Staff IT Acceptable Usage Policy

Contents

1. Scope

This policy applies to all staff users of all Information Technology (IT) systems and equipment belonging to TEN Group organisations, regardless of their location including other parties who are granted access through allocation of staff or guest IDs.

It applies to the use of all IT systems; networked, wireless, stand-alone and portable systems including those that connect remotely, to or through, TEN Group systems. They also apply to communications via video, voice, fixed or mobile devices or systems.

For clarification of further information on any matters within this document please contact your local Norfolk Educational Services (NES) IT Services team.

2. Your Responsibilities

Each staff member is allocated a User Account when they are first registered with TEN Group HR Services. Each account is unique within the Group and password protected. Signing for your account indicates that you have read and agreed to abide by this document, the "*Staff IT Acceptable Usage Policy*".

Never let anyone know your password or let anyone else logon using your account. You are responsible for the security of your account and the files stored within. Users are responsible for any misuse attributed to their account, including misuse by others.

Where possible lock the PC (Windows/start key and L) when away from a computer, or

logoff. (To unlock simply enter your password in the *Password* box).

All files of employees produced using the organisation's resources and time remain the property of that organisation.

Do not attempt to gain access to someone else's account, or data. This is a criminal offence under the Computer Misuse Act 1990.

Always store your data on the network where it is backed up regularly; local drives may be overwritten or a potential data protection risk.

Report any suspected security breaches to your local NES IT support team immediately.

3. Unacceptable Use

Staff users of IT and communications systems must not cause any of the following material to be transmitted wirelessly or over the organisation, Internet, national or public networks, or cause such to be stored in, printed, or displayed, on the organisation's IT systems or third party systems that may be attributed to the TEN Group organisations in any way:

- Obscene, pornographic, excessively violent, discriminatory, defamatory or other material that may offend.
- Material that infringes a right or inherent right of another person.
- Material that designed or likely to cause annoyance, inconvenience or needless anxiety.

The Group does not tolerate harassment in any form whatsoever. Any inappropriate material received which may cause offence to others must be reported to IT Services Management immediately, email john.pollitt@ccn.ac.uk or call 01603 773022.

All systems and equipment, including but not limited to software, hardware and printers, email, voicemail, telephones and the Internet are not to be used for private purposes (*see Exceptions section 3.9 for guidance on limited personal usage*).

3.1 Monitoring

NES utilises a range of automated monitoring tools to ensure appropriate usage of IT systems and services. Reports are regularly produced on telephone, print and email usage and they are also produced on the amount and nature of Internet usage by individuals. NES reserves the right to examine any files stored on TEN Group equipment and any information being transmitted over TEN Group networks. Information, emails, or files may be disclosed to third parties such as the Police, internal and external auditors in the process of any investigation undertaken.

Internet access is closely monitored including secure encrypted traffic and access times are logged against both the user account and the device used. Internet filtering

software is used to reduce the risk of accidental or deliberate exposure to offensive material. If you accidentally gain access to potentially offensive material, or feel that you have been barred from accessing a legitimate site, please report the incident to your local IT support team.

3.2 Changing Student Passwords

A student is able to reset their password by attending IT services with their current student planner.

If you wish to disable a student's account then ask IT Services.

3.3 Installation of Software or Hardware

If you need equipment moved please contact the Service Desk, do not attempt to disconnect and move equipment yourself.

Software or hardware must not be installed on the organisation's IT systems except by, or in arrangement with, IT Services.

USB devices that require no software installation may be connected.

3.4 Copyright and Licensing

All software in use at the organisation must be licensed and validated on the network. Licences for all software must be lodged with IT Services for possible audit by software anti-theft agencies or vendors.

Nothing should be downloaded from the Internet for use within the organisation unless express permission to do so is stated by the material owner, usually within the licence or usage agreement.

Any music or video files downloaded should be copyright free or purchased from a legitimate commercial site.

