WOODBRIDGE HIGH SCHOOL

Digital Technology Handbook

Updated: Autumn 2024

Contents

Adding to the Digital Handbook

If at any time you think there could be a useful addition to the Digital Handbook, please liaise with Jeremy Clifton (Deputy Headteacher – Whole School ICT) to see if its inclusion is appropriate.

Communication: Parents/Carers

It is acceptable to communicate with parents/carers using your school e-mail account, but always keep copies of any e-mails you send to them. Please ensure that appropriate language & tone are used and established communication protocols are adhered to. Do not communicate with any parent/carer using your personal e-mail account, a personal account with a social networking site, or your personal mobile telephone. In some instances, e.g. on a trip for an emergency situation, the use of a personal mobile telephone may be acceptable. Staff should prefix any phone calls using their mobile with the number 141. This blocks their mobile number from view.

Communication: Students

Do not communicate with any student using ICT unless it is work-related. Communicating about their class work, academic progress or a related matter is acceptable using your school e-mail account. You must establish safe and responsible online behaviour. Do not communicate with them on any social networking site. All communications must take place within clear and explicit professional boundaries. You should not access social networking sites of students; do not give any student any of your personal contact details, including your mobile telephone number. Do not use any web-based channels to communicate with students apart from official school systems. Never send any student personal messages. There may be rare occasions when going outside agreed protocols is absolutely necessary; on such occasions a member of the Leadership Group should sanction it.

Consumables

Consumables cover such items as toners, ink, etc. The print management system means that toner is replaced automatically, except for a number of standalone printers. Please refer to the section on 'Printing' for further information. Departments and other cost centres will receive a one-off charge at the start of the financial year to cover the cost of consumables. This charge is monitored on a yearly basis and is dependent on the previous year's usage.

Copyright and Intellectual Property Rights

All materials that are saved on any of our ICT systems must follow copyright and intellectual property rights. If you are in any way unclear or unsure as to if such rights are being adhered to, please refer to the following web links: https://www.gov.uk/intellectual-property-an-overview & https://www.gov.uk/topic/intellectual-property/copyright

CPD

Please refer to the following colleagues, depending on your need:

- The IT support team for specific training needs in relation to hardware or software.
- Data Manager for training related to our SIMS database

Data: SIMS and School Databases

All such data is strictly private and confidential and as such we all have a duty of care to ensure that it is used and accessed safely. If you are accessing SIMS from home, please ensure you are the only individual privy to this data and do not leave such data unattended. This also applies to the work place i.e. do not leave a work station (user screen) unlocked and unattended where other individuals (e.g. students, visitors, parent/carers) could see such data.

No personal data (staff or student) shall be taken from the school unless it is on encrypted media. This includes, but is not exclusive to, laptop computers, netbooks, external hard disks, memory sticks, smart phones and other removable media.

Data Security

All of our computers are set to lockout after 10 minutes of inactivity as a security feature. Please note that you will need to log off your PC to make it available to other users, otherwise it stays locked in the first user's name and can not be unlocked by the new user coming into the room. The lockout also applies to the PCs that students use, so please ensure that students log off at the end of each lesson or it will involve one of the ICT technicians coming to unlock the PC; therefore holding up other students. If you have sensitive data on your PC and you need to step away for a short while you will need to lock your computer quickly by

pressing the “Windows logo” key and the “L“ key together. Please do not hesitate to contact IT support if you need any further advice.

Digital Projectors

Some digital projectors give warnings as to when bulbs are going to reach capacity. In these circumstances, please immediately refer it to the ICT Technical Support Team who will make the necessary arrangements to ensure a replacement is purchased as soon as possible. Some older models do not give any warning, so please be aware that some disruption to your use may occur; we will continue to look at ways to minimise such disruption. Please turn off projectors when not in use.

E-mail: Work

We have our own school e-mail system that uses Microsoft 365 and Outlook. This is our default internal communication method. You are advised to check your e-mail account at least twice a day during the school day. The system should be used for all communications – internal and external of a work-related nature. If communicating electronically with students, use your school e-mail account (see other sections within this document for further guidance in relation to such communications).

