E-Mail and Internet Use Policy
September 2017

1. Introduction

Schools are using E-mail and the Internet more and more to support their activities. This E-mail and Internet use policy, which will form part of our ICT Security Policy, contains the rules for using the E-mail and Internet facilities. It applies to all school staff who use either or both of these facilities.

As well as saying what you are not allowed to use E-mail and the Internet for, the policy also provides guidance on the good practices that you should use and the practices that you should avoid.

The school will periodically review the policy in response to guidance issued by the County Council.

2. Access to E-mail and Internet services

2.1 Your connection to E-mail or the Internet must be authorised (in writing or in electronic form) by your System Manager. All school Internet access will be via an approved Internet Service Provider (ISP). Any variations to this must be authorised in writing by the Headteacher.

You must choose the ISP’s filtering option if one is available.

The school E-mail and Internet facilities are for business use but we will allow staff to use them privately, as long as it is reasonable. If you use these facilities, you must keep to and not break any of the conditions in this policy.

2.4 The school has the right to monitor E-mails and Internet use.

2.5 If you intentionally access a computer system or information without permission, you are breaking the law under the Computer Misuse Act 1990.

3. Code of Conduct Declaration

If you use or have access to our E-mail or Internet facilities, you need to read this policy carefully and make sure that you understand it. The school will provide appropriate training. You then need to sign the declaration / consent form (see Annex C1 – C3) to confirm that you have read, understood and will keep to the policy. You must also understand that we may take action against you if you wilfully break the conditions of the policy.

3.2 The school will keep the signed declaration in your personal file. Sometimes, we may ask you to confirm that you still understand and accept the rules.

4. Specific Conditions of Use

4.1 General prohibitions

4.1.1 You must not use, or try to use, our E-mail and Internet facilities to create, distribute or display in any form, any activity that is or may be considered to be against the law or against our rules and policies. In this context, you are not allowed to use the E-mail and Internet facilities for reasons that are:

- pornographic or obscene;
- intimidating, discriminatory (for example; racist, sexist or homophobic) or that break our anti-harassment and equal opportunities policies in any other way;
- defamatory;
- encouraging violence or strong feelings;
- hateful;
- fraudulent;
- showing or encouraging violence or criminal acts;
- unethical or may give us a bad name; or
- a deliberate harmful attack on systems we use, own or run.

4.1.2 We will only allow you to do the above if:

it is part of your job to investigate illegal or unethical activities;

your Headteacher or System Manager asks you to in writing; or

it is in the public interest.

You must make sure that your System Manager knows what you are doing. If you find or suspect anyone of using the computer system illegally or unethically, you must report it to your System Manager who will advise your Headteacher or Chair of Governors or Internal Audit.
4.1.3 You must not use the school E-mail or Internet facilities for time-wasting activities, such as chain letters, or for sending private E-mails to everyone on the global address list.

4.2 Computer viruses
4.2.1 It is a crime to deliberately introduce a computer virus, under the Computer Misuse Act 1990. You must not use the school E-mail and Internet facilities for:
intentionally accessing or transmitting computer viruses or other damaging software; or
intentionally accessing or transmitting information about, or software designed for, creating computer viruses.
4.2.2 You must scan any material you receive or download from the Internet to make sure it is virus free. The school will ensure that virus protection exists on any standalone or locally networked computers that can access the Internet and train you in its use. You must not E-mail material that has not been scanned to other users. If you find a virus, or you think the material has one, you must immediately break the connection, stop using the computer and tell your System Manager.
4.2.3 You must always follow the instructions that your System Manager gives you about virus attacks.
4.2.4 If you are not sure how to use the virus protection system, you must get advice from your System Manager.

4.3 Passwords
4.3.1 You must not tell anyone your password, apart from authorised staff.
4.4 Other security
4.4.1 You must not use or try to use the school facilities for:
accessing or transmitting information about, or software designed for, breaking through security controls on any system;
breaking through security controls on any system; or
accessing, without permission, any E-mail that is not for you, even if it is not protected by security controls.