Scanned or digitally reproduced materials should be copyright free or fall within the remit of the Copyright Licensing Agreement.

If you require further advice please contact Dawn.Clarke@ccn.ac.uk

3.5 Printing

Printing services should be used for course, or business support related material only

and should be produced in black and white where possible. Please note that printing and photocopying is monitored and may also be allocated by a quota.

3.6 Exceptions (Personal Use)

All personal use must be within the conditions laid down in this document the *Staff IT Acceptable Usage Policy.*

Limited light use (up to two short calls, preferably local, per day) of the organisation's telephone systems or mobiles for personal calls is permitted within your own, unpaid time.

Limited light use (up to 5 small messages per day) of the organisation's email systems for personal email is permitted within your own, unpaid time. Subscription to high volume (more than 5 messages per day) list servers for non-work related purposes is specifically prohibited.

Limited light personal use (e.g. lunchtime or after work) of Internet is permitted within your own, unpaid time. Downloading of licensed software or non-copyrighted media (e.g. freeware, patches, drivers, movies, graphics, music), for personal use is permitted but should not use large amounts of file-store. Personal social networking is also permitted during unpaid time and should be closed during work periods. Further guidance around usage of social networking with students is available in the Social Media Guidelines for Staff on Blackboard and through staff Code of Conduct guidance.

Personal use does not include running a business using the organisation's IT.

Any personal material should be stored in folders clearly marked as personal.

Please note that Internet usage is carefully monitored and excessive non-work related usage will be reported on regularly by IT Services.

3. Electronic mail (email)

Email is one of the organisation's main methods of communication. You are expected to check your email regularly and to respond to messages in a timely manner.

You are required to set your Out of Office Assistant if you are out of the office and unavailable for a day or more.

Mail messages should be polite and professional, do not put into an email anything that which you would be unwilling to say to the recipient in person.

Ensure that your emails are typed in mixed case and do not use colours, backgrounds or typefaces that may cause difficulties for the recipient.

Ensure that large attachments are not distributed to multiple parties via email. If you wish to share a file then use pool areas or ask IT Services about other file sharing methods.

When addressing a message check the recipients are correct before sending.

When forwarding, remove unnecessary message history first.

Never use email to harass or otherwise cause offence or intimidation to the recipient.

Do not use the CC field to include anyone who is not absolutely necessary.

Do use the BCC field if you wish to send to multiple addresses that include private addresses.

Mail should not be sent to those who do not, or may not, wish to receive it.

Mail should not contain personal data (e.g. student details) unless encrypted.

Personal opinions should be represented as your own and not those of the organisation.

Any attached data leaving the organisation should be encrypted and certified virus free by the sender using the virus checking utilities on the network.

When composing a message remember that under the Freedom of Information Act the organisation may, in some circumstances, have to disclose the content of one or more of your emails to a third party.

Always bear in mind that emails are as legally binding as a written document.

4. Telephony & Voicemail

All calls should be answered within seven rings with callers greeted courteously and advised which service they have contacted.

Wherever possible a person, not a recorded message will answer calls during the normal office hours. Voice mail or answer phone can be used and this should be checked at least once a day - however during holidays an appropriate message should refer the caller to a number that will be staffed.

Pass on any appropriate calls and explain to the person being passed the call what the caller wants to know or take a message with care and hand it on without delay.

Respond to any telephone enquiry immediately if possible, or respond within 3 working days.

5. Health & Safety

The *Health and Safety (Display Screen Equipment) Regulations* 1992 aim to protect the health of people who work with DSE. They state, amongst other things, that:

"If you operate a VDU (computer with screen & keyboard) continuously for one hour, a break of at least ten minutes should be taken. If for any reason this period is extended to two hours then the break should be of at least half an hour. In this context a break means that work away from the VDU maybe undertaken; it does not mean a break away

from work altogether."

