Lemington Riverside Primary School

Acceptable Use Policy

Acceptable Use Policy

Created: February 2019
Review date: February 2020

Table of Contents

Introduction

In May 2018 the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) became enforceable across the United Kingdom. As part of Lemington Riverside Primary School's programme to comply with the new legislation it has written a new suite of Information Governance policies.

The internet is an essential element in 21st Century life for education and social interaction. The purpose of internet use in school is to promote pupil achievement, to support the professional work of staff and to enhance the school's management, information and business administration system. Benefits include:

- Access to worldwide resources and research materials.
- Educational and cultural exchanges between pupils worldwide (i.e. Skype).
- Access to experts in many fields.
- Staff professional development such as access to online learning and forums.
- Communication with support services, professional associations and colleagues.
- Exchange of curricular and administration data (i.e. between colleagues, LA and DfE).

The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. Consequently, in delivering the curriculum teachers need to plan to integrate the use of ICT and web-based resources including e-mail to enrich learning activities. Effective internet use is an essential life skill.
Access to the school's ICT network and use of ICT facilities owned by the school, including access to the Internet, are conditional on observance of the following Acceptable Use Policy. The Aims of this Acceptable Use Policy are to:

- Allow all users access to school ICT resources and use of the Internet for educational purposes.
- Provide a mechanism by which staff and pupils are protected from Internet sites, information, and individuals that would undermine the principles and aims of the school.
- Provide rules which are consistent, and in agreement with the General Data Protection Regulation 2018, Computer Misuse Act 1990 and other legislation relevant to the use of computers and electronic data in schools.
- Provide rules that are consistent with the acceptable procedures commonly used on the Internet, including those associated with netiquette.
- Provide rules relating to the use of computers and ICT facilities in school, which are consistent with the general policies of the school.

The Acceptable Use policy governs the use of the School's corporate network that individuals use on a daily basis in order to carry out business and curricular functions.

This policy should be read in conjunction with the other policies in the School's Information Governance policy framework.

Scope

All policies in Lemington Riverside Primary School's Information Governance policy framework apply to all School employees and pupils, any authorised agents working on behalf of the School, including temporary or agency employees, and third party contractors. Individuals who are found to knowingly or recklessly infringe these policies may face disciplinary action.

The policies apply to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper,
- Information or data stored electronically, including scanned images,
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer,
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card,
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops,
- Speech, voice recordings and verbal communications, including voicemail,
- Published web content, for example intranet and internet,
- Photographs and other digital images.

Email

The School provides email accounts to employees to assist with performance of their duties.

Personal Use

Whilst email accounts should primarily be used for business functions, incidental and occasional use of the email account in a personal capacity may be permitted so long as:

- Personal messages do not tarnish the reputation of the School,
- Employees understand that emails sent to and from corporate accounts are the property of the School,
- Employees understand that School management may have access to their email account and any personal messages contained within,
- Employees understand that the Emails sent to/from their email account may have to be disclosed under Freedom of Information and/or Data Protection legislation,
- Employees understand that the School reserves the right to cleanse email accounts at regular intervals which could result in personal emails being erased from the corporate network,
- Use of corporate email accounts for personal use does not infringe on business functions.

Inappropriate Use

The School does not permit individuals to send, forward, or solicit emails that in any way may be interpreted as insulting, disruptive, or offensive by any other individual or entity. Examples of prohibited material include, but are not necessarily limited to:

- Sexually explicit messages, images, cartoons, jokes or movie files,
- Unwelcome propositions,
- Profanity, obscenity, slander, or libel,
- Ethnic, religious, or racial slurs,
- Political beliefs or commentary,
- Any messages that could be construed as harassment or disparagement of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs, or political beliefs.

Other Business Use

Users are not permitted to use emails to carry out their own business or business of others. This includes, but not necessarily limited to, work for political organisations, not-for-profit organisations, and private enterprises. This restriction may be lifted on a case by case basis at the discretion of School management.

Email Security

Users will take care to use their email accounts in accordance with the School's information security policy. In particular users will:

- Not click on links in emails from un-trusted or unverified sources,
- Use secure email transmission methods when sending personal data,
- Not sign up to marketing material that could jeopardise the School's IT network,
- Not send excessively large email attachments without authorisation from School management and the School's IT provider.
- Not forward e-mail messages onto others unless the sender's permission is first obtained.
- Not send e-mail messages in the heat of the moment and avoid writing anything that may be construed as defamatory, discriminatory, derogatory, rude or offensive.

