Neston High School

IT & Communications Acceptable Use Policy

January 2019

1. Overview

The IT and Communication Facilities at Neston High School are led by:

Mr J Barratt - ICT Services Manager
Mr M Sumner - ICT Technician
Mr C Dwyer - ICT Technician

Mrs T Phillips - Data Protection Officer
Mr K Simpson - Headteacher
Mr J Dathan - Assistant Headteacher (ICT SLT Lead)

The IT and Communication Facilities at Neston High School are defined as:

- All Computing devices (e.g. Computer, Laptop, Tablet) and Software
- Connected peripherals such as Keyboards, Mice etc
- Printers, Scanners, and Copiers
- Digital capture devices such as Cameras and Camcorders
- Telephones
- Fax Machines
- Televisions
- Video Players
- DVD players
- TV/Satellite Receivers
- Other devices including fittings used with them

Internet and E-mail can be defined as a Communication facility used in conjunction with IT facilities, as such; these will coincide with the IT and Communication Facilities.

This policy contains:

- The school's view on the use of e-mail and the internet at Neston High School.
- An explanation of what you can or cannot do.
- The consequences if you fail to follow the rules set out in this policy.
- General information relating to IT and Communication, including the Data Protection Act.
- How the policy is implemented and monitored.
- IT Services (IT Services Manager, and IT Technicians) & Senior Leaders duties relating to this policy.

2. Policy

The use of the IT and Communication Facilities within the school is encouraged, as its appropriate use facilitates learning, communication and can improve efficiency.

Used correctly, it is a tool that is of assistance to both students and staff at Neston High School. Its inappropriate use, however, causes many problems, ranging from minor distractions to exposing the school or staff/students to financial, technical, commercial and legal risks.

As well as adhering to this policy, everyone should be mindful of this policy applies to anyone using IT and Communication Facilities at Neston High School. If you witness or are aware of any misuse or breaches of this policy, you must report it to IT Services or the Headteacher/Assistant Headteacher.

1. A misuse or breach of this policy may result in disciplinary action being taken against you, outlined later in this policy.
2. A misuse or breach of this policy could also result in criminal or civil actions being brought against you.

3. Authorised Use of IT and Communications Facilities

The IT and Communication Facilities are provided to enable users to complete tasks as required by your work duties or study needs. This includes, but may not be limited to:

- Preparing work for lessons, activities, meetings, reviews, etc.
- Researching for any school related task
- Any School encouraged tuition or educational use
- Collating or processing information for school business

Users of the school's ICT facilities must be aware that any use outside of the above categories will be monitored as described below and subject to the same restrictions as set-out below. If any such use is deemed to be excessive, inappropriate or likely to bring the school into disrepute then it will be dealt with as a serious matter.
If unsure, please seek clarification/authorisation from the IT Services Manager, your line manager or Headteacher/Assistant Headteacher.

4. Unauthorised Use of IT and Communications Facilities

You are NOT permitted under any circumstance to:

1. Use IT and Communication Facilities for commercial or financial gain without the explicit written authorisation from the Headteacher/Assistant Headteacher
2. Physically damage the IT and Communication Facilities.
3. Re-locate, take off-site or otherwise interfere with the IT and Communication Facilities without the authorisation of the IT Services or Headteacher/Assistant Headteacher. Items that are taken off site must be signed for.
4. Use or attempt to use someone else's user account. All users will be issued with a unique user account and password. The password must be changed at regular intervals.
5. Conduct activity or solicit the performance of any activity which is prohibited by law.
6. Use the IT and Communication Facilities at any time to create, publish, access, download, send, receive, copy, view or display any of the following:
    - Any content that is illegal
    - Any content that is sexually explicit
    - Any content considered abusive, profane, or sexually offensive.
    - Any content that which violates or infringes upon the rights of any other person.
    - Any content that could constitute bullying, harassment (including on the grounds of sex, race religion/religious belief, sexual orientation or disability) or any negative comment about other persons or organisations

- Remarks relating to a person's sexual orientation, gender assignment, religion, disability or age
- Remarks, which may adversely affect the reputation of any organisation or person, whether or not you know them to be true or false