Please use your school e-mail account appropriately; this includes language and tone. There is an element of personal liability where expressions of opinion are recorded. Any unjustified comment could lead to legal action against the author. If you are unsure about the tone and/or content of an email please contact your line manager or Jeremy Clifton, Deputy Headteacher.

On occasions it is not appropriate for all staff to be sent certain information and “forwarded” emails to others, i.e. forwarded e-mails that include the whole thread of emails. The school e-mail system has many “group lists” already set up within it to make communications quicker for you e.g. heads of department, year teams. If you have any additional groups that you believe would be useful for you or others then please liaise with IT Support.

E-mail: Personal

Access to your personal e-mail account is acceptable, but only outside normal working hours. However, you must ensure that any content viewed is appropriate to a workplace setting where children and young people and other colleagues are present. Do not open any attachments from unknown sources as you may put the school network at risk.

E-mailing students

Each student has a school email account. Please use this when emailing students.

E-Safety Promotion

Please ensure you promote e-safety with any child or young adult in your care. Students should be encouraged not to give out their personal details on any social networking site or in any e-mail. If you become aware of any such incident, please inform the relevant Year Co-ordinator. Please refer to the e-safety policy for further information.

Extremism and Radicalisation

Individuals, groups and organisations with extremist and radicalised views use the internet to exert influence on young people. Staff and students are prohibited from accessing any websites or social network pages that promote such views. The school has systems and filtering in place to block extremist material and monitor those who attempt to access it. Any persons deemed to be accessing extremist material will be reported to the relevant authorities. Refer to the school’s policy on extremism and radicalisation for more information.

Hardware

Hardware relates to any piece of ICT hardware owned by the school i.e. monitors, hard-drives, interactive whiteboards (IWBs), digital projectors, printers, visualisers and any other portable ICT devices such as laptops, digital cameras or mobile telecommunication hand-sets. All hardware owned by the school should be used for work-related purposes by staff and students. As stated, some occasional personal use of e-mail and the internet is acceptable (but refer to advice in this document as to what is acceptable). All hardware should be looked after and this includes ensuring that all ICT kit is turned off at the end of the working day.

Hardware: Damage

If you become aware that any item of hardware has become damaged, it should be reported to the IT Support Team. This will ensure that there is no Health & Safety danger to staff or students. In some cases, the hardware can be replaced by insurance, but not always.

Hardware: Disposal

No item of hardware should be "thrown away"; even if you think it is old and no longer used. The school must follow Government guidelines to ensure the safe and appropriate disposal of such items. If you become aware of an item that you believe to be of no more economic use, this should be communicated to Frank Gordon, Business Manager.

Hardware: Lending

Do not lend any piece of hardware to a student to take home for use. In rare circumstances this may be acceptable, but it should be agreed by Frank Gordon and Jeremy Clifton.

Hardware: Purchase

All pieces of hardware should be purchased via the IT Support team, even if the central ICT budget is not financing such a purchase. This ensures that appropriate checks related to suitability are made prior to purchase and that subsequent procurement, delivery, storage, security marking and installation protocols are followed.

Hardware: Relocation

No member of staff should attempt to relocate or move any non-portable piece of ICT hardware. Non-portable devices can only be relocated by a member of the IT Support Team, due to reasons of insurance and Health & Safety. The IT Support team maintain a detailed inventory of where all ICT hardware is located. If anyone relocates an item, they compromise the integrity of that inventory and this could create real problems related to Health & Safety and/or insurance.

Hardware: Security

All steps should be taken to take good care of all pieces of ICT hardware owned by the school. Portable devices should be locked away when you do not have direct sight of them e.g. laptops.

Hardware: Security marking

All pieces of hardware should have our security marking on them. If you become aware of an item that does not, please refer the matter to the IT Support Team.

Hardware: Staff equipment

Staff may be issued with a laptop or tablet in order to carry out their work function effectively. Staff wishing to undertake school work at home are expected to use the remote access function (see page 5) via a home computer. Please see Jeremy Clifton or Sunny Singh if your circumstances do not allow this and appropriate provision will be made.

Hardware: Taking off-site

There may be times when it is appropriate to take pieces of ICT hardware off-site by members of staff. On such occasions the appropriate permission must be obtained. This involves communicating with Frank Gordon and the completion of relevant paperwork.