Group Email Accounts

Individuals may also be permitted access to send and receive emails from group and/or generic email accounts. These group email accounts must not be used in a personal capacity and users must ensure that they sign each email with their name so that emails can be traced to individuals. Improper use of group email accounts could lead to suspension of an individual's email rights. Craig Heeley (Head Teacher) will have overall responsibility for allowing access to group email accounts but this responsibility may be devolved to other individuals.

The School may monitor and review all email traffic that comes to and from individual and group email accounts.

Internet Use for Staff

The School provides internet access to employees to assist with performance of their duties.

Personal Use

Whilst the internet should primarily be used for business functions, incidental and occasional use of the internet in a personal capacity may be permitted so long as:

- Usage does not tarnish the reputation of the School,
- Employees understand that School management may have access to their internet browsers and browsing history contained within,
- Employees understand that the School reserves the right to suspend internet access at any time,
- Use of the internet for personal use does not infringe on business functions.

Inappropriate Use

The School does not permit individuals use the internet in a way that may be interpreted as insulting, disruptive, or offensive by any other individual or entity. The use of computer systems without permission or for inappropriate purposes is a criminal offence (Computer Misuse Act 1990). Examples of prohibited material include, but are not necessarily limited to:

- Sexually explicit or pornographic images, cartoons, jokes or movie files,
- Images, cartoons, jokes or movie files containing ethnic, religious, or racial slurs,
- Any content that could be construed as harassment or disparagement of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs, or political beliefs.

Individuals are also not permitted to use the internet in a way which could affect usage for others. This means not streaming or downloading media files and not using the internet for playing online games.

Other Business Use

Users are not permitted to use the internet to carry out their own business or business of others. This includes, but not necessarily limited to, work for political organisations, not-for-profit organisations, and private enterprises. This restriction may be lifted on a case by case basis at the discretion of School management.

Internet Security

Users will take care to use the internet in accordance with the School's information security policy. In particular users will not click on links to un-trusted or unverified WebPages.

Staff and Governors must agree to and sign the Acceptable Use Agreement at the start of their employment/term of office.

Internet use for Pupils

Pupils who are to have access to the internet must understand the basic conventions and navigation techniques before going online and accessing material.

Pupils must not use the school ICT facilities without the supervision of a member of staff and ICT facilities are not available when an adult is not present. Although use of the ICT facilities and access to the Internet will be supervised, and all possible measures will be taken (including the use of Newcastle LEA firewall), Lemington Riverside Primary School and Newcastle City Council cannot accept liability for the accessing of inappropriate materials or any consequences of internet access.

Lemington Riverside Primary School is protected by the internet filtering company Smoothwall. This is a live web filtering system which monitors any inappropriate material viewed on a school computer. This material can be used as evidence in circumstances where a computer has been used to access such inappropriate material. The filtering policies for staff and students were reviewed during and agreed in November 2018.

If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the ICT subject leader and school office who will pass information onto the ICT Technician immediately who will, in turn, record the address and report on to the Headteacher, ICT services and Internet Service Provider.

Through e-safety lessons, pupils must be made are aware of the following:

- they must only access those services they have been given permission to use.
- they must not attempt to gain access to the school network or any Internet resource by using someone else's account name or password.
- the use of computer systems without permission or for inappropriate purposes is a criminal offence (Computer Misuse Act 1990).

The school strives to provide access to a broad and balanced curriculum for all learners and recognises the importance of tailoring activities to suit the educational needs of each pupil. Where a pupil has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of e-safety awareness sessions and internet access.

Social Media Use

The school recognises and embraces the benefits and opportunities that social media can contribute to an organisation. The school also recognises that the use of social media is a data protection risk due to its open nature and capacity to broadcast to a large amount of people in a short amount of time.

The school uses social media accounts on Facebook, Twitter and Instagram across multiple platforms. Nominated employees will have access to these accounts and are permitted to post general information about the School. Authorised employees will be given the usernames and passwords to these accounts which must not be disclosed to any other individual within or external to the organisation. Craig Heeley (Head Teacher) will have overall responsibility for allowing access to social media accounts. Any additional social media accounts that school use in the future will adhere to the same guidelines as above.

Corporate Social Media Accounts must not be used for the dissemination of personal data either in an open forum or by direct message. This would be a contravention of the School's information governance policies and data protection legislation.

Corporate Social Media Accounts must not be used in a way which could:

- Tarnish the reputation of the School,
- Be construed as harassment or disparagement of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs, or political beliefs.
- Be construed as sexually explicit,
- Construed as political beliefs or commentary.