4.5 Publishing information
4.5.1 You must get authorisation from the Headteacher for any school information that is to be published on the Internet. All schools have web space available for authoring of their own school web site. Images of individuals must have their permission or that of their parent/guardian before publication of the web site (see Annex C2). We will not allow the publishing or editing of Web sites which involve advertising, financial reward or are part of a business.

4.6 Copyright
4.6.1 It is illegal to break copyright protection. You could break copyright if you download or transmit protected material through E-mail or over the Internet.
4.6.2 You must not:
transmit copyright software from your computer to the Internet or allow any other person to access it on their computer through the Internet; or
knowingly download or transmit any protected information that was written by another person or organisation without getting permission from the owner.
Permission can be sought via e-mail.

4.7 Confidential or sensitive information
You must not break the conditions of the Data Protection Act 1998 when you use the E-mail services of the Internet for transmitting information.
If you need any more advice about these conditions, you should refer to the Policy summary or obtain further information/advice from the System Manager.
4.7.2 The Internet E-mail facility is not a secure way of transmitting confidential, sensitive or legally privileged information unless there are special security measures (such as encryption). Without these security measures, Internet E-mail is as insecure as a postcard that you send through the normal post. So, you should

make sure that the Internet is suitable for transmitting information that you feel is confidential, sensitive or legally privileged. If you allow anyone to see this type of information without permission, you may be breaking the law.

4.7.3 If you have to transmit any E-mail over the Internet that you think contains confidential, sensitive or legally privileged information, no matter what special security measures you take, you are strongly advised to include the following disclaimer in the E-mail.

'This E-mail (including any attachments) is only for the person it is addressed to. If you are not this person, you must delete this E-mail immediately. If you allow anyone to see, copy or distribute the E-mail, or if you do, or don't do something because you have read the E-mail, you may be breaking the law'. This disclaimer can be set using the ‘autosignature’ facility where this is available.

4.8 Bulletin board

4.8.1 There are ‘bulletin boards’ (electronic notice boards) on the County Council’s Intranet and the SLN Internet site for discussion, social and personal use. These ‘bulletin boards’ are moderated to ensure appropriate use. The conditions of use in this policy also apply to the bulletin boards.

4.8.2 Neither the school, the LEA nor the County Council is responsible for the content of any material included in the bulletin board or for anything users do because of the material.

5 Recording Internet use

5.1 You should be aware that use of ISP facilities is logged.

5.2 If you access a prohibited Internet site unintentionally, you must break the connection immediately and report it to your System Manager or Headteacher. If you do not do this, the school may take action against you.

5.3 You should protect yourself by not allowing unauthorised people to use your Internet facility.

1. Password Policy

   Passwords should be:
   - unique
   - alphanumeric
   - at least 6 digits in length
   - regularly changed, recommend at least every 90 days

   Passwords should NOT be:
   - written down
   - easy to guess

2. Monitoring Computer Use by Pupils
   - Ensure Pupil use of computers is 'visual', make sure there is a responsible person present and monitoring use
   - Consider logging access to the network using software tools, for example RM Tutor 3
   - Review the layout of the room to ensure there is good 'visibility' of computer activities
   - Ensure there is supervision at all times
   - Publish the ‘Rules of ICT Use’ next to the computers, or consider displaying them on or close to the screen when the computer is turned on
   - Maintain an audit trail of User activity

3. Monitoring Computer Use by Staff (especially in sensitive areas)
   - Use screensavers with passwords
   - Consider using 'distinctive' background colours
   - Think carefully about the location of equipment
   - Take care when disposing of paper output, floppy disks, computers etc that may contain sensitive or personal information

4. System Backup
   - Make sure the system is backed up regularly and checks are made that the backup has worked
   - Try to implement an automated system backup
   - Make sure the instructions for re-installing data or files from a backup are fully documented and readily available
   - Use 'off-site' storage for backup where possible
   - Consider using different media as a secondary backup facility

