COMMUNICATION POLICY

NWH Group Limited
Reviewed- January 2026

Policy Statement

The purpose of this Acceptable Use Policy is to allow employees to exploit the business benefits of services such as telephone, mobile devices, fax, Internet or email in a secure and legally correct manner.

The objectives of this policy are:

- To mitigate against legal liability by setting boundaries for appropriate employee conduct when using electronic communications facilities.
- To safeguard electronic communications facilities from abuse, damage or disruption.
- To ensure that employees understand that the electronic communications facilities provided to them are primarily for business use.

Facilities such as telephone, mobile devices, fax, Internet and email (referred to throughout this document as 'Electronic Communications') are useful business tools as they represent a quick, cost effective and easy way to communicate vital business information to partners, customers and suppliers.

These characteristics, though advantageous, introduce a variety of risks into our environment.
Some of these risks are:

- Unauthorised access to vital NWH Group or personal information transferred via fax or email or published on the NWH Group web servers.
- Potential loss or corruption of business information or denial of service through the unintentional introduction of malicious code (such as viruses, worms or trojans) via email or Internet services.
- Loss of productivity and spiralling costs through the excessive use of telephone, email and Internet resources for non-business purposes.
- Potential contractual liabilities by unintentionally committing The NWH Group to obligations that have not been authorised (e.g. software license obligations when downloading trial software; email, voice or fax confirmation of a successful job interview that may be interpreted as a job offer etc.).
- Potential exposure to legal liability or serious reputational damage through the distribution of offensive and/or defamatory material attributed to The NWH Group e.g. through its domain name included in the email address of the sender.

COMMUNICATION POLICY

This policy may be amended at any time.

2. Policy Requirements

2.1 Access to IT equipment and systems, identification & authentication

Information Technology department
The ICT Department is responsible for registering users to all information systems at The NWH Group and for providing user access to the system, as approved initially by the HR department and then by the appropriate line manager for additional access requests. External user access is the responsibility of the part of the Business responsible for that resource.

User identification and authentication
To ensure that individuals remain accountable for their actions, all users with access to any electronic communications facilities must be uniquely identified and authenticated. Users will be issued with a user identity. The IT Service Desk, or system administrator for the application, will issue an initial password to be used to access the system. This password should be changed on first login by the user and subsequently when prompted by the system.

Impersonation
To ensure that unscrupulous individuals do not abuse our Electronic Communications facilities by claiming to be someone that they are not, and therefore exceeding their authority, misrepresenting, obscuring, suppressing, or replacing a user's identity (pretending to be someone else) on an electronic communications system is strictly forbidden.
If it is anticipated that someone may need access to an individual's confidential files, in their absence, arrangements should be made for the files to be copied to where that person can access them, or ask ICT to grant temporary access to the relevant folder(s).

2.2 Authorisation & access control

User access authorisation
To maintain effective control over access to our Electronic Communications Services, all users wishing to obtain access to The NWH Group Electronic Communications facilities must obtain formal approval from their line management, before such access is granted (see New User Account Application form).

COMMUNICATION POLICY

Personal use

Our Electronic Communications facilities are provided by The NWH Group for employees to conduct its business. Therefore, the use of these facilities for purposes constituting clear conflict of The NWH Group interests (e.g. to conduct a private business) is prohibited.
Users are expected to exercise common sense in using the facilities. Users are permitted brief personal use (subject to the provisions the Unacceptable Use section) so long as the user does not interfere with, or have a detrimental effect on the user's work performance, or does not pre-empt any business activity.
The NWH Group will monitor use of the internet (see Section 4.6 – Monitoring of Email and Internet Usage)

Unacceptable Use

In order to protect The NWH Group from any liability due to the misuse and abuse of our Electronic Communications facilities, users may not:

- View, store or distribute any material that is sexually explicit, pornographic, racist, sexist, or derogatory of race, origin, sex, sexual orientation, age, disability, religion or political beliefs.
- View, store or send messages intended to harass, intimidate, threaten, embarrass, humiliate or degrade another co-worker or that contain defamatory references.
- Send or forward chain letters.
- Download, install, store or distribute pirated software or data, entertainment software, music or games.
- Propagate viruses, worms, Trojan horse or trap door program codes.
- Copy, destroy, delete, distort, remove, conceal, modify or encrypt messages or files or other data on any NWH Group computer, network or other communication system without the permission of an authorised individual.
- Attempt to access or access another employee's computer, computer account, email or voice mail messages, files or other data without their consent or the consent of an authorised individual.
- Violate or attempt to violate any other applicable laws, prescriptions or provisions.