Personal Accounts

The School understands that many employees will use or have access to Personal Social Media Accounts. Employees must not use these accounts:

- During working hours,
- Using corporate equipment,
- To conduct corporate business,
- To contact or approach clients, customers, parents or partners of the school.

Staff who use social media must ensure that their security settings are adjusted to safeguard themselves and the school. Staff must ensure:

- Their profile is private – all settings 'just friends'
- Profile picture and cover photo are deemed appropriate.
- They do not 'like' or 'share' any inappropriate content (for example, racism, sex, extreme views and radicalisation).
- Any references to school, both stated and implied are not made at any time. This includes photographs or written statements.

- That no photographs are taken anywhere in the school on personal devices during teaching hours and that no photographs linked to school are uploaded on social media.

General Equipment Safety

The consumption of food or drink is forbidden whilst using a computer. It is hazardous to the equipment and to individuals.
Users must treat with respect equipment and services in school and at other sites accessed through school facilities, and are subject to regulations imposed by the respective service providers. Malicious action will result in immediate suspension from use of the school facilities.

Legal Requirements

Users must agree to comply with all software license agreements. Do not attempt to copy any software from, or by using school computers. Employees must request authorisation from Craig Heeley (Head Teacher) if they would like to request any new software added to the School's IT systems. IT Support will check if the software provider is on the approved Department of Education Cloud (educational apps) list. If the software provider is not on the list the software request will not be agreed until the DFES Cloud Computing Questionnaire has been completed and checked by the NCC IT Service security team. NCC IT Services will retain a list of trusted software so that this can be downloaded on to individual desktops without disruption. Remember also that shareware is not freeware and must be licensed for continued use.

Copyright Designs & Patents Act - Copyright is infringed if a person acquires an unauthorised copy of a computer program. Mere acquisition, without regard to the actual or intended use, constitutes an infringement of the author's copyright. "Acquisition" includes loading a copy of a programme into the random access memory, or other temporary storage device, of a computer, or onto any form of permanent data storage medium.

The high cost of commercially marketed software and the ease with which it can be copied make it tempting to copy software illegally. Agents for software developers are aggressively seeking to protect their rights under the law. Schools can be audited at any time. Anyone found to have unauthorised copies of software will immediately be suspended from using the IT facilities. The matter will be investigated and the necessary action taken, the school will not accept any liability whatsoever.

"Hacking" is illegal under the Computer Misuse Act 1990. Regulations regarding unauthorised access or misuse of computing facilities are enforceable under the law, any person found attempting to or hacking the school network will be prosecuted.

Regulations regarding the transmission, storage or display of obscene material are enforceable by law under the Criminal Justice and Public Order Act 1984 which amends the Obscene Publications Act 1956, the Protection of Children Act 1978 and the Telecommunications Act 1984 to extend their provisions to transmission over a data communications network.

Sanctions for Pupils

If pupils break the rules as laid down by this policy, they will lose temporary or permanent use of the school systems. Parents will be informed and if the law has been broken the police will be informed and the school will assist the police with any prosecution.

Disciplinary Procedure for All School Based Staff

In the event that a member of staff may be seen to be in breach of behaviour and good conduct through misuse of online technologies, the Disciplinary Policy outlines the correct procedures. If the law has been broken the police will be informed and the school will assist the police with any prosecution.

Local Authority Designated Officer (LADO) - Managing Allegations

The Local Authority has designated Officers who are involved in the management and oversight of individual cases where there are allegations against an adult in a position of trust. They provide advice and guidance to all of the above agencies and services, and monitor the progress of the case to ensure all matters are dealt with as quickly as possible, consistent with a thorough and fair process. In addition to this they liaise with the police and other agencies.

Cyber Bullying

The experience of being cyber bullied can be very painful for those who are the targets. Adults need to help children and young people prepare for the hazards of using technology while promoting learning and social opportunities. Some forms of cyber bullying are different from other forms:

- Through various media children can be cyber bullied 24 hours a day.
- People who cyber bully may attempt to remain anonymous.
- Anyone of any age can cyber bully.
- Some instances of cyber bullying may be unintentional – such as a text sent as a joke or an email to the wrong recipient.

Prevention of Cyber Bullying

We recognize that the best way to deal with cyber bullying is to prevent it from happening in the first place. By embedding good, safe ICT practice into all our teaching and learning, incidents can be avoided. E-Safety is taught across the school every half-term. Teachers also refer to online safety throughout computing topics. Our community's principals of e-safety are based on "Key Safety Advice – CyberBullying (DCSF 2007).

