



NESTON
HIGH SCHOOL

ICT Systems and Acceptable Use Policy

Policy owners/leads:	JCD
Notes:	The Key
Statutory:	Yes
Website:	Yes
Review period:	2 Years

Date	Action	Comments / Follow Up
Nov 2018	Policy adopted	Next review: Nov 2020
Nov 2020	Policy reviewed	Next review: Nov 2022
Nov 2022	Policy reviewed and updated	Next review: Dec 2024
Nov 2024	Policy reviewed	Next review: Dec 2026
Nov 2026	Policy reviewed	Next review: Dec 2028



NESTON
HIGH SCHOOL

✦ *Shaping Extraordinary Lives* ✦

Contents

Contents	2
1. Introduction & Aims.....	3
2. Key Roles.....	3
3. Relevant legislation and guidance.....	4
4. Definitions	4
5. Authorised use of ICT facilities	5
6. Unacceptable use	5
7. Exceptions from unacceptable use.....	6
8. Staff (including governors, volunteers, and contractors)	7
9. Students	9
10. Parents.....	10
11. Data security	10
12. Remote access	12
13. Monitoring of school network and use of ICT facilities.....	12
14. Protection from cyber attacks	13
15. General IT Information & Guidance	14
16. Disciplinary Actions.....	15
17. Staff user agreement.....	15



1. Introduction & Aims

- 1.1 Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for pupils, staff (including senior leadership teams), governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school.
- 1.2 However, the ICT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding.
- 1.3 This policy aims to:
 - 1.3.1 Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and governors
 - 1.3.2 Establish clear expectations for the way all members of the school community engage with each other online
 - 1.3.3 Support the school's policy on data protection, online safety and safeguarding
 - 1.3.4 Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems
 - 1.3.5 Support the school in teaching pupils safe and effective internet and ICT use
- 1.4 This policy covers all users of our school's ICT Facilities, including governors, staff, pupils, volunteers, contractors, and visitors.
- 1.5 Breaches of this policy may be dealt with under our disciplinary policy and/or behaviour policy/staff.
- 1.6 As well as adhering to this policy, everyone should be mindful of this policy applies to anyone using ICT 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.

2. Key Roles

- 2.1 Key roles concerning and governing the ICT Facilities at Neston High School are as follows. Staff currently in these roles are available from the HR Manager.
 - 2.1.1 IT Services Manager
 - 2.1.2 IT Technicians
 - 2.1.3 Data Protection Officer
 - 2.1.4 Headteacher

3. Relevant legislation and guidance

3.1 This policy refers to, and complies with, the following legislation and guidance:

- ✦ [Data Protection Act 2018](#)
- ✦ [The General Data Protection Regulation](#)
- ✦ [Computer Misuse Act 1990](#)
- ✦ [Human Rights Act 1998](#)
- ✦ [The Telecommunications \(Lawful Business Practice\) \(Interception of Communications\) Regulations 2000](#)
- ✦ [Education Act 2011](#)
- ✦ [Freedom of Information Act 2000](#)
- ✦ [The Education and Inspections Act 2006](#)
- ✦ [Keeping Children Safe in Education 2021](#)
- ✦ [Searching, screening and confiscation: advice for schools](#)
- ✦ [National Cyber Security Centre \(NCSC\)](#)
- ✦ [Education and Training \(Welfare of Children Act\) 2021](#)

4. Definitions

- 4.1 **"ICT facilities"**: includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service
- 4.2 **"Users"**: anyone authorised by the school to use the ICT facilities, including governors, staff, pupils, volunteers, contractors, and visitors
- 4.3 **"Personal use"**: any use or activity not directly related to the users' employment, study, or purpose
- 4.4 **"Authorised personnel"**: employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
- 4.5 **"Materials"**: files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs.

5. Authorised use of ICT facilities

- 5.1 The ICT 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:
 - 5.1.1 Preparing work for lessons, activities, meetings, reviews, etc.
 - 5.1.2 Researching for any school related task
 - 5.1.3 Any School encouraged tuition or educational use
 - 5.1.4 Collating or processing information for school business
- 5.2 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.
- 5.3 Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.
- 5.4 If unsure, please seek clarification/authorisation from the IT Services Manager, your line manager or Headteacher/Assistant Headteacher.

