Internet Acceptable Use Policy

Contents:

1. Statement of intent

Whilst our school promotes the use of technology and understands the positive effects it can have on enhancing pupils' learning and community engagement, we must also ensure that technology is used appropriately. Any misuse of technology will not be taken lightly and will be reported to the headteacher in order for any necessary further action to be taken.

This acceptable use policy is designed to outline staff responsibilities when using technology, whether this is via personal devices or school devices, or on/off the school premises, and applies to all staff, volunteers, contractors and visitors.

2. Introduction

1.1. This policy applies to all employees, volunteers, supply staff and contractors using school ICT facilities.

1.2. The school acceptable use policy is divided into the following three sections.

General policy and code of practice
Internet policy and code of practice
Email policy and code of practice

3. Aims of the policy

This policy aims to:

- Ensure that all pupils and staff make appropriate use of the Internet for professional and educational purposes.
- Ensure that Internet use is monitored and managed appropriately.
- Provide a system by which staff and pupils are protected from inappropriate sites, information and individuals.
- Provide rules that are consistent with procedures already used on the Internet.

The Internet is an essential means of communication. The Government has made it clear that all schools need to exploit the use of the Internet.

Langmoor Primary School has connection to the Internet via a Broadband connection. EMPSN provide the Broadband connection, filtering provided by RM Unify and email is accessed through Office 365.

There is no regulatory body for the Internet, anyone can publish on the Internet and the filtering of inappropriate material on the Internet cannot be 100 % effective. For these reasons, the school has put other systems in place to ensure that the pupils and staff in our school are as safe as possible when using the Internet.

There are seven elements in place to ensure that the use of the Internet is safe and effective:

1. An Internet policy, which is frequently reviewed and updated.
2. Information to parents which highlights the use of the Internet.
3. Adequate staff training.
4. Adequate supervision of children whilst using the Internet using Net Controller.
5. A contract between child, parent and school.
6. The filtering of undesirable sites through the use of an educational Internet Service Provider.
7. A clear set of rules that pupils are expected to adhere to, and sanctions which will be implemented should children choose not to follow the school rules.

4. General policy and code of practice

3.1. The school has well-developed and advanced Computing and ICT systems, which it intends for you to benefit from.

3.2. This policy sets out the rules that you must comply with to ensure that the system works effectively for everyone.

Privacy

3.3. The GDPR and Data Protection Act 2018 require all personal and special category data to be processed with the utmost credibility, integrity and accuracy. This applies to all data the school stores on its network regarding staff, pupils and other natural persons it deals with whilst carrying out its functions.

3.4. The school will only process data in line with its lawful basis to uphold the rights of both pupils and staff and other third parties.

3.5. In order to protect pupils' safety and wellbeing, and to protect the school from any third party claims or legal action against it, the school may view any data, information or material on the school's Computing and ICT systems (whether contained in an email, on the network, notebooks or laptops) and in certain circumstances, disclose that data, information or material to third parties, such as the police or social services. The school's Privacy Policy details the lawful basis under which the school is lawfully allowed to do.

Code of practice

Times of access	The network is available during term time. Out of term time the network will be subject to maintenance downtime and so may not be available for brief periods.
User ID and password and logging on	You will be given your own user ID and password. You must keep these private and not tell or show anyone what they are. Your password must be a mix of the following: Contain at least six characters A mixture of lower case and capital letters At least one number At least one special character If you forget or accidentally disclose your password to anyone else, you must report it immediately to the school Computing and ICT technician. You must not use another person's account or allow another person to use your account. The facilities are allocated to you on a personal basis and you are responsible for the use of the machine when you are logged on. The school's system records and Computing and ICT technician monitor your use of the system. Use of the school's facilities by a third party using your user name or password will be attributable to you, and you will be held