We recognise we have a shared responsibility to prevent incidents of cyber bullying . Craig Heeley (Head Teacher) has the responsibility for coordinating and monitoring the implementation of anti-cyber bullying strategies.

Understanding Cyber Bullying

The school community is aware of the definition of cyber bullying and the impact cyber bullying has.

Staff receive guidance and review the Anti-Bullying and Acceptable Use Policies regularly. Children are taught how to recognise cyber bullying and their responsibilities to use ICT safely. ICT safety is integral to teaching and learning practice in the school.

Parents are also taught how to recognise cyber bullying and their responsibilities for supporting safe ICT use. The school provides regular parental updates on e-safety and an e-safety advice section on its website.

Cyber Bullying Record Keeping and Monitoring Safe Practice

As with other forms of bullying, the Head Teacher keeps records of cyber bullying on CPOMS. Incidents of cyber bullying will be followed up using the same procedures as other forms of bullying.

Online-Safety

Children and staff are reminded of E-Safety Codes of Conduct at the start of each academic year. Every year, parent/child e-safety sessions will be led in school (with a representative from the Extended Services team).

- Under no circumstances should you give out personal email or postal addresses or telephone numbers of any person, including the staff and pupils at the School.
- Distribution of computer viruses, electronic chain mail, computer games, use of Internet Relay Chat and similar services are strictly forbidden by pupils and staff as they can result in degradation of service for other users and they are inappropriate and do not adhere to our school rules.
- Do not download, use or upload any material that is copyright. Always seek permission from the owner before using any material from the Internet. If in doubt, or you cannot obtain permission, do not use the material.
- Users should assume that ALL software is subject to copyright restrictions, including shareware. Pupils must not, under any circumstances download or attempt to install any software on the school computers. Staff should seek the advice of Craig Heeley (Head Teacher) if they would like to download or upload software.
- Under no circumstances should users view, upload or download any material that is likely to be unsuitable for children or schools. This applies to any material of violent, dangerous, racist, or inappropriate sexual content. If users are unsure about this, or any materials, users must ask teachers or ICT co-ordinator. If in doubt, DO NOT USE. The transmission, storage, promotion or

display of offensive, defamatory or harassing material is strictly forbidden as they breach the laws of the UK under the Computer Misuse Act. Possession of certain types of unsuitable material can lead to prosecution by the police.
- Search engines (such as Google) are not to be used to search for websites or images unless the learning objective specifically demands it.

Use of the School Network

- Always respect the privacy of files of other users.
- Do not modify or delete the files of other users on the shared areas without obtaining permission from them first.
- The ICT technician and subject leader will view any material pupils store on the school's computers.
- Storage space on the network is limited. All users are requested to ensure that old unused files are removed from their area at the end of each academic year. Users unsure of what can be safely deleted should ask their subject leader or ICT technician for advice. In exceptional circumstances, increased storage space may be allowed by agreement with the ICT technician.
- Users accessing software or any services available through school facilities must comply with licence agreements or contracts relating to their use and must not alter or remove copyright statements. Some items are licensed for educational or restricted use only. Visitors will receive a guest login that limits access to the network.
- Be polite and appreciate that other users are entitled to differing viewpoints. The use of strong language, swearing or aggressive behaviour is forbidden. Do not state anything that could be interpreted as libel.
- If the network is accessed from home, this Acceptable Use Policy applies.

General Security Guidelines

Backups

All files saved on the network are stored on a local server in school. The data on the server is backed up every evening to the Newcastle City Council (Local Authority). This means files can be restored if deleted or lost in error. However, if you create and delete files on the same day then a backup will not be available to restore.

Save Regularly

It is very important to save work regularly (approx. every 10 minutes). The network is very reliable but problems do occur i.e. programs crash, power failures. If work is saved regularly and a PC or the network does fail for any reason, only the work done since the last save will be lost. If you are working in Office 365, a copy of your document is saved automatically to the cloud.

Use your Network Area

Always ensure that files are saved to your network area, NOT on the local hard drive (your C drive). This will ensure that your work is backed up and can be retrieved in the event of a hardware failure or theft.

Personal Documents

The school cannot accept responsibility for personal documents held on school equipment.

Offsite pupil data and pupil information

Staff must use remote access or one drive (Office 365) to access pupil data and information between home and school. Files must NOT be saved on the local hard drive of the laptop (your C drive).

