Acceptable Use of ICT Policy

Upper Shirley High assumes the honesty and integrity of its ICT users. Facilities are provided in as unrestricted manner as possible to offer the best possible quality of service.

It is the users' responsibility to ensure that they comply with the policy. The latest version can be found on the school website.

Usage of school systems is subject to agreement to abide by this policy and any breach of the conditions will be dealt with in line with the school behaviour and/or disciplinary procedure:

- A warning
- A removal of access to services and/or devices i.e. internet, email, school computers and mobile devices
- Letter home to parents
- Consequences such as SLT Detention/an official warning added to personnel file

In more serious cases or persistent breaches of this policy:

- Parents called into school
- Report to the school Governors
- Report to appropriate external agencies like the Police, CEOP or Trade Union
- Consequences such as Inclusion/Exclusion for students or disciplinary action for staff

All students must agree to the terms of this policy. Failure to do so will result in no access to the systems. All staff must sign and return this policy where it will be kept on their personnel file. All students starting at Upper Shirley High and their parents will be required to sign this policy prior to starting Year 7.

General Policy

The user agrees not to:

- Upload, download, post, email or otherwise transmit or store any content that is unlawful, harmful, threatening, abusive, harassing, tortuous, defamatory, vulgar, obscene, libellous, invasive of anyone's privacy, hateful or racially, ethnically or otherwise objectionable.
- Impersonate any person or entity, or falsely state or misrepresent affiliation with a person or entity including the forging of headers or to otherwise manipulate identifiers in order to disguise the origin of any content transmitted through the school services.
- Upload, download, post, email or otherwise transmit or store any content that the user does not have the right to transmit.
- Upload, download, post, email or otherwise transmit or store any content that infringes any patent, trademark, trade secret, copyright or other proprietary rights ("Rights") of any party.
- Upload, download, post, email or otherwise transmit or store any unsolicited or unauthorised advertising, promotional materials, "junk mail", "spam", "chain letters", "pyramid schemes" etc. except when directly resulting from curriculum work.
- Upload, download, post, email or otherwise transmit or store any material that contains software viruses or any other computer code, files or programs designed to interrupt, damage, destroy or limit the functionality of any computer software or hardware; or telecommunications equipment.
- Interfere with or disrupt the service or servers or networks connected to the service, or disobey any requirements, procedures, policies or regulations of networks connected to the service.
- Collect or store personal information about others without direct reference to The Data Protection Act.
- To use the school's facilities to undertake any trading, gambling, other action for personal financial gain, or political purposes unless as part of a curriculum project.
- Visit or use any online messaging service, "chat site", web-based email or discussion forum not supplied or authorised by the school.
- Store or use any software not specifically installed on the service by an authorised person.
- Visit, use, download, or store any game, either application or browser-based, without permission of a member of Support Team or supervising teacher, and only for educational purposes.

The school reserves the right to refer any breach of this policy to the respective tutor/Head of Department and/or member of the Senior Leadership Team. This may result in the suspension of any or all parts of the services provided.

Network Services & Monitoring

This comprises of network access to PCs, Macs, and other ICT equipment in the various classrooms or other areas for all users. Storage of files for all users is available on the file servers. All users shall have complete access to any files they have created, except where ownership/authorship is in question. This is then referred to a member of the Senior Leadership Team.

For reasons of e-Safety, safeguarding and wellbeing Upper Shirley High uses real-time monitoring and control software across the computer networks. Teaching staff have access to the console for student machines for the purposes of monitoring and controlling classes where computer systems are used. This software checks and logs all computer and program activity. It searches for keywords and phrases that could be used for cyberbullying, grooming or other activity that may put children at risk. The software has the ability to disable functionality on client laptops and PCs.

Internet Services & Filtering

All Internet access is logged and actively monitored and logs are stored. Usage reports can and will be provided upon request.

Each user shall have access to the Internet via the school's filters. The filters will screen any unwarranted materials and be updated regularly to maintain this high level of filtering. Any user repeatedly attempting to access such material will have their account locked and it will not be reopened until they have discussed the matter with a member of the Senior Leadership or IT Services Teams.

Should any site or content be discovered which does not comply to the General Policy it will be added immediately. We ask users to assist us with this by informing us of any offending material.

Mail Services

Each member of staff will have an Office 365 account to enable them to send mail internally and externally. It is viewable via the Outlook client or via the Office365 Mail website. Every student will have a Google Apps for Education account to send mail internally and externally, which is viewable via the Gmail website.

You are expected to use email in a responsible manner. The sending or receiving of messages which contain any material that is of a sexist, racist, unethical, illegal or likely to cause offence should not take place. If any user is found to be bulk-sending unsolicited emails to other users within the school or to external accounts, the matter will be referred to a member of the Senior Leadership Team.

