The Windsor Boys' School

ICT Acceptable Use Policy

ICT Acceptable Use Policy

Contents

Appendix

1 Introduction

This policy sets out the acceptable use of Information and Communication Technologies within The Windsor Boys' School.
Copies of this document are available on the school website and on Firefly.

2 Definition of Terms

The following terms are used in this document and relate to the following:

Network User – any person that uses the schools network infrastructure.
Staff – any employee of the school or visiting consultant, adviser or other visitor to the school.
Student – any person who attends the school for education purposes
Hacking – any attempt to bypass any of the school network's security features
The School – The Windsor Boys' School
AUP – Acceptable Use Policy
VLE – the schools virtual learning environment (Firefly)
Laptop/Device/iPad/Tablet/Computer – these terms are used interchangeable and refer to a connected electronic device.

3 School-wide policies and procedures

The Schools Acceptable Use Policy (AUP) is part of a suite of documentation which covers the safe and legal use of ICT within the school. These include child safety, anti-bullying, health and safety, data protection act, fair processing, mobile phone, social networking and copyright.

Use of ICT is monitored within the school, and cases of misuse by staff and students will be reported to the Headteacher. A log of any incidents is kept on the students' information system or in staff files. The AUP will be reviewed annually, and action taken if a need for change is identified.

Although some classes use the ICT facilities within the school more regularly than others it is the class teacher's responsibility to check the ICT Classroom prior to use and before exiting. Every reasonable attempt should be made to ensure that equipment is not damaged or removed. Where instances of loss, damage or faulty equipment occur, please contact the ICT Support Manager via Helpdesk@TWBS.co.uk

4 Communication with parents and carers

Parents are contacted directly where concerns exist regarding improper use of the Internet or schools ICT equipment. Improper use may result in students being banned from using the system and other disciplinary measures may be taken depending upon the nature of the abuse (e.g. Exclusion from school).

All emails/communication/documents/etc. must be thought through and entirely professionally worded.

5 Acceptable use guidelines for staff

Any school computer equipment or service utilised by a member of staff is provided for the primary purpose as a work tool, for work related duties only. It must not be used to conduct a personal business/enterprise or for personal gain or to access/store any information/media/photos/files that could be seen to be inappropriate on the device. Any electronic communication with other members of the school must be made using the internal school systems taking in to account that all communication/files must be of a professional nature.

Staff must keep their passwords secure and make sure their passwords are of significant strength. They should include a mixture of upper case, lower case and numbers to make it difficult for anyone to guess. Passwords must not be given to any other members of staff or students at any time and care must be taken when typing in passwords to a device/computer/laptop to make sure that no other person can identify the password or pin code. It is recommended that passwords are at least 8 digits in length and a mixture of lower and upper case letters, together with a mixture of numbers, letters and symbols. Please do not use the same password or pin as personal mobile devices.

Staff are responsible for the security and acceptable use of their laptop/device/network account. Staff must ensure that their laptop and other computer equipment is stored securely when not in use. Staff must not keep passwords with their laptop. If a laptop is lost or stolen, a report must be made to the Police. Staff must provide the Police with a

phone number for ICT Support so that the equipment's serial number can be provided. ICT Support must be provided with the crime reference number for insurance purposes.

Laptops store their files on their own internal hard discs which require backing up to the network on a periodic basis. The system will remind the member of staff when this is due but it is the responsibility of the member of staff to make sure this is carried out. Should a hard disc fail and no recent backup exists ICT support may not be able to rescue damaged files. In relation to devices such as smartphones or tablets any important documents should be emailed securely to your own school account to keep them safe should the device fail. Documents on personal devices are still the property of the school and should still be kept securely according to school policies and the law. Note that deleted documents may still be help on the device or a third party system such as email in clear text.