Virus Checks

All computers in school have anti-virus software, although very new viruses will not be found. If you suspect a virus please report it to the ICT technician straight away and/or record in the ICT problem book if ICT Technician is not available.

Mobile Devices

- Pupils in Years 3/4/5/6 are permitted to bring mobile phones to school, but these must be switched off and handed to the office upon arrival. They can then be collected from the office at home time.
- Any pupil without permission who is seen with a mobile device during the school day will have their phone removed from them to be collected at the end of the school day by a parent or carer. The device will be secured in the school office.
- Pupils may not make or take personal calls or send/receive text messages or social media messages from a mobile phone during the school day.
- Mobile phones may not be used to take pictures of pupils and staff (use class cameras/ipads provided by the school).
- Any inappropriate use of mobile devices, such as cyber bullying, during the school day must be reported to the Head Teacher (see Cyberbullying).
- Parents/Carers will be reminded that personal mobile phones should be turned off or set to silent and must not be used when in school.
- Parents/Carers will be allowed to photograph their own children at the end of productions, assemblies etc. It is not permitted to take any photos or videos during any productions, assemblies or other events for safeguarding reasons. Parents will be reminded of this before any event to protect the identity of other children.
- All visitors will be reminded that personal mobile phones should be turned off or set to silent and must not be used when in school unless permitted to do so by a member of school staff.
- Staff should only use their mobile phones at appropriate times of the day only e.g. break times. During the school day their mobiles should be turned off or set to silent. These devices must be kept in a secure area away from areas where children access. Staff must not use personal mobile devices or cameras to take images of pupils or staff. On school visits, staff may use their mobile phone to contact school in the event of an emergency.

School Telephone Use

Personal Use

Whilst the telephone should primarily be used for business functions, incidental and occasional use of the telephone in a personal capacity may be permitted so long as:

- Usage does not tarnish the reputation of the School,
- Employees understand that School management may have access to call history,
- Employees understand that the School reserves the right to suspend telephone usage at any time,
- Use of the telephone for personal use does not infringe on business functions.

Inappropriate Use

The School does not permit individuals to use the telephone in a way that may be interpreted as insulting, disruptive, or offensive by any other individual or entity.

Other Business Use

Users are not permitted to use the telephone to carry out their own business or business of others. This includes, but not necessarily limited to, work for political organisations, not-for-profit organisations, and private enterprises. This restriction may be lifted on a case by case basis at the discretion of School management.

Video-Conferencing and Webcams

Permission should be sought from parents and carers if their child is engaged in video conferencing with individuals or groups outside of the school. This process should always be supervised by a member of staff and a record of dates, times and participants held by the school.

Children need to tell an adult immediately of any inappropriate use by another child or adult. (This is part of the Acceptable Use Agreement).

Where children, young people (or adults) may be using a webcam in a family area at home, they should have open communications with parents/carers about their use and adhere to the Acceptable Use Agreement.

Managing Allegations against Adults Who Work With Children and Young People

In order to deal with any incidents that occur as a result of using personal mobile or e-mail technologies we will refer to the Head Teacher. The procedures detail how to deal with allegation of misuse or misconduct being made by any member of staff or child about a member of staff.

Allegations made against a member of staff should be reported to the Designated Safeguarding Lead (Craig Heeley – Head Teacher) within the school immediately. In the event of an allegation being made against a Head teacher, the Chair of Governors should be notified immediately.

Local Authority Designated Officer (LADO) - Managing Allegations:
The Local Authority has designated Officers who are involved in the management and oversight of individual cases where there are allegations against an adult in a position of trust. They provide advice and guidance to all of the above agencies and services, and monitor the progress of the case to ensure all matters are dealt with as quickly as possible, consistent with a thorough and fair process. In addition to this they liaise with the police and other agencies.

Additional Information

When pupils and employees leave Lemington Riverside Primary School, their user account and any associated files and email address and any associated emails will be removed from the school system and will no longer be accessible. The school cannot continue to receive emails sent to an email address that has been disabled.
If pupils, staff or parents do not understand any part of this Acceptable Use Policy, please ask the Headteacher and subject leader for further guidance.
A copy of this policy can be accessed by visitors via our school website.

Named Personnel

Our Named Governor for ICT Acceptable Use is Margaret Shipley.

The Person Responsible for E-Safety and Acceptable ICT Use is Craig Heeley (Head Teacher)

Policy Reviewed by Craig Heeley and Victoria Jeffcock (ICT Leader) February 2019

Review – February 2020

Approved by ______________________________ (Chair of Governors)

Date________________