	NAME	<u>Email and Internet Policy</u>
	REF	PS-003-WB
	ISSUE DATE	13/02/2025
	REVISION NO	1
	PREPARE BY:	SM
	APPROVE	RM

Policy Statement

The company views the Internet and Email as essential tools for employees. However, the use of those tools can expose the company to technical, commercial and legal risks if they are not used sensibly. The widespread availability of social media means it is important to understand how to use it effectively and sensibly, both in the workplace and during personal use.

This policy aims to ensure that the company is not exposed to legal and governance risks through the use of email, internet or social media and that its reputation is not adversely affected.

This policy also aims to ensure that employees are protected while using social media, email and the Internet and feel empowered to contribute to collaborative online activity when it supports their role within the company.

The policy applies to all workers and employees of the company, from management to temporary workers, and to all users of email and Internet.


Purpose

The purpose of this policy is to define acceptable email and internet use within working time.

Email and internet use for work purposes

Many employees will be required to use email and the internet regularly for work purposes. This is clearly acceptable when it is fulfilling work duties. However, it is important that employees are mindful of the need to use email and the internet appropriately. In particular:

- No obscene or offensive language should ever be used in emails;
- Emails of a discriminatory, derogatory or defamatory nature should never be sent;
- Email should never be used as a form of communication which could cause harassment or be abusive to someone;
- Emails should not be copied to people inappropriately;
- If an employee receives an offensive email this should be reported to his/her line manager. It should not be passed on to other employees;
- Internet sites should only be accessed if they are appropriate to the work that is being carried out;
- Email content and language should remain consistent with the company's best practice;
- Email messages should be concise and appropriate;
- Emails containing confidential information should be treated appropriately as such and all necessary steps taken to protect confidentiality. The company will be liable to infringing copyright or any defamatory information that is circulated either within the company or to external users of the system;

	NAME	<u>Email and Internet Policy</u>
	REF	PS-003-WB
	ISSUE DATE	13/02/2025
	REVISION NO	1
	PREPARE BY:	SM
	APPROVE	RM

- Employees should be conscious of the fact that offers or contracts transmitted by email are as legally binding on the company as those sent on paper.

If you do use email inappropriately including some of the examples above, you may be liable to disciplinary action up to and including summary dismissal.

During an employee's absence (for holiday, sickness or any other reason) the company reserves the right to access the employee's email account. This is necessary to ensure that any issues are addressed in a timely manner.

Email use for personal purposes

Employees should not send personal emails during work time, unless the email relates to an urgent matter that needs addressing immediately.

During official breaks (e.g. lunchtime) employees may access their personal email accounts. However, in responding to emails the code of conduct relating to work emails (as explained above) applies.

Employees may only use their work email address for work purposes. They are not to send personal emails using this address.

Internet use for personal purposes

Employees should not use the internet for personal purposes during work time.

During official breaks (e.g. lunchtime) employees may access the internet for personal use. However, only appropriate sites may be accessed (see below).

Internet sites that cannot be accessed

Under no circumstances can any pornographic internet site be accessed during working hours or at any time using a computer belonging to the company.


Any other internet sites that contain offensive, obscene or otherwise unacceptable material should not be accessed using a computer belonging to the company, or during working hours.

Downloading of material

Viruses and similar problems can bring an entire computer network to a standstill. It is important, therefore, that all employees are aware of the need to act responsibly and minimise the risk of this occurring. To help protect the company's network, employees should not download any documents on to a computer belonging to the company without being confident that it comes from a legitimate source.

No software can be downloaded onto a computer belonging to the company without the express agreement of management.

You should not under any circumstances use the company's email system or internet to access, display, circulate or transmit any material with a sexual,

	NAME	<u>Email and Internet Policy</u>
	REF	PS-003-WB
	ISSUE DATE	13/02/2025
	REVISION NO	1
	PREPARE BY:	SM
	APPROVE	RM

violent, graphic or discriminatory content. This may constitute a criminal offence and both you and the company could be liable.

The display on screen of material with a sexual content and/or its transmission to another may also amount to sexual harassment – for which you could be liable.

On-line blogs

Employees should not contribute to on-line blogs during working hours, or using a computer belonging to the company.

Employees should not contribute to any blog which criticises the company, or otherwise brings the company into disrepute, at any time (this includes during personal time). If the employee is dissatisfied with some aspect of their employment this should be addressed using the company's grievance procedure.

Using a blog to criticise or damage the reputation of the company may result in disciplinary action.

Passwords

Access to the company's computers should be password protected. Employees are required to use their passwords, and not put in place any process which bypasses the requirement for a password. Passwords should not be stored by the computer.

Employees should ensure that their line manager has a record of their most recent password. This is important to allow their email account to be accessed, if required, during their absence.

