Lockington CE VC Primary School

Acceptable Use Policy

Date Policy Formally Agreed By Governors	January 2018
Date Policy Becomes Effective	December 2017
Review Date	December 2017
Person Responsible for Implementation and Monitoring	Headteacher

1. General Aims and Objectives

The Internet provides a valuable contribution to enhance learning and understanding in all areas of the school curriculum. As a result, it has become an important part of the education environment. A vast range of opportunities are present by new and emerging technologies.

Due to the open nature of the Internet, there is some material which is unsuitable for children. It is essential that schools have an Acceptable Use Policy in order to keep children safe whilst working online.

We will ensure that children are protected from such information by:

- Having an Acceptable Use (Internet Safety) Policy, outlining acceptable use of the Internet
- Using security software
- Limiting internet features
- Teaching children to use the facility sensibly
- Supervising internet usage
- Having rules for safe internet usage

The policy sets out what the school considers as 'Acceptable Use' of the Internet for all users of our computer network. It must be noted, however, that neither the school nor the Internet Service Provider (ISP) can guarantee complete safety from inappropriate materials.

Our Acceptable Use Policy runs in conjunction with the school policies:

- Safeguarding
- E-Safety
- ICT
- Anti-Bullying
- Behaviour and Discipline
- Social Networking Policy

This policy covers all internet access on any of our schools devices, e.g. computers, laptops, iPad, etc.

2. Acceptable Use Agreement

All staff and pupils at the school are required to sign the Acceptable Use Agreement. If volunteers/visitors are required to use our computer network, they will also need to read this policy and sign an Acceptable Use Agreement.

This document has been drawn up to protect anyone using the internet and our computer netwok. This document is revised regularly.

For staff/ volunteers/visitors

The Acceptable Use Agreement is to be signed by all staff and kept in the School Office.

For pupils

The Acceptable Use Agreement for Pupils is to be signed by parents/guardians/cares and is retained with all other permission declarations in the School Office.

Pupils who do not have this Agreement signed should not be allowed to access the Internet. This means that pupils will only be able to access the statutory elements of the Computing curriculum and will need close supervision by a member of staff at all times. Pupils who do not have a signed Acceptable Use Agreement will not be allowed to have any 'free' access to the internet. All computer activities (even those using non-internet based resources such as Word, PowerPoint will be monitored.

Where a pupil does not have an Acceptable Use Agreement in place, the parent/carer of the pupil will be contacted by the Headteacher/ICT Subject Leader to discuss the reasons why permission has not been granted.

Copies of both of these Agreements are attached to this policy and copies are available from the ICT Subject Leader/School Office. The ICT Subject Leader will monitor signed Acceptable Use Agreements for all users.

The school reserves the right to routinely monitor internet usage and will maintain logs of internet activities as a means of compliance with this policy.

Staff and pupils, irrespective of whether or not they themselves are authorised internet users, are required to inform the appropriate manager if they become aware of, or suspect, the school's internet facilities are being misused.

3. Acceptable Use/Rules

The following are the school's rules for internet safety. These rules will help to keep everyone safe and are to be displayed in the classrooms.

Pupils will:

- Not access other people's files
- Only use computers for school work
- Only use the internet when instructed by a member of staff
- Only access websites that have been checked and approved by a member of staff or whilst being supervised by a member of staff
- Not give their home address/telephone number or make arrangements to meet people over the internet
- Tell a member of staff if they see anything they are unhappy with
- Not download anything from the internet, unless instructed to do so by a member of staff

The school reserves the right to keep detailed log of computer files and internet sites visited. If inappropriate use of the internet/network is discovered, the child may no longer be able to use computers in school. If this is the case, parents will be contacted immediately.

Staff Will:

- Access the computer network using only his/her own username and password. If there are any problems with a login, this must be reported to the School Office who will liaise with the agreed provider of ICT Services.
- Avoid activity that threatens the integrity of school ICT systems. Removable storages (such as memory sticks) will need to be checked when used on the school network. Teaching staff will only use encrypted hard-drives (provided by the school) for saving sensitive school information.
- Ensure that all internet sites used should be appropriate to staff professional activity.
- Be responsible for all email sent and for contacts, including using the same levels of language and content that would be applied to other methods of communication.
- Not post anonymous messages or forward chain email messages.
- Not use the computer network / internet for financial gain, gambling, political purposes or advertising.
- Not contact pupils via email, unless prior arrangements have been made with the Headteacher. In this instance, personal email addresses should not be used, the school office can provide you with a genetic email address for this purpose. Staff can also send messages via the school office, if required.

Examples of misuse could include excessive personal or inappropriate use of the internet, personal use during normal working hours, downloading executable files or accessing non-work related streaming media. This list is not exhaustive. Any identified misuse will be investigated and could result in action under the school's disciplinary policy and procedure.

All users are advised to lock screens/devices when not in use, to prevent unauthorised use of logged –in accounts, such as email.

4. Unacceptable Use

The following relates to LA policy on Acceptable Use for council employees.

It is illegal to create, access, copy, store, transmit or publish any material which falls into the following categories:

- National security: information on bomb-making, illegal drug production, terrorist activities.
- Protection of Minors: inappropriate forms of marketing, displays of violence or pornography.
- Protection of Human Dignity: incitement to racial hatred or racial discrimination, harassment.
- Economic Security: fraud, instructions on pirating credit cards.
- Information Security: malicious hacking
- Protection of Privacy: unauthorised communication of personal data, electronic harassment.
- Protection of Reputation: libel, unlawful comparative advertising.
- Intellectual Property: unauthorised distribution of copyrighted works, e.g. software or music.