7. Generate messages or documents that appear to originate from someone else, or otherwise impersonate someone else.
8. Install hardware or software without the consent of IT Services.
9. Introduce any form of stand-alone software or removable hardware likely to cause malfunctioning of the IT and Communication Facilities, or that will bypass, over-ride, or overwrite the security parameters on the network or any of the School's systems. This comes under the Computer Misuse Act and is illegal.
10. Use or attempt to use the School's IT and Communication Facilities to undertake any form of piracy including the infringement of software licenses or other copyright provisions whether knowingly or not. This is illegal.
11. Use or attempt to use the schools' phone lines for Internet or email access unless given authorisation by IT Services.
12. Use the Internet for any auctioning activity or to purchase items unless given authority to do so by the Headteacher or Finance Department.
13. Access and use social media services (Facebook, Twitter etc) for personal use is strictly forbidden. Official school related use must be prior authorised by IT Services or Headteacher/Assistant Headteacher. Such access must be linked to an official school email account, and password stored on file with IT Services.
14. Knowingly distribute or introduce a virus or harmful code onto the school's network or Computers.
15. Copy, download or distribute any material from the Internet or email that may be illegal to do so. This can include computer software, music, text, and video clips. If it is not clear that you have permission to do so, or if the permission cannot be obtained, do not do so.
16. To obtain and post on the internet or send via email any confidential information about other employees, students, the School, or suppliers.
17. Interfere with someone else's use of the IT and Communication Facilities.
18. Be wasteful of IT resources, particularly printer ink, toner and paper.
19. Use the IT and Communication Facilities when it will interfere with your responsibilities to supervise students.
20. Take offsite copies or links containing any personally identifiable data relating to any member of the school community.
21. Use of the school's telephone facilities is strictly for educational and business use relating to Neston High School. Personal *emergency* calls are permitted, however you must notify IT Services or the Headteacher/Assistant Headteacher after the call.

5. E-mail and the Internet

E-mail accounts and Internet access are available for communication and use on matters directly concerned with school business or school curriculum. Everyone using the school's e-mail system and Internet connection should give particular attention to the following points:

1. If an e-mail message is confidential, you must ensure that any necessary steps are taken to protect confidentiality. The School will be liable for any defamatory information circulated either within the School or to external contacts.
2. All e-mails that are sent or received must be retained within the School for a period of six months.
3. Offers or contracts sent via e-mail or the Internet are as legally binding on the School as those sent on paper. An exchange of e-mails can lead to a contract being formed between you, or the school, and the recipient. Never commit the school to any obligations by e-mail or the Internet without ensuring that you have the authority to do so. If you have any concerns, contact the Headteacher.
4. Buying online is only permitted with the Business or Finance Manager consent. Hard copies of the purchase must be made, for yourself and for the Finance Manager. This is in addition to any purchasing arrangement followed according to School policy.

5. You are not permitted to login to any third-party email accounts (such as Hotmail, Gmail), IT Services have no control over content/use of such services. Anyone found using third-party email accounts will face disciplinary action. Sending unsolicited emails (spam) to other Network users or to the outside world will not acceptable. Users should not alter any advanced settings found within the schools email system.
6. Access to websites is restricted based on safeguarding requirements and discretion of the Headteacher/Assistant Headteacher. If a website is blocked, and you feel it should be allowed, please raise this with IT Services. This may require authorisation from the Headteacher/Assistant Headteacher.
7. Any confidential data regarding named individuals must be sent via an encrypted service which is password protected. This includes performance data or personal details about named students.

6. Account access, Security and Passwords

Users are expected to;

1. Ensure they have a strong password; see our "password guidelines" document on the intranet (help and tips) for advice
2. Change their password regularly to maintain password security. You will be required to change your main network password every 8 weeks, you will be reminded about this 10 days before your password expires at login. Please note, if you let your password expire you will not be able to access your account remotely (email or remote portal). Your password needs to be reset **in school** or over the telephone with IT Services – you will be asked certain security questions. You cannot have your password reset by email or via a third party.
3. Safeguard their password. For example, users should not write down or store their password on paper or on a computer system where others might acquire it.
4. Never share their password, even with a best friend or relative.
5. Reserve a password for use at Neston High School only. Individuals should have different passwords for external services such as stores, banks, music services, home computers etc.

   Any users who suspects their password has been compromised are required to change it immediately, and report this to IT Services. If you are not able to change your password for any reason you should contact IT Services who will assist.

6. Staff will have access to a vast amount of confidential information, including student's personal details. You must ensure this data remains secure. Do not leave any computer logged on unattended, either *lock* the system or logout.
7. Access to the schools management system (SIMS) is secured by a secondary logon, for security you must ensure you use a different password for both logging on to the Network and to SIMS.
8. You must not leave any confidential information, including but not restricted to student details visible on screen or on a projected display.
9. If you print any confidential information it is your responsibility to ensure the print out remains secure. Should the printout fail to print, it is unacceptable to just leave the print job in the system. The document could print out some time later and be picked up by someone not authorised to access such information. You must notify IT Services of any confidential document that fails to print.

7. Remote Access

Neston High School IT Services also offer a remote 'work at home' portal so you can access school software and your documents from your home computer. The Citrix Portal service is provided to help staff and students meet the management, educational, curricular and administrative requirements of the school. For more information on how to use this system at home, please see the Citrix user guide and installation manual which can be found under 'Support Docs' on the Intranet.

1. All users of the Citrix Portal remain bound by all aspects of this policy, even if accessing it from a remote location.
2. While logged into the Citrix Portal you have a direct and live connection to the school network. Users must not leave this connection unsupervised for any period of time – it is the users' responsibility to ensure no-one but the undersigned has access to a Citrix Portal session while logged in.
3. IT Services or the Headteacher/Assistant Headteacher reserve the right to remove access to this service at any time without notice.
4. Use of this remote access portal is logged.

