ICT Acceptable Use Policy

Senior Leader Responsible: Mr J Wright
Date of approval by Governors: 1.5.18
Next review date: 1.5.20

ICT Acceptable Use Policy

Access to IT facilities, the Internet and social media must be in support of educational activities and appropriate to the aims of the school. The aims of this policy and agreements is to ensure that all students and staff are clear about what constitutes appropriate use of ICT, the internet and social media, within the school and when using school IT resource and that all users are aware of the possible consequences of inappropriate use, which could include temporary or permanent loss of access to IT facilities, or even result in serious disciplinary action being taken.

All students and staff who access the internet or social media from the school site or using school ICT resources when off site, must be aware that they are responsible for everything that takes place on their computers, tablets or mobile phones and that all activity, including use of the internet may be logged.

BENEFITS

- Access to the internet, email and social media will enable students and staff to:
- Access and explore a wide variety of sources of information to support and enhance the educational experience
- Access curriculum resources and exchange work with staff and other students
- Access webinars, videos and other resources to support the curriculum
- Keep abreast of news and current events
- Take part in live discussions and other events
- Extend the curriculum and be included in initiatives relevant to their education and take part in global educational projects
- Make links with experts
- Publish and display work via websites
- Communicate with other internet users around the world

EFFECTIVE USE

Internet and social media access will be planned to enrich and extend learning. Students will make best use of the internet and social media if:

- They have been given clear objectives for using the internet and social media.
- They have been educated in safe, responsible and effective internet or social media use. They are supervised when appropriate.
- They appreciate and control their internet use, ensuring that they balance learning and they understand and apply safeguarding principles, how to handle themselves safely on-line and how and where to report any Child Exploitation, On-line Protection, counter-terrorism and radicalisation issues.
- They are encouraged to evaluate sources and to discriminate between valid and inappropriate materials.
- They know how to copy, save and edit material from the internet or social media without infringing copyright and data protection.

RESPONSIBILITIES
As a professional organisation with responsibility for safeguarding it is important that staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using technology, they are required to read and sign the Acceptable Use Policy.
It is the student's responsibility to use these resources in a manner that is efficient, ethical and legal. They are required to read and sign the Acceptable Use Policy. The use of ICT resources is a privilege and inappropriate use may result in this privilege being withdrawn.

DATA SECURITY AND PRIVACY
All Data is stored in accordance with provision of the General Data Protection Regulations (GDPR).

SAFETY, SOCIAL MEDIA PLATFORMS AND REPORTING MISUSE
Internet access from the school site is carefully filtered and monitored. Access to inappropriate websites will be blocked, either on a website by website basis or by blocking inappropriate key images, words or phrases. Internet activity on the school premises is monitored and logged. School ICT equipment used off site may be checked for inappropriate use.
In the case of tablets and laptops students, parents and staff have a responsibility to act in accordance with the policy and associated guidance. Appropriate sanctions are in place and will be carried out in the event of misuse.

Staff must obtain permission from Senior Leaders to use any chat room services. Live chat rooms must not be used unless posts are filtered prior to posting.

Social Media
The authorised social media platforms for school use are solely:

- Twitter for departmental, individual staff and extra-curricular activities
- Twitter for whole School use

Staff must not use any existing personal social media accounts for school social media activity. Staff must only use the School accounts for school social media. Any request for a new social media account must be made to the Headteacher for approval. All school social media postings must be professional and appropriate in tone and content. If a member of staff has any concern about a social media posting which they have already made they should contact the Headteacher for guidance.

It is ultimately the responsibility of staff to ensure that they set and convey appropriate standards for ICT social media and internet use. Staff and students should be aware at all times of the potential consequences of inappropriate use of the internet or social media, which could include loss of access to school ICT facilities, disciplinary action and, in extreme cases where misuse could constitute a criminal offence (for example, an incident of cyber-bullying, exchanging indecent images, accessing extreme pornography, extremist/radicalisation material or hacking) will be reported to the appropriate police or child protection authority.

Staff should not 'friend' students or their families on social media unless they are related to them.