5. Anti Virus Protection
   - Always use an approved and recommended product
   - Make sure there is a process to ensure it is regularly updated and ALL equipment is included, this is especially important for stand-alone PC's, laptops and PC's used at home
   - Make sure there is a clear procedure for dealing with any actual or suspected infections
   - Make sure the process for 'cleaning' infections is documented - this may involve requesting assistance from the Council's ICT Unit

6. Illegal or Inappropriate Use of the Network
   - Make sure there are appropriate procedures in place for auditing access to the network and systems
   - Regularly check the network for 'unauthorised' files
   - If possible ensure auditing is performed both at the Management System level and also at the Operating System level
   - Consider using appropriate software to assist with auditing - this can help monitor activities such as logons, file usage etc
   - Consider using a firewall or proxy server to restrict external activity and access

7. Internet Use / Filtering
   - Make sure an Internet Use policy has been adopted for each 'category' of User and all Users have signed up to it
   - Define and document any local agreements / policies on restricting web sites, access to newsgroups and chat-rooms etc
   - Obtain parental permission where appropriate
   - Ensure there is a clear process for reporting any access to inappropriate material
   - Consider restricting specific functions such as the downloading of .exe files
   - Publish safe guidelines
   - Make sure Internet use is supervised

8. Email Use
   - Make sure an Email Use policy has been adopted for each 'category' of User and all Users have signed up to it
   - Define and document any local policy on the use of email and email addresses, including the use of 'non-approved' email accounts
   - Consider implementing limits on inbox sizes, size and types of attachments etc
   - Be clear about what is considered 'appropriate' use of email and language
   - Involve staff, parents and students in these decisions

9. Documentation

   Ensure adequate documentation is available for
   - The network infrastructure
   - The network systems, hardware, software etc
   - Administration procedures
   - Housekeeping procedures

- Problem resolution

Ensure support disks, recovery disks, backups etc are available

10. Training
    - Ensure there is adequate training for System Managers and Users
    - Introduce 'good practice' guidelines where appropriate e.g. using screen savers with passwords

11. Authentication / Operating System Level Security
    - Consider using system policies to provide additional security
    - Ensure there is a rigorous policy for approval / removal of Users
    - Avoid the use of 'generic' accounts, where their use is unavoidable set up only for the duration of the particular requirement.
    - Limit the number of Administrator and Manager accounts
    - Avoid the use of Groups with Administrator or Manager rights
    - Only log on as Administrator or Manager when performing functions requiring this level of access, use an ordinary level User account where this is not required
    - Set clear security levels on the network and ensure these are documented and followed
    - Restrict access to applications and data areas where appropriate
    - Consider using 'read only' access where possible

12. Network Review
    - Monitor system downtime, ensure there are support arrangements in place to react to problems with critical equipment or infrastructure
    - Monitor performance of the network - ensure there is a process in place to develop and upgrade the network infrastructure and equipment as necessary
    - Monitor service disruption - ensure support arrangements are in place to resolve problems in a timely fashion
    - Regularly review appropriate documents e.g. Computer Security policy, Email and Internet Use policies, this could include reviewing official documents such as the BECTa 'Superhighway Safety'
    - Review procedures for dealing with all security breaches or compromises, whether deliberate or innocent

13. Monitoring Systems Usage
    - Monitoring of data on a school network could contravene Article 8 of the European Convention of Human Rights and Fundamental Freedoms, e.g. the right to respect for private and family life, which is protected by the Human Rights Act 1998. The Telecommunications (Lawful Practice) (Interception of Communications) Regulations 2000 also limit monitoring. The 2000 Regulations apply to all forms of electronic monitoring and interception irrespective of whether the material monitored is generated by private use or in the course of the school’s day to day activities.

    - A school may only monitor authorised private use of a computer system if it can justify monitoring on the basis that it is lawful, necessary and in the interests of amongst other things, the protection of health or morals or for the protection of the rights and freedoms of others. Schools should ensure that the monitoring is not out of proportion to the harm that could be done if the monitoring did not take place.