Staff are expected to maintain reasonable care with all portable equipment. This includes taking measures to ensure that the equipment is transported in a safe and secure manner. Staff should be aware that all portable equipment is insured whilst in school or at home via the schools insurance where forced entry can be proven. The school's insurance does not cover equipment which is left unattended in a motor vehicle so do not leave equipment unattended. Staff must not keep 'personal information' or 'person identifiable' information on their laptops in case of theft – data such as contact details etc. should not be stored on laptops.

The Windsor Boys' School laptops have been unlocked to allow the user to install software that can be used for school purposes. This is to encourage innovation and development of practice in the classroom. If you unsure whether software should be used, or require assistance to install it, you should contact the ICT Support team. Any software designed for personal use must not be installed onto the school laptops.

ICT Support will maintain a software audit, containing a list of the software installed on each computer or laptop. This audit will be made available to any official body who require it for the purposes of copyright enforcement. The use or copying of software without the licensor's permission is illegal and equally the terms and conditions of software licenses must always be adhered to.

The copying of music files, video and other copyright material if not legally purchased by the member of staff onto school computers may be illegal and removed if discovered. This will be reported to the Headteacher and further action may take place. DVD's may only be played to an audience if it is within the terms of their license agreement. School mobile devices may be locked to not allow such content in which case no member of staff should circumvent this setting.

Whilst it is the user's responsibility to take reasonable care over the configuration of their computer hardware, it is possible for software to be installed on a machine without the full comprehension of the user. Users discovering software that has been installed in an unsolicited manner and which contravenes the licensing regulations above must contact ICT Support who will assist in resolving any issues.

The school has the right to seize/reclaim any laptop or computer or other school device without explanation. ICT Support have the ability to view all files on the network and devices but are prohibited from doing so without permission from the Headteacher or Chair of Governors permission.

Staff are responsible for backing up data when they end their employment with the school. Staff must be aware of the Data Protection Act and are prohibited from taking copies of any personal data about students or other members of staff or any other creative works produced or derived whilst under contract to the school unless with the written permission of the headteacher and document owner.

No use of personal email/social networking systems/mobile messaging etc. should ever be used to communicate with students of the school for child protection and staff protection (e.g. allegations against a member of staff etc).

All emails/communication/documents/etc. must be thought through and entirely professionally worded.

Staff should also follow the Acceptable use Guidelines for Students as detailed in Section 6 and against the safe use guidelines in section 10.

6 Acceptable use guidelines for students

Students:

- Must only use their own user area and not attempt to access other user's files or attempt to impersonate another user in any way.
- Must keep their passwords secure and make sure no one else knows it. Passwords are used on public facing systems likely to be targeted by hackers and should be strong and not be easy to guess.
- May only use the computers/devices for school work or home study.
- May use flash drives or other media if installed on the computers, but only for purposes of transferring or saving their work. Note that responsibility still applies for files remaining on the media or not fully deleted.
- Must only send e-mails/messages to people known to themselves or with the permission of a member of staff.
- Must only send e-mails/messages that are polite and responsible and must not contain any personal information about themselves.
- Must report any damage to a member of staff immediately
- Must only use the school email/messaging system for school related messages.
- Must report to a member of staff any inappropriate messages they have received. All information will be treated in the strictest confidence.
- Must report to a member of staff any inappropriate website, image or video clip if they discover one is accessible from the schools computers.
- Are subject to checks of their computer and Internet usage. E-mails/messages may also be monitored.
- If students fail to abide by the above conditions, their Internet access will be blocked at the discretion of a senior member of staff. In severe cases network access may be removed.
- Must not attempt to breach the schools network security, intrude into other peoples 'e-space' or attempt to take the identity of another user (e.g. use another students username)
- Students must not contact staff via any 'personal systems' such as texting a member of staff or sending a message to a member of staff's personal account. Students can view the schools social network policy via the school website.

