NEWCASTLE UNDER LYME SCHOOL

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

This document applies to the Senior and Junior 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 and Safeguarding Policy, Staff Behaviour Policy, Anti-bullying and Anti-cyber-bulling Policy, Curriculum Policy (which includes information about PHSE) and Behaviour Management Policy.

1.1 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 pupils 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 Junior and Senior Schools.

Pupils study a wide ranging programme of e-Safety materials in PHSE and computing lessons. The School addresses online safety issues such as cyber-bullying and sexting through its PHSE programme and in computing lessons. Organisations such as the NSPCC https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/ and https://www.thinkuknow.co.uk/parents/ provide excellent advice. Pupils in Year 7 study for the British Computer Society Level 1 Award in e-safety. Junior School pupils receive e-safety

advice from the Police Community Officer.

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

1.2 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 Junior School Computing Co-ordinator 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. The Director of ICT keeps a record of e-safety incidents and how they were dealt with.

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 students 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 students 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. School provides parents' information evenings to help parents understand these issues. The School encourages parents to share concerns they have about their child's online life, for example gaming and using social media as ~~part~~ of good pastoral care.

1.3 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, for example radicalisation activity, 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 on the machine being used 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 Management 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.

2.1 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. 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, all pupils have supplementary policies applied that prevent access to sites that may:

- allow cyber bullying (e.g social networks)
- provide images/material of a graphic nature
- provide information on illegal activities (e.g radicalisation)
- encourage time wasting (e.g games)

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

2.2 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.

3.1 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 Junior School must abide by the terms of the Policy on the use of personal electronic devices [see Appendix].

There are additional rules to those in the ICT Acceptable Use Policy for pupil 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, Anti-bullying and Anti-Cyber-bullying 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 vi 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 student (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.

3.1 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, students 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.

Author:	S Luck, Director of ICT
Policy Reviewed at SMT:	September 2017
Policy Reviewed by Governors:	October 2017
Next Review Due:	October 2018

NEWCASTLE UNDER LYME SCHOOL *Senior School

COMPUTER NETWORK AGREEMENT FOR PUPILS

At the end of this document you and your parent/guardian will be asked to sign to indicate that you have understood the principles and rules of using the Newcastle-under-Lyme School's computer network and accessing the Internet and e-mails. If you choose not to sign this document you will not be able to use the network.

INTRODUCTION

We want each pupil to enjoy using the School's computer network and Internet, and to become proficient in drawing upon it both during your time at School, and as a foundation for your further education and career.

However, there are some potential drawbacks with the School's computer network, e-mail and the Internet, both for you and for the School.

The purpose of this Protocol is to set out the *principles* which you must bear in mind at all times and also the *rules* which you must follow.

PRINCIPLES

1 The use of e-mail and access to the Internet from the School's computers and network must only be for educational purposes during lessons and the School day.

2 You may only use e-mail and access the Internet once you have received appropriate training, or authorisation, from a member of staff. If, at any time after that, you are unsure whether you are doing the right thing, you must ask for help from a member of staff.

3 You must do all you can to protect the security of the School's computer network, and the security of networks belonging to others. In particular, this means being aware of the possibility of computer viruses and taking sensible precautions to avoid bringing them onto our system or passing them to others.

4 You must also try to protect personal and confidential information about yourself and others, even if you receive or come across this inadvertently. Receiving or using this kind of information may be unlawful under data protection legislation.

5 You must not knowingly obtain (or attempt to obtain) unauthorised access to any part of any computer system, or any information contained on such a system, including the School's system. This is known as "hacking" and is both a serious breach of School discipline and a criminal offence.

6 You should assume that all material on the Internet is protected by copyright and you must treat such material appropriately and in accordance with the owner's rights: you must not plagiarise another's work.

7 Any message or attachment which you send to another person or group of persons must be appropriate and courteous, and must not contain anything which is bullying, violent, racist, sexist, discriminatory, defamatory, blasphemous or pornographic. You may be acting unlawfully if it does. As far as you are able, you must also make sure that you do not search for, or receive, such material: it is your responsibility to reject it if you come across it, and inform the Head of Network, Infrastructure and ICT Services.

8 You must not bring the School into disrepute through your use of e-mail and your access to the Internet. For example, you must not send or ask to receive anything which you believe the Headmaster and/or your parents would find inappropriate for a pupil at Newcastle-under-Lyme School.

9 You must not enter into any contractual commitment, whether for yourself or on behalf of another (including the School), or use the network for personal financial gain, gambling, political purposes or advertising.

10 You will be liable to disciplinary sanctions including, in the most serious cases, permanent exclusion, if you breach this agreement. You (or your parents) may also be asked to pay for any significant expenditure, or indemnify any significant liability, incurred by the School as a result of the breach.

11 For your own protection and that of others, your use of e-mail and of the Internet will be monitored by the School. Remember that even once you have deleted an e-mail or something you have downloaded, it can still be traced on the system.

RULES

12 You may only use the School's computers whilst logged on with your own username and password.

13 You must never disclose your password to another pupil, nor to anyone outside the School.

14 You may not read anyone else's e-mails without their consent. Users are reminded of the danger of entering into e-mail correspondence with people whom they do not know.

15 You must not send an e-mail to an entire address list or distribution list without the express prior consent of the Head of Network, Infrastructure and ICT Services.