6. Unacceptable use

- 6.1 Unacceptable use of the school's ICT facilities includes:
 - 6.1.1 Using the school's ICT facilities to breach intellectual property rights or copyright
 - 6.1.2 Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
 - 6.1.3 Breaching the school's policies or procedures
 - 6.1.4 Any illegal conduct, or statements which are deemed to be advocating illegal activity
 - 6.1.5 Online gambling, inappropriate advertising, phishing and/or financial scams
 - 6.1.6 Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
 - 6.1.7 Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth-produced sexual imagery)
 - 6.1.8 Activity which defames or disparages the school, or risks bringing the school into disrepute
 - 6.1.9 Sharing confidential information about the school, its pupils, or other members of the school community
 - 6.1.10 Connecting any device to the school's ICT facilities without approval from authorised personnel
 - 6.1.11 Setting up any software, applications, or web services on the school's network without approval by IT Services, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts, or data
 - 6.1.12 Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
 - 6.1.13 Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities

- 6.1.14 Causing intentional damage to ICT facilities
 - 6.1.15 Removing, deleting, or disposing of ICT facilities, systems, programs, or information without permission by authorised personnel
 - 6.1.16 Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
 - 6.1.17 Using inappropriate or offensive language
 - 6.1.18 Promoting a private business, unless that business is directly related to the school
 - 6.1.19 Using websites or mechanisms to bypass the school's filtering mechanisms
 - 6.1.20 Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way
 - 6.1.21 Use ICT facilities for commercial or financial gain without the explicit written authorisation from the Headteacher/Business Manager
 - 6.1.22 Interfere with someone else's use of the ICT facilities
 - 6.1.23 Be wasteful of ICT resources, particularly printer ink, toner, and paper
 - 6.1.24 Use the ICT facilities when it will interfere with your responsibilities to supervise students
 - 6.1.25 Take offsite copies or links containing any personally identifiable data relating to any member of the school community
 - 6.1.26 Re-locate, take off-site or otherwise interfere with the ICT facilities without the authorisation of the IT Services or Headteacher/Assistant Headteacher. Items that are taken off site must be signed for
- 6.2 This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher, Business Manager and IT Services Manager will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

7. Exceptions from unacceptable use

- 7.1 Where the use of school ICT facilities (on the school premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the headteacher's discretion. Reasons for exemption will be approved by 2 members of SLT, documented, and kept on file.

8. Staff (including governors, volunteers, and contractors)

8.1 Access to school ICT facilities

- 8.1.1 Staff will be provided with unique login/email account and temporary password that they must use when accessing the school's ICT facilities. The temporary password must be changed upon first use. The password you choose must comply with the *Data Security (Passwords)* section below.
- 8.1.2 The school's IT Services Team, under the direction of SLT, manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:
 - 8.1.2.1 Computers, tablets, mobile phones, and other devices
 - 8.1.2.2 Access permissions for certain programmes or files
- 8.1.3 Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the IT Services Team.
- 8.1.4 Requests for additional or higher-level access should be raised on the internal Service Desk, where the request will be approved by SLT and actioned by IT Services.

8.2 Use of phones and email

- 8.2.1 The school provides each member of staff with an email address.
- 8.2.2 This email account should be used for work purposes only.
- 8.2.3 All work-related business should be conducted using the email address the school has provided.
- 8.2.4 Staff must not share their personal email addresses with parents and pupils, and must not send any work-related materials using their personal email account.
- 8.2.5 Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.
- 8.2.6 Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.
- 8.2.7 Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.
- 8.2.8 If staff receive an email in error, the sender should be informed, and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.
- 8.2.9 If staff send an email in error that contains the personal information of another person, they must inform the Headteacher/Business Manager immediately and follow our data breach procedure.
- 8.2.10 Staff must not give their personal phone numbers to parents or pupils. Staff must use phones provided by the school to conduct all work-related business.
- 8.2.11 School phones must not be used for personal matters. However, personal emergency calls are permitted; however, you must notify the Headteacher/Business Manager

- 8.2.12 Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use.
- 8.2.13 The school may record in-coming and out-going phone conversations.