	accountable for the misuse.
Logging off	You must log off from the computer you are using at the end of each of your sessions and wait for the standard login screen to reappear before leaving. This signals to the system that you are no longer using the service; it ensures security and frees up resources for others to use.
Access to information not normally available	You must not use the system or the internet to find or use facilities or flaws in the system that might give access to information or areas of the network not normally available. You must not attempt to install software to explore or harm the system. Use of hacking tools, e.g. 'loggers', 'sniffers', or 'evidence elimination software', is expressly forbidden
Connections to the system	You must not connect any hardware which may be detrimental to the school's network
Connections to the computer	You should use the keyboard, mouse and headphones provided. You must not adjust or alter any settings or switches without first obtaining the permission from the Computing and ICT technician You must never attempt to use any of the connections on the back of any desktop computer You may use USB memory sticks, or other portable storage media where a port is provided on the front of the computers. You are no permitted to connect anything else to the computer without first getting the permission of the Computing and ICT lead.
Virus	If you suspect that your computer has a virus, you must report it to the Computing and ICT technician immediately
Installation of software, files or media	You must not install or attempt to install software of any kind to network drives or local hard drives of networked desktop computers. You must not alter or re-configure software on any part of the school's system
File space	You must manage your own file space by deleting old data rigorously and by deleting emails that you no longer require.

	If you believe that you have a real need for additional space, please discuss this with the Computing and ICT technician.
Transferring files	You may transfer files to and from your network home directories using removable devices. When transferring files to and from your network home directories, you must not import or export any material unless the owner of that material expressly permits you to do so.
Reporting faults and malfunctions	You must report any faults or malfunctions to the Computing and ICT technician, including full details and all error messages, as soon as possible.
Food and drink	You must be careful of food and drink near the computers.
Copying and plagiarising	You must no plagiarise or copy any material which does not belong to you.
Copies of important work	It is your responsibility to keep paper copies and back-up copies, e.g. on a CD or memory stick, of your work, and you must keep copies of any important work that you might have. Any data containing personal and special category data must not be stored on unencrypted media and paper back-ups must be stored in a secure lockable location.

5. Internet policy

Access to the Internet

Pupils are encouraged to make use of the information rich resources that are available on the Internet. Pupils will be taught the skills needed to analyse and evaluate such resources.

On-line resources have opened up classrooms to a much broader array of resources. Electronic information research skills are now fundamental to the preparation of future

employees in this information age. Staff will explore the possibilities and encourage the use of such research skills as appropriate in the wider curriculum.

There are two categories of users who will make use of the school's Internet facilities:

- Teaching staff
- Pupils

Pupils will always be supervised when using the Internet and will need a parent/guardian to sign an Internet Permission letter (*see appendix A).*
A list of Internet Guidelines that all pupils are expected to adhere to *(see appendix B).* These guidelines will be kept under review.
All members of staff are responsible for explaining the rules and the implications to pupils. All staff should be aware of possible misuses of Internet access and their responsibilities towards the pupils in their care.

Breaches of the Acceptable Use Policy rules by pupils or adults could result in one of the following:

- A warning
- E-mail and/or Internet facilities removed
- Letter home to parents / reported to the Governors
- Reported to appropriate external agencies

Security when using the Internet:

- Computers with Internet access are situated where the screen can be seen by the teacher.
- All workstations connected to the Internet have appropriate anti-virus software installed (Sophos). The anti-virus software is updated regularly.
- Pupils are not allowed to bring in USB sticks and upload files from home themselves. Any homework brought into school using USB sticks will be opened up by adults.
- Pupils are not given access to 'open' newsgroups or Chat rooms.
- Each member of teaching staff will be allocated their own e-mail address. This includes the office.
- Any emails sent and received by pupils will be done in Purple Mash. This programme allows admin to monitor the content and children do not have access to these outside of school. This will mainly be used in Computing.
- The school is aware of the need to protect pupils from undesirable contact with adults via e-mail. All e-mail messages sent and received are supervised. A facility is available to restrict where the children can send their e-mails.
- Any inappropriate material found on the Internet will be reported to the ISP (EMPSN). *The Computing and ICT Lead will be the point of contact.*

Managing Internet Access:

- Internet access will be purchased from a supplier that provides a service designed for use within an educational establishment. The service will include filtering.
- The school will work with RM Unify to ensure systems that protect the pupils and staff are reviewed and updated.
- Internet access will be part of planned lessons.
- All pupils using the Internet will be supervised.
- Pupils will be given very clear objectives for Internet use.
- Parents will be asked to sign and return an Internet Permission letter. (*see Appendix A)*
- Pupils will be asked to sign and return an Internet permission letter to show that they agree to observe the rules set out.
- Pupils will be educated in taking responsibility in Internet access.
- Staff will ensure that sites are viewed prior to the lesson to ensure that the resources are appropriate.
- The school will provide a list of websites suitable and relevant to pupils' work in school (displayed on the school website).
- A record will be held of all staff and pupils with Internet access.

