Acceptable Use of IT 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
• Leading to consequences such as SLT Detention / Official Warning added to personnel file.

And 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 at every logon. 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 parents and students starting USH on or after the 2015 intake will be required to sign this policy prior to starting Year 7.

1. 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.

2. 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 School uses real- time monitoring and control software across the computer networks. Teaching staff have access to the console for purposes of monitoring and controlling their lessons where computer systems are used. Staff laptops are monitored however only SLT can access this in the console. 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. This software checks all document types that are opened within school. The software has the ability to disable functionality on client laptops and PC’s.

3. Internet Services & Filtering

All Internet access is logged and actively monitored and logs are stored for at least 1 month. 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 filter 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 ICT Support Team.

The School does not pre-screen content viewed by users, but relies on the filtering software. 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.

4. Mail Services

Each member of staff shall have an Outlook account to enable them to send mail internally and externally. It is viewable via the Outlook client or via the Gateway interface.

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.

Mail sent and received externally shall be filtered for language content and certain file types within attachments. If a user repeatedly sends material that is caught on the filter the matter will be referred to a member of the Senior Leadership Team.

Any user who receives unsolicited mail can inform the network manager who will endeavour to trace the originator and report them to their Service Provider, clearly asking for the originator's account to be terminated if the mail has been in breach of the Service Provider's Terms of Service. Likewise, if any user is found to be 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.

5. Remote Access

Upper Shirley High provides remote access to staff Via the USH Gateway and to Students in the form of our Virtual Learning Environment (Moodle).

USH Gateway will perform security compliance checks at the point the connection is made and if the connecting computer fails the checks their access will be denied. It is the responsibility of the user to ensure the system they are using to connect is compliant with security updates and up to date antivirus protection.

If the loaned device is to be taken off the school site for a prolonged period of time then it is the responsibility of the user to ensure the antivirus and system security updates are kept up to date.

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.

Remote access sessions and file transfers are monitored and logged by the IT Department

All USH issued equipment will encrypted and the IT department will continue to monitor and track the device when it is off the school premises. Any attempt to bypass or remove the monitoring and tracking agents on these devices will be dealt with a serious breach of this policy.

Equipment taken home must be shut down prior to leaving the school premises and stored in a safe and secure place offsite i.e. not in your car.

6. Printers and Consumables

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

7. Security

Each User will be given a unique ID (Username) and password that will allow them to access USH network resources. The same ID and password is used for accessing the school VLE (Moodle).

Staff will have a separate password to gain access to the School's Management Information System (SIMS) and can be changed by request to a member of the Support Team.

The ID and password are solely the responsibility of the user and not to be shared with other users or third parties for any reason.
If a user is found using the ID 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 IT Managers. The introductions of programs (including any software containing viruses or used to disrupt any part of the Network, or connected networks) onto the network is not tolerated

and will be treated as intentional damage or an attempt to cause damage to School property.

8. Storage and Safe Transfer of Personal and Sensitive Data

Upper Shirley High School 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.

Upper Shirley High School will seek to ensure that all personal data sent over the internet will be encrypted or otherwise secure.

In order to use removable storage media on the school systems, the devices/hardware must be encrypted with 'Bitlocker'. Local system policies will not allow data to be written to any removable storage media unless it is encrypted.

9. Data Security and Retention

All data stored on the Upper Shirley High School network is backed up 3 times daily and backups are stored for a minimum of two weeks. Snapshots of the network are also taken throughout the day and backups of the infrastructure are stored both on and offsite. If you should accidentally delete a file or files in your folder or shared area, please inform the ICT department immediately so that it can be recovered.

Files from the users' profile (My Documents, Desktop, My Pictures, and Internet Favourites) are replicated to the network on user logon and log off.

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.

10. 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.

11. 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.

The development of mobile technology is such that mobile phones and other similar devices connected to mobile networks have enhanced features which include: picture messaging; mobile access to the Internet; entertainment in the form of video streaming and downloadable video clips from films, sporting events, music and games etc.

In order to reduce the opportunity for behaviours that could possibly cause upset it is advisable that students limit their use of mobile technologies to necessary communication outside of school hours. In exceptional circumstances students may request permission to use their mobile phone from a member of staff.

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

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

12. Treatment of Equipment

The support team will endeavour to ensure all equipment is in working order. They will set targets for the quality of service they provide, which will be monitored regularly by a member of the Senior Leadership Team

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 Support Team of any faults. Members of staff who wish to receive some training in dealing with immediate repairs may make a request to the Network Manager. Any user who causes damage, intentionally or through neglect, to any equipment may be refused the right to

further use of the equipment and 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. All asset management systems will be updated with user loan details and the device will have an agent which has the ability to track and remotely administer the device. Staff laptops and mobile devices 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 hand it in for checking and cleaning.

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	June 2016
Next Review	12 months