Any student who suspects misuse of the internet, social media or ICT facilities by another student must report this to their form tutor or classroom teacher. Any member of staff who suspects misuse of the internet, social media or ICT facilities must report this to their line manager. Any serious or potentially illegal misuse of the internet or ICT facilities such as accessing pornography, cyber-bullying and on site use of internet and school ICT facilities for personal financial gain, or

damaging the reputation of the school through use of social media must be reported to the Headteacher, or in the case of misuse by the Headteacher, to the Chair of Governors. If a child protection or radicalisation issue is suspected, a report should also be made to the Designated Safeguarding Lead.

STAFF GUIDELINES

Staff are advised to use their school email address only for professional use and avoid using it for personal use in order to avoid concerns or accusations of misuse of school ICT facilities.
Staff must **never** allow others to use their accounts and should not reveal their password to others. The Network Manager must be informed if it is suspected that someone else knows your account details or passwords.
Staff must always log off or lock their computer when they finish working. No Personal Identifiable Information (PII) must be visible at any time when the computer is left unattended.

Staff must always implement suitable security measures on portable devices such a PIN or password, fingerprint security, ability to remotely wipe if lost. They should be encrypted and have the latest malware installed. Staff should use Remote Access when off site to work on school work thus avoiding the need for USB pens.

The school network, especially SIMS, can allow staff to have access to confidential information about students and staff. Staff must ensure that such information remains confidential at all times. The General Data Protection Regulations apply to the school, student and staff data. These requirements must be adhered to. Any queries regarding the requirements and implications of the GDPR must be directed to the Data Protection Officer.

Staff must not use school ICT facilities to access inappropriate internet content, for personal financial gain and must only access social networking sites for the purposes of enhancing the teaching and learning experiences for students.

Staff must be aware of and comply with copyright and ownership restrictions when they copy, download or use in lessons any materials from the internet.

Staff must not send photographs, video or audio of students as email attachments nor post photographs, video or audio of students on websites unless they have signed consent to do this from students' parents or carers and the permission of the school leadership team. No student should be identifiable by name. All materials must represent the school in an appropriate way.

Staff must not send data relating to students or any other restricted data to personal email accounts.

When printing confidential material staff must use a secure print method by using a password protected retrieval system. Staff must never walk away from a printer once the password has been entered especially when printing confidential Personal Identifiable Information.

Staff should be aware that email traffic is retained on school servers even if they are deleted from individual accounts.

Staff are not permitted the use of any chat room services.

Staff must ensure that they adhere to all relevant policies and procedures related to, but not limited to Data Protection, safeguarding and professional standards. As examples the following are not permitted: sharing of personal messages, photographs, video and audio, language must always be professional and appropriate. This list is not exhaustive.

Staff are reminded that misuse of the school's ICT facilities, internet or social media to access inappropriate materials or for personal financial gain, or damaging the school's reputation in any

way, could result in disciplinary action being taken, including loss of access to ICT facilities, a verbal or written warning, suspension or dismissal according to school policy. Extreme cases of misuse and all illegal activity will be reported to the police authorities.

Staff have a duty to report all suspected misuse. This should be to their line manager in the first instance. Extreme misuse must always be reported to the Headteacher, or, in the case of the Headteacher, to the Chair of Governors. Any possible child protection issues must also be reported to the Designated Safeguarding Lead.

Staff must not leave portable devices such as tablets or mobile phones unattended.

Staff must not use their own mobile devices to upload to social media / take photographs.

Staff must not use software, systems or devices that circumnavigate school managed internet safeguards including the use of mobile hot spots.

LINKS TO OTHER POLICIES AND DOCUMENTS

Students and staff are reminded that the guidelines and expectations for good conduct in and around the school that are set out in the following policies and also apply to use of the school's ICT facilities, the internet and social media.

- Student Behaviour
- Safeguarding
- Personal Welfare
- Student Code of Conduct
- Teacher Professional Standards
- Data Protection Policy

PARENTAL SUPPORT

All parents or carers should be aware of the concerns and benefits of internet and social media use. Parents and carers are invited to contact the school at any time for advice on safe use of the internet and social media. The school will also provide regular information for parents and carers, for example, through talks on internet safety and the safe use of social networking sites. Links to up to date guidance on these matters are also available on the school's website.

