Upton-by-Chester

ICT Acceptable Use Policy – Students

To whom does this policy apply?

This policy applies to:

- All students of Upton-by-Chester High School (UBCHS) who have access to School owned devices, or access otherwise any of the Schools ICT infrastructure.

Document Rationale

Upton-by-Chester High School embraces Information Communication Technology (ICT) to enhance its teaching, learning and administration within the School. All organisations that use ICT are required to have a code of practice in place that ensures the safe and lawful use of these systems. This document seeks to outline principles underpinning appropriate ICT use, making expectations clear and ensure all users are fully aware of the consequences of not following the code of practices and computer misuse. Authorised parties referred to in this document are those agreed to by the head teacher.

The purpose of this policy is to:

- Set out the key principles expected of all students of the school community at Upton-by-Chester High School with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of Upton-by-Chester High School.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- Ensure that all students of UBCHS are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

Policy Communication and Update

The Students ICT Acceptable Use Policy (SIAUP) is published on the School's website and sent to parents / carers via electronic communication.

Each student and their parent / carer is expected to read the agreement, sign and return to their form tutor to signify their acceptance of the policy. The process must be completed before the user is given access to their login details. In signing the agreement students, parents and carers also agree to accept any changes made to the agreement which will be re-published on the School's website with details of changes sent out to parents electronically.

Users will also have to accept digitally the terms of this policy when logging onto their profile for the first time. If the terms are denied by the user the computer will not logon to their account.

The SIAUP policy is updated annually, the updated is published on the school website.

Paper copies are available upon request from the Main office or ICT Support Department.

Document Review

This document is reviewed and amended in full annually or when significant changes may occur on the system, by legislation or other factors that may affect the use of ICT within the School. All

changes are ratified by the Headteacher and Governing body.

Training

Students receive information on the SIAUP as part of their induction process. Many curriculum activities carried out also cover the policy as well as educate to better understand the consequences and actions of improper use and how to be a good digital citizen.

Consequences of Improper Conduct

It is expected that all students at Upton-by-Chester High School abide by the terms set out in the Students ICT Acceptable Use Policy.

Failure to abide by the terms set out in this policy will be treated in the same way as any other misconduct issues as outlined in the Schools disciplinary procedure policy.

Illegal activities will be reported to the relevant authorities and if necessary the local safeguarding Children's authority.

User Accounts

Individual

- Each Student at UBCHS has their own account assigned to them.
- Each user accepts full responsibility for the account they are assigned.
- Users are given their network account and assigned a password. This information is stored in a protected area of the network accessible only by authorised members of staff.
- Passwords must always remain secure, must never be written down or disclosed to anyone.
- If a users password is compromised it is the users responsibility to report as soon as they are aware to ICT Support or any other member of staff.
- Users must not allow anyone else to use their account nor shall they use anyone else's account.
- It is strictly forbidden for any student to access the network via a member of staff's logon.
- When moving away from a device users are expected to log off or lock the devices screen.
- Accounts should never be left logged on when unattended.

General ICT Use

- All users at UBCHS are expected to be responsible for using the school ICT systems in accordance with this policy document.
- All students are electronically required to accept the terms laid out in this policy when they logon to the system for the first time.
- All students, parents and carers must sign this document before the student is given access to school systems.
- Use of ICT at Upton-by-Chester High School should primarily be focused on enhancing students learning.
- Use for business purposes or personal gain unrelated to School activities is strictly forbidden.
- The core functions of the School take priority over computer use at all times.
- Accessing, viewing or saving of any form of pornographic, offensive, obscene, violent, dangerous, inflammatory, or illegal material is strictly forbidden. If any inappropriate material is found, the account will be suspended immediately and disciplinary action will take place.

- The School reserves the right to access and check any computer or account at any time.
- Pupils must not intentionally debilitate or disable ICT hardware, systems or networks. Any act carried out by a pupil which compromises this will be dealt with in line with School Disciplinary Procedures.
- Any activity that breaks or goes against the terms set out in the Acceptable Use Policy will be dealt with in line with the Schools Disciplinary Procedures.