Remote Access

Upper Shirley High provides remote access to staff and students via USH Remote. This will enable them to access their documents and some school programs from anywhere they have internet access..

Users are expected to use the remote systems in a safe and secure manner ensuring all data is kept secure and on the Upper Shirley High network storage systems for backup and Data Protection Act 1998 compliance. School data must not be stored on any system other than USH issued equipment.

All USH issued laptops will be encrypted and the IT Services Team will be able to track the device when it is off the school premises. Any attempt to bypass or remove the tracking agents on these devices will be dealt with as a serious breach of this policy.

Printers and Consumables

Printers are provided across the school for use by staff and students. You must use the printers sparingly and for school purposes only.

All printer use is recorded and monitored and therefore if you deliberately use the printer for non-education or offensive material you will be subject to the behaviour management measures of the school.

A printer security and accounting system is in operation across the school. This facility is used to monitor staff and student use. Where students are unable to act responsibly when using the printing services, their use of these facilities will be removed. Staff must not allow students to use their staff badges to access the printers.

Security

Each user will be given a unique username and password that will allow them to access USH network resources, such as email and USH Remote. Students will have a different username for their emails.

Staff will have a separate username and password to gain access to the school's Management Information System (SIMS).

Your username and password are solely your responsibility and are not to be shared with other users or third parties for any reason.

If a user is found using the username and password of another user, their services may be suspended and immediately referred to their respective tutor/Head of Department and then the Deputy Head/Head.

The only programs that may be used within the school are those agreed on by the Senior Leadership Team and/or the IT Services Team. The introduction of any other programs onto the network or systems is not tolerated and will be treated as intentional damage or an attempt to cause damage to school property.

Storage and Safe Transfer of Personal and Sensitive Data

Upper Shirley High holds information on all staff and students. All information about staff and students will be dealt with in compliance the Data Protection Act 1998 and only given to authorised agencies. Information covered by the Data Protection Act 1998 should not be taken off the school site.

Data Security and Retention

All data stored on the Upper Shirley High network is backed up multiple times a day and backups are stored for a minimum of two weeks. If you should accidentally delete a file or files in your folder or shared area, please inform the IT Services Team immediately so that it can be recovered.

Local drives (C:\) on computers and laptops are not backed up and Upper Shirley High will not be held responsible for any loss of data stored on the local system in the event of data loss or hardware/software failure.

Biometric Data

Upper Shirley High uses a thumb print biometric scanner to allow students to purchase food from the canteen. The system does not store the actual image of the thumb, but creates a large numeric file from the thumb image. This numeric file cannot be used to re-construct a thumb print. When a student leaves the school the file relating to their account, and their biometric data is automatically deleted as part of this process.

Mobile Technologies

For reasons of safety and security students should not use their mobile phone or any other technology in a manner that is likely to bring the school into disrepute or risk the welfare of a child or young person.

Mobile phones should be switched off during the school day.

In order to reduce the opportunity for behaviours that could possibly cause upset it is required that students limit their use of mobile technologies to outside of school hours, unless authorised by a teacher for educational purposes.

Students' personal mobile devices are not permitted on the school Wi-Fi network.

If you are sent inappropriate material (e.g. images, videos etc.) please report it immediately to a member of staff within the school.

Treatment of Equipment

The IT Services Team will endeavour to ensure all equipment is in working order.

The school will not be responsible for any damages or loss incurred as a result of system faults, malfunctions or routine maintenance. These damages include loss of data as a result of delay, non-deliveries, mis-deliveries or service interruptions caused by the system or elements of the system, or your errors or omissions. Use of any information obtained via the school's ICT system is at your own risk.

Users are not to tamper with the connections to any of the school's ICT equipment, and should inform the IT Services Team of any faults. Any user who causes damage, either intentionally or through neglect, to any equipment may be refused the right to further use of the equipment and/or may be asked to cover costs towards any repairs or replacements.

All equipment loaned to staff as part of their contract (e.g. staff laptops), or to a student to use externally for purposes of learning will be issued on completion of a loan agreement form. The asset management system will be updated with the loan details and the device will have an agent installed with the ability to track and remotely administer the device. Staff laptops will be and must remain encrypted. The equipment is the personal responsibility of the user and you are advised to check that its loss or damage is covered by your personal insurance.

If you suspect that equipment has any form of virus or malware, you must immediately discontinue use of the equipment and notify the IT Services Team.

Any equipment provided by the school remains the property of the school and should only be used in connection with the aims and objectives of the school and not for personal use. Personal data, programmes or information should not be stored on school equipment and the school reserves the right to remove such data.

If you have any questions about the policy, please contact the IT Services Department.

Policy/Document Owner	IT Services
Last Review	May 2017
Next Review	May 2018