USAGE RULES AND GUIDELINES

Privacy

The school will access student and staff accounts and may review documents and log files in order to ensure that inappropriate use is not taking place. School equipment such as laptops, tablets or mobile phones may be checked from time to time and will be checked on return to ensure that it has been used appropriately.

Software

Students and staff must not download, load or install software, shareware or freeware, nor load any such software from USB pens or other memory storage devices without first consulting and obtaining permission from the IT Team. All software installed must have an appropriate, current licence which must be provided by the IT Technician Team.

Sharing Files

Students and staff must not copy each other's work or intrude in to each other's files without permission. Please be aware of compliance with copyright or downloading any materials from the internet, portable media or memory storage devices.

Backup
The school network is backed up regularly by the IT Technician Team. However, students and staff are also encouraged to make back up files for their work and for work not held on the school network. Students and staff using personal devices such as tablets or mobile phones should ensure suitable backup solutions are implemented and maintained.

Purchasing Hardware and Software
Only the IT Team will purchase any hardware or software, therefore ensuring that is compatible with the school network.

Cyber Security and Device Protection
The school network is protected against malicious attack or use by various systems such as anti-virus software and firewalls. It is the responsibility of students and staff to ensure that any personal ICT equipment is also similarly protected against malicious attack or use. It is also preferable that any portable media such as USB pens, DVD's or mobile phones brought in to the school are also scanned for malicious software before they are used on school's equipment. Care should also be taken when opening emails or attachments; always first contact the IT Technician before opening any suspicious or dubious email or attachment.

Inappropriate Materials or Language, Chat Rooms and Computer Games
Abusive materials or language should not be used to communicate nor should such materials be accessed. A good rule is never to view, send or access materials which you would not want governors, students, staff or parents to see. If encountered, such materials should be immediately reported in accordance with this policy.

Students and staff should not access chat rooms from the school site unless such chat rooms have an educational purpose and, in the case of students, they have been specifically directed to do so by a teacher or other supervising adult.

It is not appropriate for staff and students to play computer or internet games during the school day unless they have an educational purpose or at social times and, in the case of students, they have been directed to do so by a teacher or other supervising adult.

Theft, Vandalism and Wilful Damage to ICT Facilities
Theft and vandalism deplete the school's resources and are detrimental to the learning of students. Students are expected to treat all ICT facilities with respect. Staff should ensure that students are supervised when using ICT facilities and that any incidents of theft or vandalism are challenged, recorded and dealt with in an appropriate manner. It is important that ICT facilities remain secure at all times. Rooms and areas containing ICT facilities, for example, must not be left unlocked and unsupervised during open days, parents' evenings and other events when members of the public could be on site unsupervised.

BRING YOUR OWN DEVICE (BYOD)
The school recognises that as technology has changed more students and staff have access to Internet capable devices. Access to the Great Sankey High School wireless network, whether with school-provided or personal devices, is filtered in compliance with the Children's Internet Protection Act (CIPA). Students and staff will not have access to any documents which reside on the school network from their personal devices.

Access to the Great Sankey High School wireless network is a privilege, not a right. Any use of the wireless network entails personal responsibility and compliance with all school rules. The use of the network also allows IT staff to conduct investigations regarding inappropriate Internet use at any time, by teacher request. To obtain access to the network staff or pupils will need to provide

the IT Network Manager with the MAC address of their device enabling them to be given the access key. The network access key will be changed every term.

Guideline for Use
Use of personal devices during the school day is at the discretion of staff. Students must use devices as directed by their teacher. The primary purpose of the use of personal devices at school is educational. The use of a personal device is not to be a distraction in any way to teachers or pupils.

The use of personal devices falls under Great Sankey High School Acceptable Use Policy for students and staff. Students shall not use personal devices unless otherwise directed by their teacher e.g. on school visits or activities. Students should make no attempts to circumvent the school's network security and filtering policies. This includes setting up proxies and downloading programs to bypass security. Students should not distribute pictures or video of pupils or staff.

Consequences for Misuse by Students
- Access to the wireless network will be removed.
- Device taken away for the period.
- Student is not allowed to use personal devices at school.
- Serious misuse of Internet capable devices is regarded as a serious offence within the School's Behaviour Policy and will be dealt with in accordance with this policy.