E-mail

- All users at UBCHS are provided with an email account with the prefix @uptonhigh.co.uk.
- Use of the e-mail at UBCHS is solely limited to educational activities and should not be used for personal reasons.
- Users can access their email via any web browser, through the Microsoft Outlook App or on any internet connected computer or device via Outlook Web Access both in School and externally.
- Users are fully responsible for their mailbox including but not limited to deleting and archiving items.
- As with any type of correspondence students are advised to beware of the language they use and content of any email they send. Students are advised to always STOP and THINK before they CLICK.
- Users must never send defamatory or malicious information about a person or the School.
- Users are instructed not to send, forward, transmit or print in any form offensive, obscene, violent, dangerous or inflammatory material via email.
- The sending or forwarding of chain letters, jokes or spam is not permitted.
- Personal information, such as home address, age, date of birth etc., should never be shared over email.
- We advise students to remember the following when sending an email
    - Be Polite – Never send or encourage others to send abusive messages
    - Use appropriate language – User are representing the School on a global system. What users say and send can end being publicly viewed by others.
    - Do not reveal personal information about yourself or others – Especially home addresses, personal telephone numbers, usernames or passwords. Electronic mail is not guaranteed to be private.
    - Do not open file attachments you are not expecting – File attachments can contain viruses and other nastiness which can be harmful to both the user and the School.
- Misuse of email will result in disciplinary procedures as outlined in UBCHS discipline policy.

Hardware

General

- All users are responsible for the care and safe keeping of UBCHS ICT equipment.
- It is the expectation at UBCHS that all hardware devices, such as computers and their surrounding areas are kept clean and tidy at all times.
- All portable equipment must be carried in a safe responsible manner.
- All users must keep liquids and food away from ICT equipment and be aware of health and safety hazards related to electrical devices.
- Hardware already in situ must not be moved or re-configured without the express permission of the ICT Support department.
- Under no circumstances are users permitted to unplug or move cables.

- Users are expected to report all hardware related issues to the ICT Support Department.
- Any action that harms or damages any ICT equipment is classed as vandalism. Deliberate or unintentional damage caused by unacceptable behaviour which results in damage to ICT Hardware such as PCs, Monitors, Mice or any other hardware will be charged to the pupils parents.

Damage to the ICT Hardware in School reduces the availability and reliability of ICT equipment as well as impacting on other pupil's abilities and access to essential ICT resources. Damaged equipment will also incur costs to the School, which will reduce the Schools whole School ICT budget allocated to improve on the ICT solution.

Portable School Devices

Some portable devices, such as iPads are provided to students in lessons from a shared supply. Students using these devices are expected to take care of the devices as a shared school resource provided to enable and enhance the learning of all users in the school. Students using the devices must also understand the outlines for software and internet access described in this document.

Personal Devices

- Unless otherwise required, users are requested to turn off their Wifi, Bluetooth or other wireless settings whilst on School premises to avoid signal degradation or conflict of the Schools wireless.
- The use of personal devices is only permitted where activity doesn't infringe on theirs or other users working practices.
- Secondary students with personal devices are only permitted access to the Wifi network if the device is not a smartphone.

Software

- Software used on School Premises must have a valid license agreement, be installed only on computers as per the license agreement and shall only be installed by the ICT Support department.
- Users are not permitted to download or install software without the express permission of the ICT Support department.

In order to comply with the *Copyright, Designs and Patents Act 1988*:

- Unlicensed software is not permitted to be installed on any machines / Devices.
- Pupils must not place any unauthorised applications on the School network.
- Users of ICT are not permitted to copy licensed software for installation on other machines.
- The copying, sending or receiving of pirated materials, such as software or music, is strictly prohibited.

Data

To increase the security of sensitive data Staff and Student shared and personal areas are stored on different servers.

Information or Data should not be disclosed to any third party that is considered sensitive in nature.

To reduce the risk of accidental disclosure students must:

- Lock or log out of their computer when leaving unattended.

- Keep their password secure, never write it down or leave visible and never disclose to anyone else.
- Never display sensitive information or personal data on a public display.

It is a requirement of UBCHS for its users to:

- Never allow anyone else access to their account.
- Never use anyone else's account
- Protect sensitive data with passwords and where possible 128 bit encryption
- Ensure unwanted data is regularly archived or deleted. UBCHS users are fully responsible for the management of their data stored on data servers.