7 Data Protection Act

Personal Data is collected, stored and processed in accordance with the principles laid out by the Data Protection Act. We will take every reasonable precaution to protect information and ensure that it is relevant, accurate and up to date. Appropriate physical, electronic and procedural safeguards are in place to ensure the security, integrity and privacy of all information kept in our electronic and paper records and during communication with accountable and acceptable third parties. The need for confidentiality will be respected, and sharing of data will only occur with the permission of parents/carers in line with our fair processing notification. All 'personal data' will only be allowed out of the school with the knowledge of the Headteacher.
If it is suspected that data has been collected, stored or processed inappropriately or a process requires a change in order to better safeguard personal data then please inform the Headteacher.

8 Computer Misuse Act

Anyone attempting to gain access to a school computer, application or program, or data to which they do not have authorised access will be criminally liable under the Computer Misuse Act.

This act is far reaching and covers all conceivable ways to attempt to guess a password as well as what is commonly known as hacking and phishing. It also covers observing someone entering a password or distracting them once they are logged in or using a program to impersonate that person or a system for the purpose of gaining access to a system/data.

If such an act or attempt is suspected then inform the Headteacher as it is a very serious matter.

9 Internet safety skills development for students

Students are made aware through ICT and Citizenship/PSE of their rights and responsibilities with regard to their use of ICT based technology. This includes issues such as cyber bullying, personal safety, data security and sexting. Whole school activities promoted internet safety will be provided for all students across the year.

10 Personally Owned Equipment

Students may bring personally owned equipment (Laptops, Cameras, Tablets etc.) into school but must be aware that they are not covered by the schools insurance and are brought in to school at the owner's risk. If personally owned equipment is brought into school it is down to the member of staff in charge as to when/if the equipment is allowed to be used within lesson time. Students must seek the permission of the member of staff in charge of the class before using the equipment. Should equipment use be abused or inappropriate use be discovered within school the students right to bring in such equipment into school may be revoked and disciplinary sanctions may be used dependent upon the nature of the abuse.

If personally owned equipment is used within school it should not be used to make recordings (video and/or sounds) of others if the other parties permission has not be

sought prior to the recording. Such recording is taken seriously as it may constitute an invasion of personal privacy or breach other laws and school polices especially if it were to appear on social media or in the public domain.

The school reserves the right to confiscate any such equipment and it will be held securely until a parent/guardian is able to pick up the equipment from school. Any personally owned equipment must be used in accordance to this acceptable use policy.

Students should be aware that any work undertaken on non-school equipment or stored on memory sticks (or other removable media) is not backed up by the school system. Students must ensure they take adequate steps to back up their work to prevent loss of work and particularly any vital coursework.

11 Using the technologies safely

All users of the schools systems (staff and students) must be aware that any electronic communication or document is open for public access/accountability and scrutiny via such legislation as the Freedom of Information Act.

All emails/communication/documents/etc. must be thought through and entirely professionally worded.

11.1 Internet

All Network Users must use their own network account to logon to the network. The School's auditing software automatically records the address of all websites accessed and this information can be retrieved by ICT Support. All Internet access is filtered. Despite all reasonable steps being taken if an unsuitable content is discovered this should be reported immediately to a member of staff or ICT support. Attempts to bypass the filtering system are strictly prohibited and may result in a user's Internet access being removed.

ICT Support have access to an unfiltered access for testing purposes and its use is governed by this AUP. Use of the unfiltered access must be sanctioned by the Headteacher and ICT Support Manager

11.2 Email and Messaging

All Staff and Students have an individual email account. All Network Users must use their school email account for all school related correspondence.

Staff should be aware that, where necessary, their email account may be monitored by the ICT Support Manager. Staff should immediately report any inappropriate emails they receive to the Headteacher or ICT Support. ICT Support may be involved in extracting emails from the server.

Students and staff should be aware that their school email account may be monitored, either randomly or where any suspicion has arisen. The random monitoring of the accounts will be done by ICT Support.

Where suspicion has arisen, the ICT Support Manager will be responsible for reviewing the emails, and ICT Support may be involved in extracting the emails from the server.

