NEWCASTLE UNDER LYME SCHOOL

E Safety, Mobile Device and ICT Acceptable Use (Computer Network Agreement) Policy

This document applies to Newcastle under Lyme School and EYFS and is published to parents and prospective parents on the School's website and is available upon request to parents and prospective parents. Parents will be asked to sign to indicate that they have understood the principles and rules which pupils must follow when using the Newcastle-under-Lyme School's computer network and accessing the Internet and emails. If they choose not to sign this document, pupils will not be able to use the network.

See also: ICT Acceptable Use [Computer Network Agreement] Policy, Child Protection (Safeguarding Policy), Staff Behaviour Policy, Social Media Policy for Staff, Anti-bullying and Anti-cyber-bulling Policy, Curriculum Policy (which includes information about PSHE) and Behaviour, Rewards and Sanctions Policy.

1 E-Safety:

School recognises that it has a duty to ensure the safety of pupils in the digital 'virtual' world. Pupils use technology inside and outside school providing opportunities for learning but there are also risks to young people. We use technology to deliver innovative lessons, educating pupils in the potential and responsibilities which come with new technology. We provide a safe online environment within school and teach students about different risks, including bullying, harassment, grooming, identity theft and personal data protection. The nature of technological advance means School reviews its provision and policies regarding safe ICT use. E-safety is a topic incorporated into PSHE lessons and computing lessons in the Prep and Senior Schools.

Pupils study a wide ranging programme of e-Safety materials in PSHE and computing lessons. The School addresses online safety issues such as cyber-bullying and sexting through its PSHE programme and in computing lessons. Organisations such as the NSPCC (https://www.nspcc.org.uk/preventing-abuse/child-abuse-and-neglect/online-abuse/) and Think U Know

(https://www.thinkuknow.co.uk/parents/). Prep School pupils receive e-safety advice.

This policy covers both devices provided by the School and devices owned by pupils and staff and brought into school.

2 Responsibilities for E-safety:

The Deputy Head Pastoral as the Designated Safeguarding Lead (DSL) has overall responsibility for e-safety issues. The practical management of e-safety in the School lies with the Director of ICT and the Head of Network, Infrastructure and ICT Services, working alongside the two Senior School Deputy Heads and the Prep School Computing Coordinator who review and develop the strategy for e-safety.

Staff are given updates regarding e-safety as part of their safeguarding briefings during the year. This includes making sure that staff are aware of their responsibilities to promote safe ICT use in their lessons and how to report an e-safety incident.

Through the PSHE programme, and the work of Heads of Year and the Deputy Head Pastoral, in addition to the work of the Director of ICT, staff and pupils are made aware of possible child protection issues to develop through

- sharing of personal data
- access to inappropriate materials
- inappropriate on-line contact with strangers
- potential or actual incidents of grooming
- cyber-bullying

The Head of Network, Infrastructure and ICT Services [HNIS] has responsibility for ensuring that the School's ICT infrastructure is secure and is not open to misuse or malicious attack and that users may only access the networks and devices through a properly enforced password protection policy. The Director of ICT and HNIS will ensure filtering is fit for purpose and that Mobile Device Management (MDM) enables effective monitoring of devices when required. With this in mind, the Director of ICT, HNIS and their staff are also required to keep up to date with e-safety technical information.

It is accepted that, for good educational reasons, pupils may need to research topics (e.g. drugs) that would normally be filtered. In such a situation, staff can request that those sites are temporarily removed from the filtered list for the period of study.

Pupils are responsible for using the digital technology systems in school in accordance with the Student Acceptable Use Policy. In addition pupils will be

taught to understand issues surrounding bullying, plagiarism, use of digital imagery and social media in and outside of school. This is usually, but not exclusively, delivered as part of the PSHE curriculum and computing lessons. Form periods help to promote a whole school approach to e-safety.