Unauthorised illegal activity

The *Computer Misuse Act 1990* makes it illegal to:

- Gain unauthorised access to a computer's software or data, including the illegal copying of programs.
- Gain unauthorised access to a computer's data for the purpose of blackmail.
- Gain unauthorised access to a computer's data with the intention of altering or deleting, including planting viruses.
- Copy programs illegally.

Any attempt to gain access to data users are not authorised to access for the purposes as listed above (this includes access of the Schools network) is considered an extremely serious offence. To comply with the *Computer Misuse Act 1990* the School will discipline as necessary any user found breaking the law or with material intended to carry out an attack.

Copyright

The School understands its commitment to adhere to copyright laws and has the appropriate copyright license in place to cover an educational establishment. UBCHS holds the PVSL (Public Video Screening License) and is licensed under MPLC (Motion Picture Licensing Company) by the Department for Education. The terms of the licenses cover the broadcast of music and videos as follows:

- The playing of videos is permitted in their entirety providing the publisher falls under either the PVSL or MPLC license.
- Only properly purchased media can be transmitted on the School Site in the form of DVD, CD, and downloaded Media such as those from the Apple Store.
- The transmission of media downloaded from Pirated sites is strictly forbidden and not covered under the Schools License Agreement. Any user found with pirated materials will be disciplined in line with the Schools disciplinary procedures.
- The transmission of content from YouTube or similar Video streaming services is covered under 'Fair Dealing' and 'Exceptions' allowing the limited broadcast of relevant segments of copyrighted works.
- Accessing internet sites that that circumnavigate copyright law is strictly forbidden.

The new 'Fair dealing' and 'Exceptions' added to the *Copyright, Designs and Patents Act 1988* for educational establishments apply to 'in-copyright' works, defined as follows:

- Permission is required to copy or re-use works that are 'in-copyright'.
- The educational 'Fair Dealing' and 'Exceptions' apply only to materials that are 'in copyright'.

- The 'Fair dealing' and 'Exceptions' of the educational aspects allow *limited* use of copyright works without the permission of the copyright owner.
- 'Fair dealing' and 'Exceptions' do not prefer any copy 'rights' on a user; because a user is permitted to use a piece of copyright work in a particular way doesn't give them any copyrights over it - which means they can't copy it on an external drive, put it on a website or add to the school resources for others to use.
- 'Fair dealing' and 'Exceptions' REQUIRE that the creator/owner is acknowledged. UBCHS requires all users to acknowledge the creator and title of resources that they may use in teaching or presenting with.

Data Storage

- UBCHS users are fully responsible for all data stored in their personal areas (home directories). This includes making sure all content is properly licensed and adheres to UBCHS Acceptable Use Policy.
- UBCHS users are made aware of UBCHS data storage limits and file exceptions via electronic communication, their form tutor, e-mail and teaching staff.
- UBCHS users are not permitted to store large data sets such as video and photography on UBCHS data servers.
- The storage of personal files not related to UBCHS such as phone backups and holiday pictures is strictly forbidden.
- The storage of unlicensed, downloaded, copied or distributed music, video or image files on UBCHS data servers is forbidden.
- The School operates a 30 day daily backup system. If a user loses data they must contact ICT as soon as possible if they need the file(s) recovering.
- Data that has not been stored on the system in the last 30 days is unrecoverable.
- It is the responsibility of individual users to understand imposed data limits, backup non networked data and apply UBCHS data policies. Those seeking further information are advised to see the ICT Support Department.

Removable Media and Cloud Storage

- Data stored on removable media such as CDs, DVDs, data sticks and external drives are at greater risk to exposure and are subject to the data protection act.
- Users are only permitted to use cloud storage solutions to store non sensitive information.
- Users using cloud storage solutions to store data used at UBCHS must adhere to UBCHS Acceptable Usage Policy.
- Users are fully responsible for the data stored on removable media or in cloud storage, this includes the size of data, backup and security of that data.
- Users are advised to store large data files such as videos and pictures on external disks, DVDs or cloud storage solutions. Users requiring assistance with this need to seek help from ICT Support.