16 You must not use the School's computer system to play non-educational games, or use "chat" programmes, bulletin boards, usergroups, file transfer programs etc unless authorised by the Head of Network, Infrastructure and ICT Services.

17 You must tell the Head of Network, Infrastructure and ICT Services immediately if you have accidentally read, downloaded or have been sent inappropriate material, including personal information about someone else.

18 You must not send encrypted messages. If you receive any encrypted messages these must be referred to the Head of Network, Infrastructure and ICT Services.

19 No devices may be connected to the School network without the permission of the Head of Network, Infrastructure and ICT Services

20 Violations of the above rules will result in a temporary or permanent ban on Internet/computer use. Parents will be informed. Additional disciplinary action may be taken. When applicable, external agencies may be contacted and informed.

✂ ----------

COMPUTER NETWORK AGREEMENT FOR PUPILS

PUPIL (full name): ……..……..... *(please print)*

Signature: ……... Date: …… Form: …….…….

PARENT/GUARDIAN (name): ……..…… *(please print)*

Signature: ……... Date: ……

Please return this completed form to:
Lancaster Site School Office, Newcastle-under-Lyme School, Mount Pleasant, Newcastle, Staffs ST5 1DB

September 2016

Junior School Policy on the Use of Personal Electronic Devices

- Electronic devices may only be brought into the Junior School once an agreement (See attached) has been signed by both parent and child and returned to School.
- The device may only be used by the owner.
- Electronic devices may only be used for reading purposes in School (9:00am – 3:30pm) under the supervision of the class teacher. They may not be used before this time.
- Electronic devices may not be used during playtimes, wet or otherwise.
- Electronic devices may be used in After School Care under the supervision of a member of staff for a period of 30 minutes from 4:00 – 4:30pm. The use of the devices for reading or playing games will take place in a controlled environment. Children without an electronic device will not be allowed to participate.
- The responsibility of the device remains with the owner at all times.
- Claims for damages against another child can only be made if wilful damage can be proven. The claim will be between the two parties involved and the School will not intervene, other than assisting with the investigation of such a claim.
- Devices should not be shared with other children
- The following uses are not permitted under any circumstances:
    - playing of inappropriate games
    - the watching of inappropriate videos
    - the taking of photographs
    - the taking of videos
    - the taking of any audio recording
    - any other action deemed inappropriate
- Sanctions for contravening the correct use of the device will be determined by the severity of each individual case. Sanctions could include any of the following:
    - Removal of device for 1 week
    - Inability to bring the device into school
    - Suspension
    - Expulsion

Junior School Agreement Use of Electronic Devices

Children are permitted to bring in their electronic devices such as a Kindle, Kindle Fire, iPod touch, iPad, iPad Mini, etc, for the main purpose of reading in School. During wet lunchtimes and at After School Care these devices may be used to play age appropriate games that parents have approved for downloading. In agreeing to this contract children and parents understand that the following uses are not permitted under any circumstances:

1. playing of inappropriate games
2. the watching of inappropriate videos
3. the taking of photographs
4. the taking of videos
5. the taking of any audio recording
6. any other action deemed inappropriate

If a child is in breach of this agreement it would be a serious disciplinary offence. The responsibility for any electronic device will remain that of the child. Any child wishing to bring an electronic device in to School must, with their parents, complete and return the slip below.

AGREEMENT on Use of Electronic Devices

I understand the terms of this agreement and will ensure our child _____

(name) in _____ (form) complies with them.

Signed_____ Printed _____

Parent / Adult with parental responsibility

I understand the terms of this agreement and the consequences of failing to follow it.

Signed_____ (Child) Printed _____

Date _____

Junior School Policy on the Use of the Internet

General Background

Children are granted individual access to the Internet to use as an educational resource. Other uses may result in disciplinary measures (see below). Before use, children will be given training on how to use the Internet and warned of the inherent dangers.

The School Internet System

The only machine directly connected to the Internet is our Internet Proxy Server (a single computer in the I.T. office). This computer is on the School network, and distributes the Internet services to **any** computer on the School network. Many computers can use the services simultaneously.

Safeguards Regarding Unsuitable Material, Viruses etc.

- All machines used by children are in public areas, which has a self-censoring effect.
- All access is logged by the School in the proxy server. Users know this.
- It is possible to filter out some undesirable material, but we can never be certain and it is better to realise from the start that children will have to have self-responsibility.

Disciplinary Procedures

As a guideline, for various classes of Internet misuse, children may expect the following disciplinary measures, at the very least, to be applied:

- frivolous use – accessing games, silly information:- verbal warning.
- repeated frivolous use:- access denied for week or term.
- accessing offensive material:- interviewed by Head of the Junior School/detention/access denied for specific time.
- repeated accessing of offensive material:- referred to Headmaster.
- accessing illegally offensive material:- referred to Headmaster, parents and police.

At the discretion of the Headmaster, certain of the offences mentioned above may result in suspension or expulsion.

These measures will be reviewed regularly.

September 2016

Junior School Contract for Responsible Internet and Computer Use

We use the school computers and Internet connection for learning.

The following rules will help us to be fair to others and keep everyone safe.

I will only use websites that my teacher has already approved and asked me to use.

I will not use the computer or Internet without an adult being present.

If I see anything I am unhappy with or do not like, I will tell a teacher immediately.

I understand that if I deliberately break these rules, I could be stopped from using the Internet or computers.

I will not waste limited resources such as disk space or printing ink and paper.

I will ask permission before printing documents in colour.