Parents play a crucial role in ensuring that their children understand how to use devices appropriately. The School encourages parents to share concerns they have about their child's online life, for example gaming and using social media as good pastoral care.

3 Unsuitable or inappropriate activities:

Some internet activity, e.g. distributing racist material, is illegal and is filtered from School systems. Other activities, e.g. cyber-bullying and harassment, where allegations are made, are investigated in accordance with school policies and reported to the police if it seems that a crime has been committed. There are however activities which may be legal but are inappropriate in a school context, possibly because of pupil age or nature of activity.

In the event of suspicion of ICT misuse the School will use the following procedure to protect all those involved and to preserve evidence for a subsequent investigation. Senior staff will use a designated computer to which pupils do not have access. All sites and content visited are closely monitored and recorded. The URL of any site containing the alleged misuse will be recorded, as will the nature of the content causing concern. It may also be necessary to record and store screenshots of the content for investigation.

Once this has been fully investigated, a judgement will be made whether the concern has substance or not. If it does then appropriate action will be required in line with the Behaviour, Rewards and Sanctions Policy and Staff Behaviour Policy.

If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances which would be reported to the police would include: incidents of 'grooming' behaviour, the sending of obscene materials to a child, material which may breach the Obscene Publications Act, criminally racist material and other criminal activity or materials. In this situation the computer used to investigate the concern will be isolated pending advice from the police.

4 Use of Internet and Email:

There is strong anti-virus and firewall protection on the School network and therefore the network can be regarded as secure as possible. Sometimes the protection will block legitimate sites and staff should contact the ICT Department

to request a site to be unblocked. Staff should also be aware that attempting to access blocked sites will be recorded on the school systems and that email will also be monitored.

School internet filtering systems are constantly updated by external providers to deliver accurate analysis. This helps deliver a safe online environment for everyone in School. All internet users are bound by a policy that prevents them from accessing materials that are inappropriate for school use or possibly damaging to the school network. In addition, pupils are, where possible prevented from having access to sites that may:

- allow cyber bullying
- provide images/material of a graphic nature
- provide information on illegal activities
- encourage time wasting

In addition to filtering, School also monitors all web activity for pupils and staff. From this monitoring reports are produced that highlight any safeguarding issues. Reports are reviewed daily by Deputy Head Pastoral, Deputy Head Academic and Head of Network, Infrastructure and ICT Services [HNIS]. Any incidents deemed low key will be managed in house; any illegal activities will be reported to police with all evidence gathered.

Staff must immediately report to the Director of ICT or a member of SMT the receipt of any communications that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature. They should not respond to any such communication. Pupils are also encouraged to report similar incidences to a member of teaching staff and to retain screen shots of the relevant and related material to help with investigation.

Any online communications (including posting) must not either knowingly or recklessly:

- Place a child or young person at risk of harm
- Bring the School into disrepute
- Breach confidentiality or copyright
- Breach data protection legislation
- Do anything that could be considered discriminatory

5 Data storage and storage of digital images:

In accordance with our Data Protection Policy and Acceptable Use Policy staff should not store personal data on unsecured devices or data storage solutions, for example memory sticks. At the request of the ICT department laptop computers loaned to staff must be returned each term for routine maintenance.

There are specific dangers as a result of publishing digital images on the internet because they provide opportunities for cyberbullying, stalking or grooming to take place. The School's role is to educate pupils, staff and parents to be vigilant and to consider these possibilities before they publish their images electronically.

Staff who take pictures of pupils for educational purposes should do so within the rules of the Acceptable Use Policy and Staff Behaviour Policy and take care to ensure pupils are appropriately dressed. Staff should not routinely keep digital images of pupils on their own devices, instead downloading any pictures taken of school activities or events onto the School Network as soon as possible. Personal image capturing devices are not to be used in the EYFS.

6 Bring Your Own Device and use of personal devices:

Staff using either their own or a school device must have a password or device lock so that unauthorised people cannot access the content. Staff are permitted to use mobile phones during the school day within the rules outlined in the Child Protection (Safeguarding) Policy and the Staff Behaviour Policy.