Internet and Computer Usage

- The School utilises a 200Mb link. The link is filtered via a device hosted in the School.
- All users' computer and internet activity is monitored and logged.
- The filters in place are designed to remove controversial, offensive or illegal content.
- Although best efforts are made, it is not possible to guarantee that all inappropriate material will be filtered.
- ***If any user comes across any inappropriate content they must report it immediately to a***

member of staff.

- Under no circumstances are pupils permitted to attempt to hack the Schools web filter systems or circumnavigate the way they connect to the internet. This includes internet bypass applications that may be used for such purposes.
- Use of the internet is a privilege and should primarily be focused on learning at UBCHS.
- It is accepted that users may occasionally have the need to use the internet for personal reasons. This is permitted as long as it does not interfere with, lesson their work or conflict with any of the codes of practice laid out in this document.
- Use for business purposes or personal gain unrelated to School activities is strictly forbidden.
- Students are not permitted to use the internet for illegal unlawful activity. Any student found breaching this rule will be disciplined.
- Students are strictly forbidden use of the internet to access pornographic material
- Other than for legitimate reasons and at the request of teaching staff for curriculum reasons Students the use of gambling sites is strictly prohibited.
- The downloading of unlicensed material such as music, video, games, documents or other similar files is illegal and not permitted.
- Downloading, sending, printing, display or transmitting material that could cause offence or break the law is strictly forbidden.
- Students are not permitted to access Chat sites.
- Other than for educational purposes, online Gaming sites are strictly forbidden.
- Printing directly from the internet is not permitted. Any content that needs printing should be copied and pasted into a suitable software package first.

Social Networks

- Access to social networking sites is forbidden within School except where special concessions are made by the SLT or for use in a class session or part of a project.

Monitoring

- All computer activity is monitored and logged.
- All internet and e-mail activity is monitored logged.
- All files and e-mails stored on UBCHS systems and OWA are the property of the School. As such, authorised parties have the right to access them if required.
- Network access, web browsing, e-mails and any other activity carried out on UBCHS systems where monitored or logged may be randomly monitored at any time by authorised parties without the user's knowledge.

Printing

- As an eco-School UBCHS strives to reduce its carbon footprint and consumable consumption, printing is a major contributor to both. With the introduction of the Schools new printing strategy eco friendlier devices are now spread around the School in shared areas using a follow-me solution.
- The School utilises a print accounting system which is used generally on student accounts to monitor activity. Any users abusing their right to print, be it personal documents or other non-School related outcomes risks their printing privilege being withdrawn.
- Printing output is strictly limited to School based output only.
- Each printout is assigned to the printing user and logged against the Curriculum Year the user is based in.

- Only work that necessitates a print should be printed. As an Eco-School UBCHS works and encourages its users to utilise email, network storage and cloud solutions as much as possible to create electronic document access.
- The printers' onsite carry a next day onsite support contract. Under no circumstances are users allowed to attempt to fix devices which encounter problems, this will invalidate the terms of the external support contract. Problems are to be logged via the ICT helpdesk only and addressed by the ICT support department only.

Photography and Video

- Students are not permitted to take videos or photos of any member of the School community on personal devices without their prior consent.
- Any videos, photos or audio taken of any of the School community may only be posted to the internet with the prior consent of the person who's Image / Audio was taken.

Wireless (Wi-Fi)

The School provides an enterprise class restricted wireless within the site boundaries. Access to the network is strictly enforced via the ICT Support Department and subject to the following:

- Wi-Fi access is primarily for the use in teaching, learning and administration.
- Wi-Fi access is only granted to Secondary Students who are part of the Schools 1:1 iPads scheme.
- Wifi is provided to Sixth Form users via the Hub.
- Mobiles or smartphones are not permitted access to the schools WiFi without the express permission of the ICT support department.
- Users are asked not to download large files such as video or audio, software updates or any other data type that is bandwidth intensive over the Wifi network. These types of downloads are only permitted to be carried out on School Hardwired machines or outside of the School grounds.
- Permission to access the wireless network must be sought from the ICT Strategic Manager.
- Students are required to inform the ICT support department immediately if they become aware of any access keys or understand any other unauthorised user has access to such keys.