8. General IT Information

Below are general notes users should be aware of when using IT and Communication Facilities at Neston High School:

1. Following new GDPR policy, all users at Neston High will be able to continue to use USB data devices. However it **NO PERSONAL DATA** (such as assessment sheets, data analysis, attendance information or phone numbers) should ever be stored and transported on a portable device. Any need for access to PERSONAL DATA must be done through a secure remote login, (available as Citrix). It is suggested the only use for a USB stick that would be required would be for large files to be used as lesson resources such as videos or images etc.
2. Users are allocated a quota of space on the server by IT Services. Users will be warned when they are over their quota. Users are expected to clear out any 'out of date' or no longer relevant material at regular intervals.
3. Information and data on the schools network and computers should be kept in an organised manner and should be placed in a location of an appropriate security level. If unsure, please ask your line manager or IT Services.
4. IT and Communication Facilities at Neston High School may not always meet users' requirements or be uninterrupted or error-free. Facilities are provided on an "as is, as available" basis. The School does not make any warranties with respect to any service and any information or software contained therein. Where possible we will try and inform users of planned down time in advanced, but this may not always be possible. Users are advised to ensure they have backups of their data.
5. The copyright owner of any files created on a school computer is by default Neston High School.
6. Users are not permitted to commission install/connect any new/additional equipment onto the school network without explicit written permission of IT Services. This includes, but is not limited to staff/personal laptops.
7. IT equipment (Base units, Monitors, Printers, Scanners, Keyboard, Mice, Cables etc) is commissioned, positioned by IT Services and logged against an equipment asset register. Users are **not** permitted to relocate/move any piece of equipment from its designated location/room unless they have the explicit written permission of IT Services. Equipment commissioned/installed by IT Services may not be decommissioned by anyone other than IT Services. If you require equipment moving, please log this as a request on the Helpdesk.
8. No-one should assume the right to alter any piece of equipment without explicit consent from IT Services.
9. Anyone who feels that they have cause for complaint should raise the matter initially with their Line Manager, or Headteacher as appropriate.
10. All equipment faults or requests should be reported to IT Services via the Helpdesk.

9. Implementation and Accountability

To implement, monitor and effect accountability of this policy, the following applies:

1. Staff are requested to report any breach of this policy to IT Services, or Headteacher/Assistant Headteacher. Any breach of PERSONAL DATA must be immediately reported to the Data Protection Officer (TPH).
2. All user accounts are accessible by IT Services to monitor/investigate policy compliance.
3. Daily checks of computer activity of all user accounts is performed by IT Services and any inappropriate use is reported to the line manager or Headteacher.
4. Regular monitoring and recording of e-mail messages will be carried out on a random basis. Hard copies of e-mail messages can be used as evidence in disciplinary proceedings.
5. Use of the telephone system is logged and monitored.
6. Use of the school's internet connection is recorded and monitored.
7. Random checks against school asset register are conducted to ensure equipment is located and logged correctly.
8. IT Services adjust access rights and security privileges in the interest of the protection of school data, information, the school network and computers. This is also done on instruction of Senior Leadership or when breach of this policy is suspected by IT Services.
9. IT Services can remotely view or interact at any time with any of the computers on the school network; this includes computers accessing the schools systems through remote access such as Citrix. This may be used randomly to implement this Policy and to assist in any difficulties.
10. The schools network has anti-virus software installed with a centralised administration package; any virus found is logged to this package.
11. Users must ensure that critical information is not stored solely within the school's computer system. Hard copies or backup copies must be kept or stored separately on the system. If necessary, documents must be password protected.
12. Termly the data protection team in the school will randomly select five staff to check data flow of content and use of Citrix / USB access for files and content to monitor compliance with GDPR and school policy.
13. Users are required to be familiar with the requirements of the Data Protection Act 1998 & the General Data Protection Regulations 2018 and to ensure that they operate in accordance with the requirements of the Act. The obligations under the Act are complex but prominent issues are:
    - Do not disclose any information about a person including a student, without their permission which you would object to being disclosed about yourself
    - Such material includes information about a person's racial or ethnic origin, sex life, political beliefs, physical or mental health, trade union membership, religious beliefs, financial matters and criminal offences
      Do not send any personal data outside the UK

10. Disciplinary Actions

Any action by a user that is determined by IT Services or the Headteacher/Assistant Headteacher to constitute as a breach of this policy may result in disciplinary action. Disciplinary actions may include but are not limited to, temporary access ban, permanent termination of access to school networks, in-school suspension, suspension from school, dismissal, or legal action. This is in conjunction with the school's discipline policy.

Senior leadership are consulted regarding disciplinary actions, and this will, at their discretion, involve contacting parents, guardians or the authorities.

11. User agreement (Digital and hard-copy)

Users are required to read and agree to this policy when logging onto a computer for the first time, and are reminded of their agreement each subsequent logon. In addition to 'digitally agreeing', staff are required to initial and sign a hard copy of this agreement, a copy of which is placed on their personnel file.