



ICT Security Policy

Northwards regards the security of data and the integrity of information technology as most important. Our policy is to take all measures necessary to ensure that information held in our computer systems is secure and all ICT resources are fully protected against disruption. In order to achieve our aims the following guidelines have been put in place and you are required to comply with them.

Breach of the guidelines may result in disciplinary proceedings and could give rise to criminal and/or civil liability. Fraudulent or other misuse of our systems or other serious breaches of the guidelines could, in certain circumstances, amount to gross misconduct.

Any member of staff who suspects that a fellow employee (of whatever seniority) is abusing their access to our computer systems may speak in confidence to the Head of Human Resources.

All breaches of computer security must be referred to the ICT Manager.

Access and Passwords

Employees' network user id and password(s) are their means of gaining access to the computer network and the ICT resources held with it. As an Employee, they are responsible for the security of their password(s). They must not disclose their password(s) to any one else or allow anyone to use their user id on their behalf, unless asked to do so by ICT staff in order to assist with a problem. Once the problem has been resolved they should immediately change their password.

All passwords should be changed on a regular basis (at least every 90 days and or as required by a specific application) and employees should change their password(s) immediately if they suspect it has become known to anyone else. Network passwords have to be a minimum of 8 characters and employees have to change this every 60 days.

All Employees are permitted access to those parts of our computer system, which they need to enter in order to carry out their normal duties. Access to

other areas is restricted to authorised personnel only. Managers will decide levels of access. There is a formal procedure for requesting access or changing users access rights. All such work is done by trained staff in the ICT Section. Attempting to access systems which employees are not authorised to do, is forbidden whether they do damage or not and may result in the disciplinary procedure being invoked.

Use of the Internet and e-mail

The use of Internet and e-mail is governed by the Internet and EMail Access Policy which forms part of employment contracts.

Disks/CD's etc from outside sources

All CDs, DVDs, floppy disks and USB memory sticks are automatically checked for viruses when attached to Northwards PCs. If employees have any worries about CDs etc they have received they should contact the ICT section to discuss.

Unauthorised use of software

All software must be formally authorised, licensed and installed by the ICT Team. The ICT Team Section maintain an asset register of all software licensed by Northwards. All software CDs/DVDs are securely stored by the ICT Section.

Software that has not been authorised, by the ICT Section, must not be installed on our equipment.

Software licensed to Northwards must not be copied or installed on home computers without authorisation.

Confidentiality

All information relating to our business activities is confidential. Employees are expected to treat electronic information with the same care as they would confidential paper-based information. Keep all such information secure, use it only for the purpose intended and do not disclose the same to any unauthorised third party (which may sometimes include other employees).

Employees should not leave their desk for any prolonged period of time without locking their screen.

The safekeeping of disks/CD's etc sent from external sources is the

responsibility of the person to whom the disk was sent. Disks/CD's etc generated internally must be kept in a secure place.

Use of mobile IT equipment

Employees are not permitted to synchronise or download e-mail, calendar entries, files etc to their own Personal Digital Assistant (PDA), mobile phone

Or any other personally owned device either remotely or by direct connection to your office PC or network. However, they are permitted to synchronise or transfer contact details, emails and data onto Northwards supplied mobile devices, subject to their ability to keep such information safe and secure at all times.

Personally owned equipment must not be connected remotely to our network unless this has been authorised by the ICT Section.

The loss of Northwards' equipment or personally owned equipment containing confidential information should be reported to the Manager as soon as is reasonably practicable.

Northwards' equipment must not be altered by employees from its original specification.

Disposal of ICT Equipment

Northwards dispose of all equipment in line with the EU WEEE regulations. Where computers are donated for reuse then all data and software (except the OS) are removed.