The Health and Safety Executive also recommends that when using a projector:

"Staring directly into the projector beam should be avoided at all times. Standing facing the beam should be minimised. Students should be adequately supervised when presenting or when pointing out information on the screen."

All IT equipment, desks, lighting and chairs are installed to comply with current Health and Safety regulations and recommendations. Further Health & Safety advice and procedures are available healthandsafety@ccn.ac.uk

6. Security

Students should never be left unsupervised in rooms containing IT equipment.

Care should be taken to prevent loss of or damage to portable equipment. For example, tablets, laptops and mobile phones should not be left in public areas or in view in an unoccupied car and should be stored securely when not in use.

Loss or damage to mobile equipment through negligence may result in a personal charge being made for replacement or repair of that equipment.

All users are expected to take care not to introduce a virus infection to the organisation's systems when downloading information via Internet or email or bringing in files on USB devices. Never distribute unchecked files to other users and report any suspected virus infection immediately.

If you require assistance with virus checking then ask your local IT support team.

7. Bring your own device (BYOD)

BYOD allows you to potentially use your own phone or tablet for example for business use where appropriate. For example you may wish to setup your work email to download to your device (which IT Services can help you with).

The TEN Group encourages the usage of BYOD at organisations where that is possible, however within the following constraints:

Your device must be virus protected and updated regularly.

Your device must contain the latest security patches and updates and should not be jail-broken or rooted.

You must set a password or code on any device used (to protect email for example).

No student data or images should be stored on the device.

In the event of the device being lost it should be remote wiped ASAP.

In the case of an investigation or complaint, NES reserves the right to examine any personal device used for business purposes.

7. Legal & Compliance

In addition to these conditions, the use of computers in general is regulated by three Acts of Parliament: the Data Protection Acts 1984 and 1998, the Copyright, Designs and Patents Act 1988 and the Computer Misuse Act 1990. Similarly, the use of the public data telephone networks is regulated by the Telecommunications Act 1984. These and several other Acts (including the Obscene Publications Act 1978 as amended by the Criminal Justice Act 1994, and the Protection of Children Act 1978) identify a number of prohibited actions related to the use of computers for viewing or distribution of materials.

Staff may be asked for information or data by the authorities either informally or under The Police and Criminal Evidence Act (1984). In both cases the request should be referred to NES IT Services Management.

Data about individuals may not be stored on the organisation, or other IT systems for any purpose unless the use of such data has been previously registered under the Data Protection Act. If you wish to hold data about individuals or need data protection advice contact

Data stored on mobile devices such as laptops, tablets, usb pens, or other portable or handheld devices should not include data about individuals or other company confidential information unless in a secure encrypted format.

Staff writing emails or posting on forums, blogs or social media should ensure their facts are accurate and in no way defamatory within the scope of The Defamation Act (1996).

8. Disciplinary Procedure

Minor breaches of these conditions will be raised by IT Services Management, with the member of staff concerned. IT Services will record and document these breaches. It may be necessary to copy this documentation to the appropriate line manager.

Serious or persistent offences may constitute gross misconduct and will be considered on an individual basis involving all relevant parties, using the organisation's Disciplinary Procedure. All available evidence as well as the severity of the offence will be considered as part of the disciplinary procedure. Disciplinary action may result in long term to permanent loss of IT privileges or, in more serious cases, to disciplinary warnings and/or dismissal.

Those offences regarded as serious include:

- Failure to comply with legal obligations

- Criminal Acts
- All aspects of the Unacceptable Use section (with the exception of accidental damage to equipment)
- All aspects of the Your Responsibilities and Security sections (excepting storing data on local hard drives, unless it constitutes third party personal data)
- Excessive or repeated exploitation of the quoted "Exceptions"
- Excessive or repeated breach of lesser conditions

Breaches of criminal law will be referred to the appropriate authorities. Staff will be bound to aid any investigation undertaken by the police where an alleged breach of criminal law is involved.

Paper copies and large print versions of this document can be requested from IT Services.