8.3 Personal use

- 8.3.1 Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Headteacher, Business Manager, or IT Services Manager may withdraw permission for it at any time or restrict access at their discretion.
- 8.3.2 Personal use is permitted provided that such use:
- 8.3.2.1 Does not take place during contact time/teaching hours/non-break time
 - 8.3.2.2 Does not constitute 'unacceptable use'
 - 8.3.2.3 Takes place when no pupils are present
 - 8.3.2.4 Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes
 - 8.3.2.5 Does not result in personal non-work-related information or materials being saved to school systems.
- 8.3.3 Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities. Where breaches of this policy are found, disciplinary action may be taken.
- 8.3.4 Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents could see them.
- 8.3.5 Staff should take care to follow the school's guidelines on social media (see appendix 1) and use of email to protect themselves online and avoid compromising their professional integrity.

8.4 Personal social media accounts

- 8.4.1 Members of staff should ensure their use of social media, either for work or personal purposes, is appropriate at all times.
- 8.4.2 The school has guidelines for staff on appropriate security settings for social media, please see the [Social Media Policy](#).

8.5 School social media accounts

- 8.5.1 The school has official social media accounts, these managed by the Business Manager, IT Services Manager and approved members of staff. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.
- 8.5.2 The school has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

9. Students

9.1 Access to school ICT facilities

- 9.1.1 Students will be provided with unique login/email account and temporary password that they must use when accessing the school's ICT facilities. The temporary password must be changed upon first use. The password you choose must comply with the *Data Security (Passwords)* section below.
- 9.1.2 ICT facilities are available to pupils only under the supervision of staff.
- 9.1.3 Sixth-form pupils can use the computers independently for educational purposes only.

9.2 Search and deletion

- 9.2.1 Under the Education Act 2011, and in line with the Department for Education's [guidance on searching, screening and confiscation](#), the school has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.
- 9.2.2 The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.
- 9.2.3 Staff members may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse contains an online element.

9.3 Unacceptable use of ICT facilities, and the internet outside of school

- 9.3.1 The school will sanction students, in line with the behaviour and discipline policy, if a student engages in any of the following at any time (even if they are not on school premises):
 - 9.3.1.1 Using ICT or the internet to breach intellectual property rights or copyright
 - 9.3.1.2 Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
 - 9.3.1.3 Breaching the school's policies or procedures, including the entirety of this policy
 - 9.3.1.4 Any illegal conduct, or statements which are deemed to be advocating illegal activity
 - 9.3.1.5 Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
 - 9.3.1.6 Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
 - 9.3.1.7 Activity which defames or disparages the school, or risks bringing the school into disrepute
 - 9.3.1.8 Sharing confidential information about the school, other pupils, or other members of the school community
 - 9.3.1.9 Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel
 - 9.3.1.10 Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
 - 9.3.1.11 Causing intentional damage to ICT facilities or materials
 - 9.3.1.12 Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation

10. Parents

10.1 Access to school ICT facilities

- 10.1.1 Parents do not have access to the school's ICT facilities as a matter of course.
- 10.1.2 However, parents working for, or with the school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the school's facilities at the headteacher's discretion.
- 10.1.3 Where parents are granted access in this way, they must abide by this policy as it applies to staff.

10.2 Communicating with or about the school online

- 10.2.1 We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.
- 10.2.2 Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.
- 10.2.3 We ask parents to sign the agreement in appendix 2.

11. Data security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place. It therefore takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times.

11.1 Passwords

- 11.1.1 Users of the school's ICT facilities must set strong passwords for their accounts and keep these passwords secure. A strong password contains both alphanumeric and punctuation/special characters and is at least 10 characters in length.
- 11.1.2 Unique passwords must be used for accounts at Neston High School. **You must NOT reuse a password you use elsewhere.** Users should have different passwords for external systems/services such as stores, banks, music services, and home computers etc.
- 11.1.3 **Staff should NOT re-use their main login/email password for other school systems,** such as Arbor etc. New, strong, and unique passwords must be used for all systems.
- 11.1.4 Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.
- 11.1.5 Members of staff or Students who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.
- 11.1.6 Users must 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.
- 11.1.7 Any users who suspect 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.