The schools email system will monitor against a set of banned words for any messages including these words being 'referred' until either accepted or rejected by ICT Support.

11.3 Webmail

Webmail is available via the schools email system, enabling users to access their email account from any computer with Internet access. The webmail is a publicly accessible website and as such users must ensure that they have strong network login passwords in place to protect against unauthorised access.

11.4 Spam and Spoofing

The School uses a mail filtering service. This service reduces the amount of spam and spoofing emails but users should still be aware on how to recognise spam and spoofing emails and delete them immediately without opening them.

Spam refers to unsolicited email – email that is sent without your permission, usually offering medication or other products such as computer software at lower prices. The subject of a spam message is usually designed to attract people to reading it and therefore you may see subjects such as 'Hot Stock Notice' or 'OEM Software'.

Spoofing refers to an email which claims to be from a bona fide company, such as a bank, requesting that you visit 'their' website and confirm your details. Email subjects will often be similar to 'Regarding Your Online

Account' or 'Confirm Your Internet Banking Records'. These sites do not belong to the company they claim to be from and subsequently use your details to access your bank account. A genuine organisation would never ask you to confirm details in such a manner.

Any file attached to a suspicious email or obtained via a link within the email is likely to have an entirely plausible name but be a .zip or .exe or .scr file. These may be Trojans or viruses that can be used to gain access to secure data on the system and so should not be opened or previewed or saved in any way. If in doubt contact ICT support.

11.5 Social Networking Sites and Chat Rooms

Staff and Students should not access social networking sites or chat rooms on the school network unless these systems are owned and or managed by the school (e.g. The schools VLE system).

Should Staff or Students wish to set up a social networking site or visit a chat room (or similar) in their own time outside of the schools IT system, they must ensure they do not give away any personal information, such as address. For their own protection, the school would like to remind all students to never upload a photo along with their full name or personal details such as which school they attend.

The School regularly monitors websites to discover any inappropriate material about the School, Staff or other Students and will take appropriate action where necessary.

Students and Staff should make themselves aware of the schools E-Safety Policy which is available on the school website.

11.6 Instant Messaging

Student users are unable to install software and the use of websites offering an alternative are not to be accessed.

11.7 Webcams

Where video conferencing/webcams are used within school, it must be with an authorised third party and overseen by a member of staff. If webcams are used within school it should be with permission of the member of staff in charge and should never be used to record people if they are unaware of the recording.

Staff and Students should be aware that certain viruses and Trojans do exist which can activate a webcam without the owner's permission.

11.8 Peer-to-Peer (P2P) Networks

Staff and Students are forbidden from connecting to and/or downloading data from peer-to-peer networks. Peer-to-Peer networks (such as LimeWire, BearShare or Morpheus) often contain copyrighted content, viruses, spyware or other inappropriate materials and users should be aware that downloading files from a Peer-to-Peer network may be illegal or compromise their computer.

12 School websites

The school has its own website. It is the responsibility of the staff member or pupil creating the content for the website to ensure that all materials do not infringe the intellectual property rights of others. The Headteacher will take all reasonable steps to ensure that material created by the school is protected under copyright. The ICT Support Manager or website owner will ensure that the website is regularly checked for inappropriate content or material and that access to the website server and databases are suitably controlled and secured.

The school cannot be held responsible for the content of external sites, even if they are linked to from the school website.

13 Use of Student Photographs

Students will have their photographs taken both formally (by school photographers and for use on the schools information systems) and informally (for example trips/visits or around school during activities). If photos are to be used for media/website/publications/newsletters then parental permission must be sought.

Parents are asked for permission when students enter the school and yearly with information update forms. Students that have no permission or have 'exclusions' (such as not using on the web etc.) can be identified via the Photograph Permission List on SIMS, in Staff Only and on Firefly. If exclusions exist or permission is denied then

contact should be made with the parent to seek permission – if permission is not given in writing (form available from Exams and Data office) then the photo must not be used.