Information Screens

There are several large TV screens situated around the school site. We use these screens as one of our means of communicating with students; namely for relaying key information to them for the day, upcoming events and activities and as a means of sharing and celebrating their individual successes.

Internet: Staff

Using the internet on any piece of ICT hardware connected to the school should be done for work-related matters. You cannot use the internet (on any piece of our hardware) for: gambling, accessing pornography and/or indecent images, accessing extremist material, to incite any form of discrimination, to conduct any personally-run business matters, share-dealing, religious and political causes or beliefs, playing games, harassment or accessing social networking sites. Some occasional use of the internet for non-work-related matters is acceptable outside of school hours. However, it is important to note that all such activity is monitored and disciplinary action could be taken if the school deems such activity to be inappropriate or not covered by our Guidance for Safer Working Practices for adults who work with children and young people in education settings.

Internet: Students

If you become aware that a student is using the internet inappropriately, please report it to the IT Support Team. Inappropriate use follows the same guidelines as for staff. Students should not be accessing social networking sites.

Internet Sites

There are many occasions when you may wish to access a particular site to facilitate learning and teaching. On such occasions, all such content should be related to the curriculum and appropriate to the age group concerned. If you need advice as to whether a particular site is appropriate, then please liaise with your Head of Department. In short, students should not be exposed to unsuitable material or web-links on the internet. You must not access the internet for personal use in lesson time.

Monitoring

All activity on our ICT systems is monitored. The school is aware that the interception and monitoring of electronic communications is unlawful. It is lawful if the sender and recipient are aware that such monitoring will take place and/or there are lawful exemptions that will prevent or detect a crime and/or we need to investigate or detect unauthorised use of the internet. Therefore, this document acts as a means of communicating to you that such interception and monitoring will take place. Where we become aware that guidelines in this document are not being adhered to and there is misuse, we will adopt the London Borough of Redbridge's Personnel Procedures. These procedures cite that most serious misconduct activities can lead to disciplinary action and possible dismissal.

Online Bullying

This is where ICT is used deliberately to cause someone harm, distress or upset. There are some unique features of online bullying less present in more traditional forms of bullying – the immediacy, the absence of interactions, the absence of a safe home environment and the anonymity. As part of our Pay and Conditions of Service, it is our duty to ensure, as far as possible, that students are free from bullying and harassment – online or otherwise. If you become aware of any student involved in online bullying using hardware owned by the school, their own mobile device, or from/at home, then this should be reported immediately to the relevant Year Co-ordinator.

Personal Privacy (internet and e-mails)

You cannot expect absolute privacy on any ICT system within the school. Monitoring takes place, so please bear this in mind when using our ICT systems.

Print Management System

We have a fleet of printers that use 'follow me' technology. You will need to undergo biometric registration or obtain a pin code before use. There are a number of additional printers in offices and departments. All printers are monitored for usage. Toner is replaced automatically, except for a handful of standalone printers. Please contact IT support for further information. Printing should be restricted to work-related matters and not for personal purposes.

Reporting Misuse

Should you become aware that there has been a departure from the various guidance sections in this document, you should report it immediately. The nature of the departure will dictate the person that you should report it to. If the issue is related to a student or group of students, please follow the guidance within the 'Sanctions' section. Where the Network Manager is in direct receipt, they will decide whether it is appropriate to escalate this to a member of the Leadership group and/or middle leader. If the issue is related to a colleague or group of colleagues, please refer it to the DHT with Strategic Oversight for ICT (Jeremy Clifton) who will deal with it directly or escalate the matter to the Head Teacher as appropriate. Obscene material involving children will be reported to the police.

Reporting Inappropriate Material

Should you see any material that is inappropriate on any of our e-communication tools, e.g. the website, information screens etc., you should report it immediately. You should detail what you have seen (text and/or images) in a written e-mail to our IT Support Team. You should also copy in the DHT with Strategic Oversight for ICT (Jeremy Clifton). Corrective action can be taken immediately. Obscene material involving children will be reported to the police straight away.

Sanctions

If you become aware that a student has engaged in anything that is clearly unacceptable (as detailed in our Student Acceptable Use Policy), you must follow it up using our standard procedures. There are occasions when certain behaviours need to be reported to the IT support team. Year Co-ordinators: please be aware of this and ensure that the Network Manager is made aware as soon as possible to take action as appropriate. Teaching staff: please see the code of conduct for appropriate sanctions.