School Liability Statement
Students and staff bring their devices to use at Great Sankey High School at their own risk. They are expected to act responsibly with regards to their own device, keeping it up to date and as secure as possible. It is their duty to be responsible for the upkeep and protection of their devices.

Great Sankey High School is not responsible for:
- Personal devices that are broken while at school or during school-sponsored activities
- Personal devices that are lost or stolen at school or during school-sponsored activities
- Maintenance or upkeep of any device (keeping it charged. Installing updates or upgrades, fixing any software or hardware issues).

STUDENT MONITORING
Monitoring of student activity will be undertaken routinely as part of the school Safeguarding procedures. The authorised personnel are:
- Headteacher
- Deputy Headteacher
- Designated Safeguarding Lead
- IT Technician Team
- Heads of House
- Pastoral Support Team

STAFF MONITORING
Monitoring of staff activity must be authorised by the Headteacher, or in their absence the Deputy Headteacher. Monitoring will be at the request of the Headteacher where there is reason to believe the individual has acted inappropriately or contrary to their contract of employment. Monitoring reports will be prepared by the IT Technician Team. Reports will be classified **STRICTLY CONFIDENTIAL** and be submitted to the Headteacher or, in their absence, the Deputy Headteacher.

GREAT SANKEY HIGH SCHOOL

ICT ACCEPTABLE USE POLICY – STUDENTS

As a student at Great Sankey High School I agree to use ICT facilities, social media and the internet responsibly. I agree to follow the rules set out below when using the school's ICT facilities.

- I will only use my own login, email address and password, which I will not share
- I will not access anyone else's work on the school's network without their permission
- I will not eat or drink near computer equipment
- I will not download or install software, shareware or freeware on the school's network either directly or via portable devices
- I will not violate copyright laws or licensing agreements
- I will not pass off work downloaded from the internet as my own. I will give clear references to sources where I have downloaded someone else's work
- I will not take photographs, video or audio of staff or other students
- I will not share or post images or audio of staff or students
- I will not use software, devices or mobile hot spots that get round the school's internet safeguards
- I will not bring in disks, USB pens or other portable devices without permission. I will screen all such devices for malicious software before I connect or load any files on to the school network
- I will not attach any device to the school network which may contain files which breach copyright, data protection or other laws
- I agree not to bring in ICT hardware from outside of the school and use this hardware on the school network
- I will not play computer games or access social networking sites during lessons
- I will not search, view, send or display offensive, threatening or time-wasting materials or post inappropriate images on websites
- I will only print copies of my work when it is necessary. I will reduce my printing by selecting pages. I will only print in colour when this is essential. I understand that the school will monitor any printing that I do and may take action if this is excessive
- I will not use inappropriate chat rooms during the school day and will only access social networking websites at social times
- I will not use the school's ICT facilities for personal financial gain, gambling, political purposes, advertising or cause damage to the school's reputation
- I will not access my personal 'home' email account during lessons unless given direct permission to do so in association with a task
- I will not give out personal information such as full name, home address, telephone numbers or personal email to anyone whose identity I cannot be certain of over the internet
- I will not arrange to meet anyone I have met over the internet
- I will notify an adult immediately if I encounter materials or messages that make me feel uncomfortable
- I will notify an adult immediately if I suspect someone else of misusing ICT facilities, social media or the internet
- I will respect school's resources and not damage or steal ICT facilities
- I understand that the school will check files and monitor the internet sites used by students
- I understand that sanctions will be used if I misuse ICT facilities, social media or the internet

I have read and understood the above statements and I agree to comply with the school's rules for use of ICT facilities, social media and the internet. I understand that failure to do this could result in the loss of my access rights to these facilities or the internet, along with further sanctions for serious misuse.

Student Signature: ……

Student Name: ……

Date: ……

As a parent or legal guardian of the student signing above, I grant permission for them to use electronic mail, social media and the internet. I understand that students will be held accountable for their own actions. I also understand that some material on the internet or social networking sites may be objectionable and I accept responsibility for setting standards for them to follow when accessing selecting, sharing and exploring information and media.

