ACCEPTABLE USE OF IT POLICY

Upper Shirley High School

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. People should have an entitlement to safe access at all times.

This Acceptable Use Policy is intended to ensure:

- That people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that everyone has good access to digital technologies to enhance their learning and will, in return, expect them to agree to be responsible users.

Terms of Use

- **Responsibility**: School IT systems must be used in a responsible way, to ensure that there is no risk to your safety or to the safety and security of the IT systems and other users.
- **Monitoring**: The school will monitor use of the systems, devices and digital communications.
- **Vandalism**: Please report any cases of vandalism to the IT support team and appropriate action will be taken by the school to recover any costs for loss or damage. In case of students vandalising any equipment, parents may potentially be asked to pay for any damaged equipment.
- **Personal Use:** The school systems and devices are primarily intended for educational use and you cannot use them for personal or recreational use unless you have permission.
- **Own Devices:** If allowed to use your own devices in school, you agree to follow the rules set out in this agreement, in the same way as if you were using school equipment.
- **Concerns**: If you have any concerns about the validity of an email (due to the risk of the attachment containing viruses or other harmful programmes), please inform the IT support team immediately.
- **Data Security & Retention**: Data is backed up daily**.** If you should accidentally delete/lose files in your folder or shared area, please inform the ICT support team immediately so that they can check if it can be recovered.

DOs	DONTs
• Keep usernames and passwords safe and secure	• Do not share it, or use any other person's username and password. • Do not write down or store a password where it is possible that someone will steal it.
• Be aware of "stranger danger", when communicating on-line.	• Do not disclose or share personal information about yourself or others when online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
• Report any unpleasant or inappropriate material, messages, or anything that makes you feel uncomfortable when you see it online.	• Do not make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
• Respect others' work and property	• Do not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
• Report any damage or faults involving equipment or software, however this may have happened.	• Do not take or distribute images of anyone without their permission.
	• Do not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others
	• Do not use any programs or software that might bypass the filtering/security systems in place to prevent access to inappropriate content.
	• Do not open any hyperlinks in emails or any attachments to emails, unless from a trusted person/organisation who sent the email.

School Specific Systems

Biometric Data

The school uses a fingerprint biometric scanner to allow students to purchase food from the canteen. The system does not store the actual image of the fingerprint, but creates a large numeric file from the fingerprint image. This numeric file cannot be used to re-construct a fingerprint. When a student leaves the school the file relating to their account, and their biometric data is automatically deleted as part of this process. More information on our use of biometrics is available on our website.

Email

The School will provide you with an email address, and the expectation is that you will use this facility for legitimate educational and research activity. 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.

Remember when sending an email to:

- Be polite - never send or encourage others to send abusive messages.
- Use appropriate language - remember that you are a representative of the school on a global public system. What you say and do can be viewed by others. Never swear, use vulgarities or any other inappropriate language.
- Do not reveal any personal information about yourself or anyone else, especially home addresses, personal telephone numbers, usernames or passwords. Remember that electronic mail is not guaranteed to be private.
- Consider the file size of an attachment, files exceeding 25MB in size are generally considered to be excessively large and you should consider using other methods to transfer such files.
- Do not download or open file attachments unless you are certain of both their content and origin. File attachments may contain viruses that may cause loss of data or damage to the School network

G Suite for Education

Students will have a G Suite for Education account created for them. G Suite for Education is a set of education productivity tools from Google including Gmail, Calendar, Docs, Classroom, and more used by tens of millions of students and teachers around the world. Students will use their G Suite accounts to complete assignments, communicate with their teachers, collaboratively create, edit and share files for school related projects. These services are entirely online and available 24/7 from any internet-connected computer.

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 inappropriate 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 Team.

Microsoft Office 365

Each student will have a Microsoft Office 365 account created for them; this is for the purposes of using the Microsoft Student Advantage program to provide all students with access to the latest Microsoft Office applications at both school and home for free.

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.

Network Monitoring

For reasons of e-Safety, safeguarding and wellbeing Upper Shirley High uses real-time monitoring and control software across the computer networks. 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.

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.

Remote Access

The school offers remote access to students, and appropriate use of this technology is important.
The remote access system will enable users 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 school storage systems for backup and compliance. School data must not be stored on any system other than issued equipment.

Any breach or misuse of this technology will lead to disciplinary procedures.

Security

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

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.

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. Students should not attempt to install any programs, any attempt to do so will be treated as intentional damage to school property.

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.

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.

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.

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

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 or CEOP
- Consequences such as Inclusion/Exclusion for students

All students must agree to the terms of this policy and a signed agreement by the parents. Failure to do so will result in no access to the systems.

I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, or when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).	Yes / No
I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to consequences under our behaviour and relationship policy. This may include loss of access to the school network/internet, catch ups, contact with parents and in the event of illegal activities involvement of the police.	Yes / No

I have read and understood the above information.

Student Name:	Year Group:
Parent Name:	Parent Signature:
Date:	