Saving Files

Save files on a regular basis. All files should be saved on your Home Drive (U Drive) or in OneDrive. Files that you wish to share with other staff should be saved in pigeon holes (T-drive) or shared via OneDrive; files to be shared with students should be saved in the shared area (P drive). Please note that no files should be saved on to individual desktops; such files could be lost, so please be aware. All files on the school network drives are backed up regularly.

School Website

Our website address is www.woodbridgehigh.co.uk It is the home page whenever you log onto the internet from a curriculum network work station. It is very easy to set it as the home page on other work stations. The school website is another useful communication tool for parents/carers, students, governors and staff.

Please contact the data office if you would like to publish information on the website or if you notice that something is out of date.

Software: Copying

School licensed software must not be copied; making copies without permission is an infringement of copyright law. Where we become aware these guidelines are not being adhered to, we will adopt the London Borough of Redbridge's Personnel Procedures.

Software: Installation

You should not install or attempt to install any piece of software on **any** piece of ICT hardware owned by the school. It must be referred to our IT Support Team. A member of the IT Support Team will ensure that the appropriate safeguards and licensing arrangements are in place.

Software: Licences

These are held centrally by the IT Support Team. They should not be held by individuals or within departments.

Software: Purchase

It is acceptable to purchase new software from individual/department cost centres but the purchase should only proceed if the software has been deemed appropriate by the IT Support Team and DHT with ICT Oversight (Jeremy Clifton). The IT Support Team maintains a software register.

Staff ICT Acceptable Use Policy (AUP)

All staff should read and sign the AUP at the start of the academic year or, if new to the school, as soon as they start working at Woodbridge.

Student ICT Acceptable Use Policy (AUP)

All staff should support the contents and promote its positive application; a copy of the AUP can be found in student planners. Please communicate this with your tutees. Year co-ordinators: for any casual admissions, please ensure that the student understands the document. Please also read the 'Sanctions' section for further guidance in this area.

Turning off Digital Projectors, Hard-drives and Monitors

Staff should ensure that all digital projectors are turned off when they are not in use, or at the end of the day. You will compromise their use if you do not follow this advice. Please also ensure that all hard-drives and monitors are appropriately logged off and shut down when not in use and at the end of the day. Once again, if you do not, you compromise their use in terms of reliability, but also it can present a security risk in our non-working hours.

USBs

USB devices cannot be used with school hardware in order to prevent viruses entering the system. Please use alternative, cloud-based methods to save work, such as Dropbox, Google Drive or OneDrive. Any USBs containing school data must be encrypted.

Usernames and Passwords: Staff

Usernames and passwords are needed to access most ICT systems in the school – sims.net, school e-mail accounts, the curriculum network, remote access. Communicate with the Data Manager regarding SIMS and the Network Manager for the curriculum network, remote access and the school e-mail account (as they are the same). In cases where you set your own password, passwords should not be easy for others to guess - ensure passwords contain letters, numbers and special characters, and are at least 7 characters long. It is an offence under law to access or use another person's username and/or password. Do not let anyone else use any of your usernames and passwords on any system.

Usernames and Passwords: Students

Usernames and passwords are needed by students to access the curriculum network and the MLE. If for any reason a student does not have a username and/or password for either of these systems, they should be directed to the IT Support Team. Students should be encouraged to set passwords that are easy for them to remember but not easy for others to guess – they should try to ensure passwords contain letters, numbers and special characters, and are at least 7 characters long. It is against our student ICT code of conduct for any student to access or use another person's username and/or password, and students will be told not to let anyone else use any of their usernames and passwords.

Viruses

We have relevant protection in place, but due to the nature and emergence of viruses, some can find their way onto our networks. So, if you are using removable devices, always check before you access saved files that no virus is on them. If there is, immediately disconnect and refer the issue to the IT Support Team.

Approval: Approved via Full GB Chair's Action on 10th September 2024 in advance of the F&GP Committee Meeting on 8th October 2024.

Date of Next Review: Autumn 2025

Reviewer: Mr J. Clifton (Deputy Headteacher)