Passwords should not be disclosed to any other person.


Protection of Personal Data

The company is required to comply with legislation concerning the protection of personal data. Failure by the company to adhere to that legislation could expose the company to civil liability and to enforcement action by the data protection authorities.

The obligations of the company are complex but you can help ensure compliance by adhering to the following rules:

- Do not disclose any information about a person in an email or on the Internet, which you would object to being disclosed about yourself.
- Be particularly careful when dealing with information concerning a person's gender, civil status, family status, age, disability, race/ethnicity, sexual orientation, religious belief or political opinion, health or financial matters.
- Do not send any personal data outside the European Union.

Copyright

	NAME	<u>Email and Internet Policy</u>
	REF	PS-003-WB
	ISSUE DATE	13/02/2025
	REVISION NO	1
	PREPARE BY:	SM
	APPROVE	RM

Copyright rules do apply to articles on the internet. Hence, care should be taken when using internet information. If there is any doubt whether material can be used then a member of management should be contacted for specific advice.

Defamation

You should not send or circulate any materials on the internet or by email that contain negative remarks about other persons or company s unless you are very sure that what you are saying is not defamatory and is factually correct. If in doubt, do not send.

Company's website

No employee may add any information to the company's website without express consent of the manager responsible for the website.

Monitoring

Monitoring of an employee's email and/or internet use will be conducted in accordance with an impact assessment that the company has carried out to ensure that monitoring is necessary and proportionate. Monitoring is in the company 's legitimate interests and is to ensure that this policy on email and internet use is being complied with.


Monitoring will normally be conducted by the company 's security team. The information obtained through monitoring may be shared internally, including with members of the HR team, an employee's line manager, managers in the business area in which the employee works and IT staff if access to the data is necessary for performance of their roles. However, information would normally be shared in this way only if the company has reasonable grounds to believe that there has been a breach of the rules set out in this policy. The information gathered through monitoring will be retained only long enough for any breach of this policy to come to light and for any investigation to be conducted.

Information obtained through monitoring will not be disclosed to third parties (unless the company is under a duty to report matters to a regulatory authority or to a law enforcement agency).

Workers have a number of rights in relation to their data, including the right to make a subject access request and the right to have data rectified or erased in some circumstances. You can find further details of these rights and how to exercise them in the company's data protection policy. If workers believe that the company has not complied with their data protection rights, they can complain to the Information Commissioner.

Action to be taken in the case of inappropriate use

If an employee is found to have used email or the internet in an inappropriate manner disciplinary action may be taken. This could include summary dismissal, depending on the nature and severity of the offence.

	NAME	<u>Email and Internet Policy</u>
	REF	PS-003-WB
	ISSUE DATE	13/02/2025
	REVISION NO	1
	PREPARE BY:	SM
	APPROVE	RM

Bullying and harassment

If an employee feels that they are being harassed or have been harassed or bullied or are offended by material received from a colleague, the employee should immediately inform their line manager of the situation.

Protecting Information and IT Resources

Key takeaways:

Protecting our information is vital to the company's ability to carry out our mission. The company's IT systems do a great job keeping us safe but we cannot rely on these systems alone. Always remember that you play a crucial role in helping to protect the company's information.

When using IT resources for company purposes:

- Ensure this is professional, in compliance with the company's policy and applicable laws.
- Do not engage in offensive or inappropriate behaviour that could reflect poorly on the company.

Personal use of the company's IT Resources is to be kept to a minimum, is not to have an impact on your work, and is not to breach the company's policy.

Using passwords:

- Always use strong passwords that contain a variety of letters, numbers and symbols and are not easily guessable.
- Never use the same password for personal devices and for access to the company's systems.

Storing data:

- Only store the company's information in systems or on Cloud services that are managed by the company's IT or by the management-approved Third Parties.

Protecting Information:

- Never leave the company's devices open and unattended in public places and be aware of your surroundings at all times.


Disposing of data - Do:

- Always follow appropriate procedures for disposal of the company's information, management requires the most rigorous disposal procedures.

Avoiding malware - Do:

- Use extreme caution when clicking on links or downloading attachments- they may be phishing attempts or other attempts to acquire confidential company data.
- Only use approved software for company purposes.

Personal devices - Do:

	NAME	<u>Email and Internet Policy</u>
	REF	PS-003-WB
	ISSUE DATE	13/02/2025
	REVISION NO	1
	PREPARE BY:	SM
	APPROVE	RM

- Only use approved applications on personal devices for company purposes.
- Remove the company's information from the personal device before recycling or disposal.

Using email/ social media - Do:

- Never forward or upload Confidential Information to public email accounts or to a non-company owned or approved website/ application.
- Always use secure email or approved encryption technology when transferring content that contains confidential information.
- Be cautious when clicking on links or downloading attachments.