Third party users

In order to manage the exposure that our organisation may face (e.g. legal liabilities, public embarrassment etc.) as a consequence of improper use of our Electronic Communications facilities by third parties, external parties such as visitors, contractors, consultants or partners, must read and agree to abide by the provisions of this and related policies, before access to our Electronic Communications facilities is authorised.

2.3 Secure Information Exchange

No default protection

Employees are reminded that The NWH Group's electronic communications facilities (whether email, Internet, mobile device, voice or fax) are not automatically protected against disclosure to unauthorised individuals.

2.4 Information Integrity & recoverability

Receiving email

The receipt, failure to detect or the introduction of a virus embedded in an email message can not only damage the recipient's computer and data but can also spread throughout The NWH Group network, wreaking havoc. Therefore, all email content must be scanned for viruses or other malicious code before it is opened. Users should take care when receiving emails with file attachments, even if that email appears to come from a known source.

Junk email (Spam)

Spam (the electronic equivalent of junk mail), may cause The NWH Group's email systems to overload and affect the availability of the service. Therefore, users are not permitted to use The NWH Group email facilities to send advertisements of a personal nature. Any junk email received must be treated with caution (preferably deleted) and not responded to.

Downloading program software, files or information from the Internet

Because the Internet is generally considered an unreliable source of information, the risks associated with downloading large and/or virus infected files and programs as well as the potential legal liabilities associated with the use of unlicensed software downloaded from the Internet:

- Users must exercise caution when downloading files or information from the Internet and should not place undue reliance on its correctness.
- All files or information downloaded from the Internet must be scanned for viruses.
- Users are not permitted to load software onto The NWH Group's equipment.

2.5 Non-Repudiation

User Responsibility

Because the safe use of our electronic communications facilities is dependent on the discipline of individual users, with respect to keeping their personal passwords, tokens or PINs safe and on the termination of open sessions and logging out of the electronic

communications facilities when any such systems are left unattended, all users are reminded that they shall be held responsible for any illegal activities that may take place as a consequence of their failure to exercise this discipline.

2.6 Monitoring of Email and Internet Usage

Expectations of Privacy

Whilst the NWH Group respects the individual's right to privacy as that right is guaranteed under The Human Rights Act 1998, in the context of electronic communications facilities, which are provided for The NWH Group's operational needs, certain restrictions are unavoidable.

The NWH Group will monitor the general levels of usage of email and the internet, including specific web sites visited on the internet. Software will be used to aid this process, which will be searching for specific categories, words, sentences or images. Access to predetermined sites or categories will be blocked and access to such sites will only be available following consultation with ICT.

Employees are expected to exercise common sense in their internet usage. Managers can request information from the ICT Manager about the specific levels of usage, including web sites visited, for their team. However, managers must show clear justification to support their request for this information.

Employees have the general right, under the Data Protection Act, to receive, on written request, a copy of any information, including information held electronically on systems owed by The NWH Group. There are a few exceptions to this such as data held for crime prevention/detection purposes, but most individuals will be able to have a copy of the data held on them. Full details of how employees can obtain information are set out in the Data Protection Act Policy & Guidance.

2.7 Customer & Third-Party Communication

NWH encourage and welcome feedback and open communication from our employees, customers, suppliers, the general public and stakeholders. We are available to all parties via telephone, mail, email and online chat via our website www.nwhgroup.co.uk

COMMUNICATION POLICY

Our Social Media Policy outlines company and employee expectations in terms of communication across all our used social media platforms as well as the controls and safeguards we have in place. Our staff communication channels such as our monthly staff newsletter and internal Facebook page continuously reiterate expected conduct in this area.

All customer interaction is confidential and is treated with the same respect and terms as described under the rest of our GDPR Policy.

All communication from The NWH Group is branded and secure and our company values and culture continuously reiterate our tone of voice.

Disciplinary Process

The NWH Group reserves the right to audit compliance with the policy from time to time. Any disciplinary action, arising from breach of this policy, shall be taken in accordance with The NWH Group's Rules and Disciplinary Code as amended from time to time. Disciplinary action may lead to dismissal.

Policies & Procedures

4. Deviations from Policy

Unless specifically approved, any deviation from this policy is strictly prohibited. Any deviation to or noncompliance with this policy shall be reported to the ICT Manager & Compliance Director.

Signed: Date: 15/01/2025

Gavin Money

Managing Director