The Senior School encourages pupils to 'Bring Your Own Device (BYOD)' and pupils are encouraged to use their own devices as appropriate in lessons, recognising that BYOD is becoming an increasingly accepted way to access ICT services inside and outside the classroom. The School supports users of BYOD by means of a school-wide Wi-Fi network; information systems including Firefly, the VLE, which is designed to operate on a range of devices; and appropriate filtering and blocking access to content deemed inappropriate to the setting. Pupils bringing their own devices into the Prep School must abide by the terms of the Policy on the use of personal electronic devices.

There are additional rules to those in the ICT Acceptable Use Policy for pupils using their own devices. When a personal device is used as a work tool to access the school systems and/or its data, the usual responsibilities apply. The School reserves the right to prevent access to the network by any device that is considered a risk.

All staff and pupils using BYOD are required to conform to expected standards of online behaviour and not download or transmit any material which might be harmful or offensive to any School pupil or member of staff or bring the School into disrepute. Any breach of this protocol will be treated as a serious disciplinary matter. (See Child Protection and Safeguarding Policy, Staff Behaviour Policy, Social Media Policy for Staff, Anti-bullying and Anti-Cyberbullying Policies for further details on use of Social Media.)

The School will seek to manage, by filtering the risks to pupils from BYOD, of:

- accessing inappropriate web content;
- hosting of inappropriate services on pupil–owned devices via the school network

All BYOD users should refer to the School's ICT Acceptable Use (Computer Network Agreement) Policy and note the following additional rules and requirements relating to BYOD use:

- the user is responsible for the safe keeping, maintenance and insurance of the device at all times;
- all BYOD devices brought into the school must only be connected to the wireless network as instructed.
- users must keep their device's software up to date and ensure that no content threatens the integrity and security of the device;
- users should:
  - delete from their device any sensitive e-mails and files (including e-mail attachments) as soon as they have finished using them; and
  - limit the number of e-mails and other information they sync to their device to limit the possibility of inappropriate or excessive data transfer.
- in the case of a BYOD device belonging to a pupil (or belonging to a relative or third party, but used in school by the pupil), the School reserves the right to remove the device to secure storage pending further enquiries under disciplinary procedure; and
- the loss of any device holding data relating to the School or with access to the School Network must be reported immediately to ICT Support and the owner must immediately change his/her password(s) for all access.

7 ICT Acceptable Use (Computer Network Agreement) Policy:

The School's network provides data communication links within the School and beyond including the Internet. The Internet offers valuable learning experiences and sources of information. At the same time, there are potential hazards. While our staff make every effort to avoid misuse of the Internet, by pupil education, staff supervision and the use of filtering technology, pupils may still access material which is not appropriate. There are opportunities with computer networks for pupils to conduct themselves in ways that are unacceptable and to create and distribute inappropriate materials.

The School teaches pupils good practice, imposes control on what pupils see and do and informs parents of potential risks and benefits. School will monitor use and ICT Staff may review files and communications to maintain system integrity. Backups are made every evening but the user is responsible for independently maintaining copies of valuable data.

Use of another individual's password-protected account is prohibited. Where password protected accounts are used, network users are personally responsible for all activity that occurs within their account. Any attempts at unauthorized access of School data will result in termination of the user's computer and network privileges. Any attempt to vandalise School network accounts or systems will result in termination of the user's computer and network privileges. Vandalism is defined as any malicious attempt to harm or destroy data of another member, the School, or any of the agencies or other networks that are connected to the Internet. This includes, but is not limited to, the uploading or creation of computer viruses.

School reserves the right to modify this ICT Acceptable Use (Computer Network Agreement) Policy for ICT, as appropriate. Changes will be published on the School website.

	J A Simms
Policy Reviewed by SMT:	October, 2019
Next review due:	October 2020