Parental Permission is required even for students that are over 18 years old.

14 IP and Copyright

All work carried out on the school machines during the school day remains property of the school. Work carried out at home on the school network also remains property of the school.

Learning, teaching and course materials produced by staff while working at TWBS must not be published or commercially exploited without permission from the School. However, staff may use such materials which they produced themselves for their own teaching and research purposes outside TWBS (including use in future employment), provided:

- The use is non-commercial; and
- Any logos or other text or markings which might suggest an association with TWBS are removed.

When using works produced by other people inside or outside TWBS ("third party material"), staff and students must ensure that intellectual property rights are respected and that any conditions imposed by the School's copyright licences are met.

Staff who produce works in the course of their employment which they think are capable of being exploited commercially must inform TWBS, and must not exploit the work without the School's permission.

Appendix i

ICT Use Frequently Asked Questions

Introduction

The purpose of this frequently asked question sheet is to give generic examples of acceptable and safe use of the schools ICT systems in accordance with the schools ICT policy. If at any point you are unsure as to what is acceptable or safe then please contact the schools ICT support office who can advise.

Q: **A student has emailed me from their own personal email address (eg. Hotmail, Googlemail). Can I respond to that email address?**

A: **You should reply to that students' school email account (ending in @twbs.co.uk) and not enter into communication using the external system.**

Q: **A student has asked me to be their 'friend' on Facebook (or other social networking site/online gaming system – Xbox etc). Can I accept them?**

A: **No – you should not make contact with students via any social networking site or messaging system (such as MSN messenger, Windows Live Messenger, text messaging, etc). Any such contact should be reported to the ICT Support Manager or Headteacher so follow up can occur with the student. You should also read the schools e-safety policy which is available from the schools website.**

Q: **Can anyone request my communication/files/messages? Do I need to keep my communication/files/messages professional at all times?**

A: **Yes - All users of the schools systems (staff and students) must be aware that any electronic communication or document is open for public access/accountability and scrutiny via such legislation as the Freedom of Information Act. All emails/communication/documents/etc. must be thought through and entirely professionally worded. It must be assumed that all emails/communication/documents/etc. will exist forever either as deleted files or on backups or on third party systems such as email repeaters and may become subject to legal or public scrutiny.**

Q: **Students are doing a presentation from my laptop/device and need my password to logon/remove screensaver. Can I give it too them?**

A: **No – your password has access to highly sensitive information and must be kept secure. Passwords should include a mix of uppercase letters, lowercase letters and at least one number to make sure they are secure. Care must be taken that when entering your password/passcode/pin that no other person is watching to try and obtain it for later use.**

Q: **I have been asked by an external contact/agency to provide them with a list of students in a year group. Can I send them this information?**

A: **No – any personal information going to external parties must be agreed by the Headteacher and the data owner. Information is protected under the data protection act. The school must have regards to this before transferring information to any external party.**

Q: **Can I take my laptop/tablet/device home?**

A: **Yes – you can take it home and join it to your own internet connection if desired. However, the laptop/tablet/device is for school use and must not be used to conduct a personal business/enterprise or for personal gain (tax implications may exist). The laptop/tablet/device must be transported securely and safely. Insurance will only cover the laptop it is locked away out of sight when transported. Where a device has been locked by ICT support no attempt should be made to circumvent the security in place. You must make sure that the device is not used to access any illegal or inappropriate content when connected to your own internet connection – if any such content is discovered this will be referred to the Headteacher who is likely to enact the schools disciplinary procedures (staff and students)**

Q: **Who is responsible for backing up my laptop/device?**

A: **You – Laptop drives do go wrong and ICT support can only get back what exists on your last backup. Staff must ensure that they do this regularly. If you have important files on other devices (mobiles/tablets etc) please regularly email these documents securely to your school email account to keep a copy off the device.**

