sites will be disabled. Provision of corporate email and Internet access to users must first be approved by individual line managers.

6 Personal Use

Durkin and Sons permits personal use of email, internet and other services as a privilege. Such usage may not be carried out in company time. The primary purpose of these services is to provide business benefit. Abuse may result in the withdrawal of the privilege and disciplinary action.

7 Appropriate Style and content

Email is a forum for measured communication and must not be used in any threatening or abusive way. Exercise the same care in email as you would in a letter. Email should not be a substitute for other more appropriate forms of communication, i.e. face to face or telephone.

8 Conditions of use - Proper use of Electronic Services

Employees are reminded that they should refrain from the following when using electronic services:

- Visiting internet sites that contain obscene or other objectionable materials.
- Making or posting remarks, proposals, or materials that are indecent, abusive, sexist, racist, pornographic, drug related, promote terrorism or are defamatory, or which are intended to annoy, harass or intimidate another person.
- Soliciting emails that are unrelated to business activities. This includes subscribing to employment lists or recreational services.
- Soliciting non-company business for personal gain or profit.
- Using the Internet or email for any illegal purpose.
- Represent personal opinions as those of the company.
- Broadcasting inappropriate material or trivial messages to other network users via company email.

9 Safeguard Company Computer Network Security

The Computer Misuse Act 1990 means that unless you are authorised to do so it is an offence to:

- Access, change, load or destroy any of the company's data.
- Run or modify the company's computer software.
- Install software on any of the company's computers without permission from the IT Administrator.

All IT equipment, including hardware and software is acquired and installed by the IT Administrator. This ensures an efficient, integrated approach, and a more robust computer environment.

10 Users are not permitted to:

- Download any software or electronic files without implementing virus protection measures that have been approved by the IT Administrator. A computer virus in any programme is designed to cause damage to data, or to prevent a computer from operating properly. The most common form of virus infection comes from media storage and unauthorised software. All media storage from outside the company must be virus checked. Games and other unauthorised software are not permitted on any company PC.
- Intentionally interfere with the normal operation of the network, including the propagation of computer viruses and sustained high volume network traffic, which affects others' use of the computer network.
- Transmit information concerning Company computer network configuration or users.
- Perform any other inappropriate uses identified by the IT Administrator.
- Examine, change or use another person's files, output or user name for which they have not been given explicit authorisation.
- Download any software, unauthorised device drivers, games or media/gambling portals.
- Use another person's login details.

Any breach of the above may result in disciplinary action.

Keeping Company Information Confidential

11 Users are not permitted to:

Reveal or publicise confidential or proprietary information which includes, but is not limited to the following:

- Personal information of Employees, Clients or Customers
- Financial information.
- New business and product ideas.
- Business strategies and plans.
- Databases and the information contained on them e.g. customer lists, technical product information, product prices.
- Computer software source codes.
- IT Network access codes.

12 Users are not permitted to:

Upload, download or otherwise transmit commercial software or any copyrighted materials belonging to others without their permission as this may infringe copyright. If in doubt, contact the IT Administrator.

13 Take care over Contractual Matters

Email messages can create an impression of intimacy and therefore there is a danger of communications between parties forming contractual obligations without a party intending that they do so.

An email can be considered a legal document in law; hence all communications of a contractual nature must follow normal contract and procurement procedures.

All emails are electronically stored on your "Outlook" file on the company server with a copy automatically filed on users' computer.

At various times during your employment with the company, you may use a portable IT device. Typically these devices will be laptops, but tablet computers and smart phones have similar functionality. These computers,

along with related equipment and software are subject to all of the company's policies and guidelines governing non-portable computers and software (see two paragraphs in software section above). However, use of a portable device creates additional problems especially in respect of potential breaches of confidentiality.

When using a portable device:

- You are responsible for all equipment and software until you return it. The device must be kept secure at all times.
- You are the only person authorised to use the equipment and software issued to you.
- You must not load or install files from any sources without the IT Administrator inspecting such files for viruses.
- All data kept on the device must be backed up regularly in order to protect data against theft or mechanical failure or corruption, NB backup is the user's responsibility and advice should be sought from the IT Administrator if required.
- You must password protect confidential data on portable storage media or on the hard drive to protect against theft.
- If you discover any mechanical, electronic, or software defects or malfunctions, you should immediately bring such defects or malfunctions to the attention of the IT Administrator.
- Should your employment at Durkin and Sons come to an end or, upon the request of the company, at any time and for any reason, you will immediately return your mobile phone and accessories to the IT Administrator.
- If you are using your own device to connect with the Durkin and Sons network, or to transfer data between it and any of the company's computers, you must ensure that you have obtained prior consent from the IT Administrator, comply with its instructions and ensure that any data downloaded or uploaded is free from viruses.

Note on Court Disclosure

Email messages, however confidential or damaging, may have to be disclosed in court proceedings or in investigations by regulatory bodies if relevant to the issues.

Good Practice Guidelines

14 Backup Data

All data on network drives is backed up every night. Documents and data must therefore be stored on the Company's Document Management System or network drive; (guidelines will be issued from time to time on the company's procedures for the storage and filing of information). If you must store files on a local hard drive, then it is your responsibility to back up this information on to the network drive or media storage.

15 Protect your Password(s)

You will be issued with a unique username and password in order for you to access the computing resources authorised to you. This enables us to monitor the security of the information contained within the corporate systems. Do not share usernames. Change your password(s) regularly. Do not tell anyone your password and log off your PC when away from your desk. Switch off your PC at the end of the day.

The unauthorised use of another username and/or password to gain access is considered an act of gross misconduct.

16 Remember the Risk of Theft

All Company equipment is security marked. Take extra care with portable PC equipment to safeguard against damage and theft. Laptop PCs are an attractive target for a thief. Do not leave portable PC equipment on view in an unattended car or in an unoccupied or unlocked building, as this may invalidate the insurance cover. Wherever possible portable PC equipment should be locked away overnight.

17 Sanctions

Breaches of this IT Policy shall be taken very seriously by Durkin and Sons. Employees found to be in breach may be subject to disciplinary action as set out in the Company's Disciplinary Procedure, which could include summary dismissal.

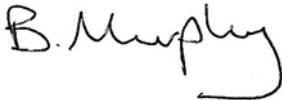
Minor breaches of the policy may lead to privileges being withdrawn. Continued minor breaches may be handled in accordance with the Company's Disciplinary Procedure.

IMPORTANT NOTE:

Durkin and Sons reserves the right to intercept and monitor telephone calls, emails and faxes either made by you or addressed to you via facilities provided by the company for the purpose of evidencing commercial transactions, detecting criminal offences and detecting unauthorised use.

This statement will be displayed on all notice boards and will be reviewed annually

Signed



Ben Murphy, Managing Director

Date
1st July 2025

Review by date
30th June 2026