11.2 Software updates, firewalls and anti-virus software

- 11.2.1 All of the school's ICT devices that support software updates, security updates and anti-virus products will be configured to perform such updates regularly or automatically.
- 11.2.2 Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.
- 11.2.3 Any personal devices using the school's network must all be configured in this way.

11.3 Data protection

- 11.3.1 All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.
- 11.3.2 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
- 11.3.3 If you print any confidential information, it is your responsibility to ensure the printout 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.

11.4 Access to facilities and materials

- 11.4.1 All users of the school's ICT facilities will have clearly defined access rights to school systems, files, and devices.
- 11.4.2 These access rights are managed by IT Services under the direction of SLT.
- 11.4.3 Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the Headteacher, Business Manager or IT Services Manager immediately.
- 11.4.4 Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and shut down / powered off completely at the end of each day.

11.5 Encryption

- 11.5.1 The school ensures that its devices and systems have an appropriate level of encryption.
- 11.5.2 School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the headteacher.

12. Remote access

- 12.1 We allow staff and students to access the school's ICT facilities and materials remotely.
- 12.2 'Remote Access' 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 user guide and installation manual which can be found on the school website.
- 12.3 Users accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site
- 12.4 While logged into the Remote Access System, users 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 user account holder has access to the Remote Access session.
- 12.5 Headteacher, Business Manager or IT Services reserve the right to remove access to this service at any time without notice.
- 12.6 Use of this Remote Access System is logged.

13. Monitoring of school network and use of ICT facilities

- 13.1 Contents of the school's IT resources and communications systems are the school's property. Users should therefore have no expectation of privacy in any messages, files, data, document or posts/conversation or message transmitted to, received or printed from, or stored or recorded on the school's information and communications systems.
- 13.2 Staff should not use the school's IT resources and communications systems for any matter that they wish to be kept private or confidential.
- 13.3 The school reserves the right to monitor the use of its ICT facilities and network to ensure that rules are being complied with and being used for legitimate business purposes. This includes, but is not limited to, monitoring of:
 - 13.3.1 ICT facility use
 - 13.3.2 Internet sites visited
 - 13.3.3 Bandwidth usage
 - 13.3.4 Email accounts
 - 13.3.5 Telephone calls
 - 13.3.6 User activity/access logs
 - 13.3.7 Any other electronic communications
- 13.4 The school monitors ICT use in order to:
 - 13.4.1 Obtain information related to school business
 - 13.4.2 Investigate compliance with school policies, procedures, and standards
 - 13.4.3 Ensure effective school and ICT operation
 - 13.4.4 Conduct training or quality control exercises
 - 13.4.5 Prevent or detect crime
 - 13.4.6 Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

- 13.5 Authorised ICT staff may inspect, monitor, intercept, assess, record, and disclose the above, to the extent permitted by law. All user accounts are accessible by IT Services to monitor/investigate policy compliance.
- 13.6 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.
- 13.7 IT Services may remotely view or interact at any time with any of the schools ICT facilities, this includes computers accessing the schools' systems through remote access systems. This may be used randomly to implement this policy and/or to assist with user support requests.
- 13.8 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 SLT or when breach of this policy is suspected by IT Services.