Q: **I am working with a student and they could benefit from using my device. Can they do this?**

A: **When working directly with students they can use your device but only under your direct supervision so you can ensure that they do not use the device to access anything they should not view such as your email or an area of the network that is only for staff; or that they install additional software or reconfigure the device unawares.**

Q: **Can I install my own software (personally owned or purchased) on to my laptop/device?**

A: **Yes – The laptops have been left unlocked for staff to install school specific software onto the machines. This must be for school use, and not for any personal uses. It is the staff member's responsibility to ensure that the software is appropriate, and does not violate any copyright issues. If you are unsure or need help to install, please contact the ICT Support Manager.**

Appendix ii

Laptop/Device Loan Agreement

The Windsor Boys' School Staff Device/Laptop Loan agreement.

Device Make:

Model :

Serial Number :

Laptop Name:

Date:

The laptop/device detailed above is loaned to _____ for the duration of their employment at The Windsor Boys' School subject to the following terms and the schools ICT policy. The laptop/device must be returned to the school on ceasing to be employed at the school or if required during a planned absence.

1. The laptop/device is for the work related use of the named member of staff to which it is issued.

2. The laptop/device remains the property of The Windsor Boys' School throughout the loan period. However the member of staff to which it is issued, will be required to take responsibility for its care and safe keeping.

3. The laptop/device is covered by The Windsor Boys' School Insurance, when at home or school, providing it is not left unattended.

4. If left unattended the laptop/device should be in a locked room or secure area.

5. Due regard must be given to the security of the computer if using other forms of transport.

6. In order to ensure the schools compliance with the Data Protection Act and to avoid breaches of confidentiality: under no circumstances should students be allowed to use the staff laptops/devices if not directly supervised by a member of staff. Staff should also be cautious when using the computer away from school particularly with files which may contain personal, person identifiable or student data.

7. The laptop/device will be recalled from time to time for maintenance / upgrade and monitoring.

I have read and agree to the terms and conditions in this agreement.
I undertake to take due care of the computer and return it when requested.

Signed:_____

Date:_____

Appendix iii

Staff Acceptable Use Policy

ICT Code of Conduct

Staff, Governors and Visitors
Acceptable Use Agreement / ICT Code of Conduct

ICT and the related technologies such as email, the Internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the school E-safety coordinator.

I will follow the Acceptable Use Policy in its entirety and specifically:

- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.

- I understand that it is a criminal offence to use a school ICT system, including a school issued laptop, for a purpose not permitted by the school or to attempt to gain access to such systems and data.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes, or for uses deemed 'reasonable' by the Headteacher or Governing Body.

- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.

- I understand that I am responsible for all activity carried out under my username.

- I will ensure that all electronic communications with students and staff are compatible with my professional role.

- I will only use the approved, secure email and phone system(s) for any school business.

- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or Governing Body.

- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

- Images of students and/or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school without the permission of the Headteacher.

- I understand that all my use of the Internet and other related technologies can be monitored and logged and may be made available, on request to the Governing Body.

- I will respect copyright and intellectual property rights and all applicable licences/contracts.

- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

- I will report any incidents of concern regarding children's safety to the Child Protection Officer or Headteacher.

- I will ensure that electronic communications with pupils including email and telephone are compatible with my professional role and that messages cannot be misunderstood or misinterpreted. Staff will use a school phone where contact with students is required

- I will support the school's E-safety policy and help pupils to be safe and responsible in their use of ICT and related technologies. I will promote E-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

- I have read and agree with the terms of the ICT Acceptable Use Policy that is available via https://firefly.twbs.co.uk

I will adhere to the provisions of the Data Protection Act, Computer Misuse Act and other laws and policies that may apply whether referred to the AUP or not.

User Agreement and Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Full name (print in capitals) ……

Job title……

Signature…… Date……

Acceptable Use Policy

Reviewed: August 2016

Reviewed by: Mr Richard Corry

To be reviewed: September 2017