If staff, pupils or visitors are found to infringe these guidelines, then the incident will be reported to the Headteacher and/or the ICT Subject Leader as soon as possible. Access will then be removed/restricted, depending on the nature of the incident.

5. Acceptable Use of Laptops/ipads – Staff

Where staff have a school laptop, the laptop remains the property of Lockington Primary School. Use of personal laptops is not permitted on our school network, unless prior arrangement has been made with the Headteacher or ICT Subject Leader. Inappropriate use of laptops may expose the school to unnecessary risks including virus attacks, compromise of network systems and services, financial and legal issues. All staff who have been issued with a school laptop/ipad have signed a Responsibility Statement; these statements have been checked by the ICT Subject Leader and are retained in the individual personnel files (in the Headteacher's Office).

Staff should take good care of the school laptop and take all reasonable precautions to ensure that it is not damaged, lost or stolen. Negligence in the care of laptops or failure to report loss/damage may result in disciplinary action against the staff member concerned.

Staff using school laptops/ipads will:

- Abide by the Acceptable Use rules stated previously for correct use of the school's computer network, when using his/her laptop/ipad.
- Always transport laptops/ipads in the protective case/bag supplied.
- In order to prolong the battery life, laptops should only be plugged in to a mains power source when the battery is running low. A warning can be set up to you know when to do this.
- Not leave laptops/ipads in unsupervised areas, for example vehicles or unlocked rooms (outside of school).

- Bring laptops/ipads in to school regularly to be updated and virus checked.
- Laptops/ipads must not be used by non-school employees.
- Limited personal use of laptops/ipads is permitted, subject to the restrictions contained in this Acceptable Use Policy. Any personal use of school laptops/ipads is expected to be in the employee's own time.
- Staff should be aware that files stored on school laptops are subject to monitoring by the Headteacher/ICT Subject Leader. We reserve the right to audit correct usage of school laptops at any time. Individuals may be responsible for any breach of policy illegally held software, or breach of copyright legislation.

6. Email

Email is recognised a proper and important method of communication at Lockington Primary School but should not be used as a way of avoiding traditional means of communication.

For example, email should not be used to impart information that should be exchanged face-to face:
-discussing concerns regarding pupil behaviour, progress or behaviour with a parent.
-discussing management issues concerning an employee's performance or conduct.

Staff should not:

- Sign up to mailing lists or newsletters unless they are work related.
- Use their school email address as a primary address for making purchase of goods and services from the internet unless it is work related.
- Use their school email address in EBay, PayPal, Amazon (or similar) to pay for personal purchases.

Staff who receive emails deemed inappropriate or excessive should contact their line manager in the first instance and, where appropriate, inform the originator of the inappropriateness of the email. Staff should note that email is a primary method for transferring viruses, malicious programs and copyright material.

Employees who receive messages informing them of viruses or other security threats must forward the email to 'Spam Reporting' at County Hall. Most messages of this nature are hoaxes, designed to disrupt email services by generating unnecessary traffic. There may also be hacking attempts, virus attachments and phishing. Staff are advised not to click on any link within unknown emails.

Email Etiquette

Do	DON'T
• Consider the message you want to convey. • Always use plain English. • Make sure that the language and style of writing is appropriate for the recipient. • Type directly into the message box, where appropriate. • Ensure that the mailing list is relevant	• Use email to break bad news or to discuss tense or confusing information. • Use 'text speak' or acronyms. • Use attachments when the detail in the attachment could be typed directly into the message box. • Send emails to people who do not require it.

and current, double check before sending. • Use a strong subject line to allow easy understanding of the subject matter. • Proof read emails prior to sending. • Use spell check before sending. • Use automatic signatures. • Delete unwanted message immediately. • Keep messages remaining in your inbox to a minimum. • Use blind copying (bcc) sparingly and only when essential. • Consider the environment before printing emails.	• Write the whole message in capital letters, as it is generally seen as shouting. • Do not include humorous remarks, jokes or sarcasm as they may not be interpreted as intended. • Use return receipts unless it is absolutely necessary. It can be considered annoying and an invasion of privacy. • Use emoticons (keyboard character combinations that convey an emotion when viewed sideways, e.g. =:-)) • Give anyone your login details/grant access to your personal emails.

7. Social Networking

The term 'social media / networking' is commonly given to websites and online tools which allows users to interact with each other in some way – by sharing information, opinions, knowledge and interests. Examples include Facebook, Twitter, Snapchat, Instagram, YouTube, Blogger, Pinterest etc. although this list is not exhaustive.

Access to social media during work time for personal use is not permitted. Employees are responsible for any content they publish and must not publish contend relating to Lockington Primary School/East Riding of Yorkshire Council.

The Headteacher/responsible person is permitted to access Twitter to update the School's Twitter account with relevant news and information. This will be monitored by our Governor with ICT responsibility.

Please refer to our Social Networking Policy for more information.

8. Computer Misuse Act 1990

The Computer Misuse Act identifies three specific offences.

1. Unauthorised access to computer material.
2. Unauthorised access with intend to commit or facilitate the commission of further offences.
3. Unauthorised modification of computer material.

It should be noted that breach of this Act could result in criminal proceedings, A copy of the Computer Misuse Act is available for consulting in public libraries.

9. Policy Review

This policy is reviewed and updated regularly to meet the changing needs of the school and in light of any new initiatives. The last review took place in November 2017.

5/2/18