Managing Web Publishing:

More and more schools are developing their own websites as a means of celebrating good work and publicising the school. However, there are issues that need to be considered.

When the school publishes its website, it is available to anyone in the public domain. It is essential that the information is accurate and that the children are kept as safe as possible.

- There should be one person within school (or employed by the school) who has been designated website editor. Any materials to be put onto the website should go to them first. This is the Head teacher in the first instance.
- Head teachers and Governors will make decisions about what they consider to be suitable and appropriate to go onto the Website.
- The use of images of named individuals will be avoided.
- Photographs will be uploaded anonymously.
- Any children whose parents have requested that their images are not used publicly will be excluded from any material that is published to the website.

6. Email policy

Managing e-mail:

5.1. The school's computer system enables members of the school to communicate by email with any individual or organisation with email facilities throughout the world.

5.2. For the reason outlined above, it is essential that a written policy and code of practice exists, which sets out the rules and principles for use of email by all.

5.3. Any breach of this policy and code of practice will be treated seriously and it may result in disciplinary or legal action or expulsion.

5.4. The school may take steps, including legal action where appropriate, to recover from an individual any expenses or liabilities the school incurs because of the breach of this policy and code of practice.

Code of Practice

- Staff should use e-mail in school for professional use only.
- The use of e-mail as a form of communication is managed by staff to ensure appropriate educational use.
- Copies of all incoming and outgoing emails, together with details of their duration and destinations are stored centrally (in electronic form).
- The frequency and content of incoming and outgoing external emails are checked to determine whether the email system is being used in accordance with this policy and code of practice.
- As with anything else sent over the internet, emails are not completely secure. There is no proof of receipt, emails can be 'lost', they can suffer from computer failure and a determined 'hacker' could intercept, read and possibly alter the contents.
- As with other methods of written communication, you must make a judgement about the potential damage if the communication is lost or intercepted. Never send bank account information, including passwords, by email.
- The forwarding of chain letters is banned.
- The sending of anonymous letters is banned.
- Pupils may send e-mail as part of a planned lesson, but they will not be given individual email addresses.
- Children must not give any personal details to any person or organisation within an e-mail.

Staff members should consider the following when sending emails:

- Whether it is appropriate for material to be sent to third parties
- The emails sent and received may have to be disclosed in legal proceedings
- The emails sent and received may have to be disclosed as part of fulfilling an SAR

- Whether any authorisation is required before sending
- Printed copies of emails should be retained in the same way as other correspondence, e.g. letters.
- To use blind copy on group emails
- The confidentiality between the sender and recipient
- Transmitting the work of other people, without their permission, may infringe copywrite laws.
- The sending and storing messages or attachments containing statements which could be construed as abusive, libellous, harassment may result in disciplinary or legal action being taken.
- Sending or storing messages or attachments containing statements which could be construed as improper, abusive, harassing the recipient, libellous, malicious, threatening or contravening discrimination legislation or detrimental to this is a disciplinary offence and may also be a legal offence.

7. Email policy – advice to staff

7.1. Staff should remind themselves of the ICT Acceptable Use Policy which relates to the monitoring, security and quality of emails. In addition, staff should be guided by the following good practice:

Staff should check their emails daily and respond, as appropriate, within a reasonable period if the email is directly addressed to them.

Staff should avoid spam, as outlined in this policy.

Staff should avoid using the email system as a message board and thus avoid sending trivial global messages.

Whilst accepting the convenience of the staff distribution list, staff should try to restrict its use to important or urgent matters.

Staff should send emails to the minimum number of recipients.

Staff are advised to create their own distribution lists, as convenient and appropriate.

Staff should always include a subject line.

Staff are advised to keep old emails for the minimum time necessary.

Updated September 2023