Parent / Carer Signature: ……

Parent / Carer Name (please print): …….

Date: ……...

PLEASE NOTE: Failure to return this document will result in loss of network privileges

GREAT SANKEY HIGH SCHOOL

ICT ACCEPTABLE USE POLICY – STAFF

As a member of staff at Great Sankey High School I agree to use ICT facilities, social media and the internet responsibly. I agree to follow the rules set out below when using the school's ICT facilities.

- I will keep my login, email address and password confidential. I will take care to ensure that others cannot use my accounts to access confidential information about students or staff by always logging off when I have finished work or locking my computer when it is left unattended
- I will not use anyone else's login, email address or password
- I will ensure laptops and desktops must be password protected and never left unattended whilst logged in
- I will never allow SIMs to be accessed/viewed by students or visitors
- I will not use any personal social media accounts for school business
- I will ensure I will only post via school's social media using a professional tone and appropriate content
- I will not access anyone else's work on the school network without their permission
- I will not download or install software, shareware or freeware on the school's network either directly or via portable devices without consulting the IT Technician Team
- I will not violate copyright laws or licensing agreements
- I will screen all USB pens, digital media and portable devices for malicious software before I download any files on to the network and take care when opening unknown email attachments. I will seek advice from the IT Technician Team if I am unsure about the safety of any such device or attachments
- I will not attach any device to the network which may contain files which breach copyright, data protection or other laws
- I agree not to bring in ICT hardware from outside of the school and use this hardware on the school network without appropriate authorisation from the IT Technician Team
- I agree to use the school's ICT facilities, social media and internet only for work related use
- I will not send photographs of students as email attachments or post photographs of students on websites unless I have consent to do so from students' parents or carers and the permission of the School's Leadership Team
- I will not search, view, send or display offensive content such as pornography, extremism or radicalisation material
- I will not use the school's ICT facilities for personal financial gain, gambling, political purposes, advertising, or cause damage to the school's reputation
- I will only access social networking sites to enhance the teaching and learning experience for students
- I will not friend students or their parents on social media unless they are related to me
- I will not send offensive threatening or time-wasting messages nor post inappropriate images on websites. All email sent will be of a professional nature and appropriate to its audience
- I will take care when giving out personal information, for example, to students and parents
- I will notify my line manager if I encounter materials or messages that are inappropriate to the work of the school or If I suspect someone else of misusing ICT facilities, social media or the internet

- I understand I must inform the Headteacher immediately if I suspect another member of the school of serious or illegal misuse of ICT facilities, social media or the internet. I will inform the Chair of Governors if that person is the Headteacher.
- I understand that I must also inform the Designated Child Protection Officer if this misuse may be a safeguarding, child protection or a Prevent issue
- I will ensure that all students under my supervision use ICT facilities, social media and the internet appropriately to support learning. I will challenge and report any misuse
- I will ensure that I follow relevant Health and Safety regulations when using ICT facilities such as not looking in to the light beam from a projector and leaving students unsupervised around projectors
- I understand I am responsible for the use and care of any personal device allocated to me whilst a member of staff
- I understand that I am responsible for the safekeeping of any ICT equipment which I use, including such equipment which I may take off site
- I understand that the school may check files and monitor the internet sites used by staff
- I understand that I must ensure that I adhere to all relevant policies and procedures including, but not limited to, Data Protection Policy, Safeguarding and Professional standards. As examples, the following are not permitted: sharing of personal messages, photographs, video and audio, language must always be professional and appropriate; this list is not exhaustive
- I understand that the school email system is not to be used for personal communication or sharing of information. This includes any non-school activities and events
- I understand that I must not do anything which may bring the school into disrepute for example posting comments and/or inappropriate images on social media and website that do not align with the ethos of the school
- I understand that I must not malign the school, students, staff, parents, trustees nor stakeholders on social media
- I understand that serious misuse of ICT facilities, social media and the internet could result in disciplinary action being taken against me

I have read and understood the above statements and I agree to comply with the school's rules for use of ICT facilities, social media and internet.
I understand that failure to do this could result in disciplinary action being taken against me

Staff Signature: …….. Date: ……...

Staff Name: ……..