14. Protection from cyber attacks

The school will:

- 14.1 Work with Trustees and the IT Services Team to make sure cyber security is given the time and resources it needs to make the school secure
 - 14.1.1 Provide training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:
 - ✦ Check the sender address in an email
 - ✦ Respond to a request for bank details, personal information or login details
 - ✦ Verify requests for payments or changes to information
- 14.2 Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- 14.3 Investigate whether our IT software needs updating or replacing to be more secure
- 14.4 Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- 14.5 Put controls in place that are:
 - 14.5.1 **Proportionate:** the school will verify this annually using a third-party audit, to objectively test that what it has in place is up to scratch
 - 14.5.2 **Multi-layered:** everyone will be clear on what to look out for to keep our systems safe
 - 14.5.3 **Up-to-date:** with a system in place to monitor when the school needs to update its software
 - 14.5.4 **Regularly reviewed and tested:** to make sure the systems are as up to scratch and secure as they can be
- 14.6 Back up critical data daily, and store these backups on cloud-based backup systems and external hard drives that aren't connected to the school network, and which can be stored off the school premises
- 14.7 Make sure staff:
 - 14.7.1 Enable multi-factor authentication where they can, on things like school email accounts
 - 14.7.2 Have a separate password for school systems
 - 14.7.3 Store passwords securely using a password manager

- 14.8 Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- 14.9 Have a firewall in place, up-to-date, and is switched on
- 14.10 Have up-to-date antivirus and antimalware installed on all applicable systems.
- 14.11 Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and seeing if they have the [Cyber Essentials](#) certification
- 14.12 Develop, review and test an incident response plan with the IT Services Team, for example, including how the school will communicate with everyone if communications go down, who will be contacted when, and who will notify [Action Fraud](#) of the incident. This will be reviewed and tested annually and after a significant event has occurred, using the NCSC's '[Exercise in a Box](#)'

15. General IT Information & Guidance

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

- 15.1 Following GDPR policy, all users at Neston High will be able to continue to use USB data devices. However, **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. 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.
- 15.2 Users are allocated a quota of space on the storage space (H: drive and OneDrive). 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.
- 15.3 Information and data on the school's 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.
- 15.4 ICT 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.
- 15.5 The copyright owner of any files created on a school computer is by default Neston High School.
- 15.6 IT facilities are commissioned and 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 Service Desk.
- 15.7 No-one should assume the right to alter any piece of equipment without explicit consent from IT Services.
- 15.8 Anyone who feels that they have cause for complaint should raise the matter initially with their Line Manager, or Headteacher as appropriate.
- 15.9 All equipment faults or requests should be reported to IT Services via the Service Desk.

16. Disciplinary Actions

- 16.1 Any action by a user that is determined by Headteacher, Business Manager, or IT Services 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 ICT facilities, in-school suspension, suspension from school, dismissal, or legal action. This is in conjunction with the school's discipline policy.
- 16.2 Senior leadership team are consulted regarding disciplinary actions, and this will, at their discretion, involve contacting parents, guardians, or the authorities.

17. Staff user agreement

- 17.1 Staff are required to initial and sign a hard copy of this agreement, a copy of which is placed on their personnel file.

By signing below, you understand and agree to adhere to this policy.

A copy of this document is available on the schools Intranet,
or a paper copy can be requested.

You must also initial at the bottom of each page.

Full Name: _____

Signed: _____

Date: _____

Acceptable use of the school's ICT facilities and internet.

Agreement for students and parents/carers

Name of student:

When using the school's ICT facilities and accessing the internet in school, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Use them to break school rules
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share any semi-nude or nude images, videos or livestreams, even if I have the consent of the person or people in the photo
- Share my password with others or log in to the school's network using someone else's details
- Bully other people

I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school's ICT systems and internet responsibly.

I understand there is a full ICT Acceptable Use Policy, and I agree I have read this with my parents and understand its contents.

I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

Signed (student):

Date:

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I have read the full ICT Acceptable Use policy. I agree to the conditions set out above, and in the policy, for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):

Date:

Acceptable use of the internet

agreement for parents/carers

Name of parent/carer:

Name of child:

Online channels are an important way for parents/carers to communicate with, or about, our school.
The school uses the following channels:

- Our official Facebook page
- Email/text groups for parents (for school announcements and information)
- Our virtual learning platform

Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).

When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will:

- Be respectful towards members of staff, and the school, at all times
- Be respectful of other parents/carers and children
- Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure

I will not:

- Use private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive, and the school can't improve or address issues if they aren't raised in an appropriate way
- Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident
- Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers

Signed:

Date: