Rodings Primary School

Acceptable Use Policy

Date Policy was formally adopted	September 2017
Review Date	September 2018
Chair's Name	
Chair's Signature	

Core Values

Respect

Enjoyment

Care

Confidence

Challenge

IT and emerging technologies are an important part of the teaching and learning that occurs at Rodings Primary School. This policy provides procedures and guidelines to make sure that the learning that occurs at Rodings Primary School is safe, aids learning and is ultimately enjoyable.

This policy has been put together with the agreement of staff and governors.

Below is a set of guidelines that should be adhered to by all staff, governors and children. Any outside agency staff or visitors that will be dealing with technology within the school should also be made aware of the Acceptable Use Policy. With technology constantly evolving it is important that staff regularly review their own practice and apply common sense and basic online safety when using school systems or hardware.

This Acceptable Use Policy will be reviewed annually.

Networked resources, including Internet access, are available to children and staff in the school. All users are required to follow the conditions laid down in this policy. Any breach of these conditions may lead to withdrawal of the user's access; monitoring and or retrospective investigation of the users use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

These networked resources are intended for educational purposes, and may only be used for legal activities consistent with the rules of the school. Any expression of a personal view about the children, school or Essex County Council matters in any electronic form of communication must be endorsed to that effect. Any use of the network that would bring the name of the school or Essex County Council into disrepute is not allowed. The school expects that staff will use new technologies as appropriate within the curriculum and that staff will provide guidance and instruction to pupils in the use of such resources, children's independent use of the Internet or the schools. All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion.

CONDITIONS OF USE

Personal Responsibility

Access to the networked resources is a privilege, not a right. Users are responsible for their behaviour and communications. Staff and children will be expected to use the resources for the purposes for which they are made available. Users are to take due care with the physical security of hardware they are using. Users will accept personal responsibility for reporting any misuse of the network to the Headteacher or Computing Subject Leader. Any misuse will be recorded on the Online - Safety Log kept in the Headteacher's office.

Acceptable Use

Users are expected to utilise the network systems in a responsible manner. It is not possible to set hard and fast rules about what is and what is not acceptable but the following list provides some guidelines on the matter:

NETWORK ETIQUETTE AND PRIVACY

Users are expected to abide by the rules of network etiquette. These rules include, but are not limited to, the following:

1. Be polite – never send or encourage others to send abusive messages.

2. Use appropriate language – users should remember that they are representatives of the school on a global public system. Illegal activities of any kind are strictly forbidden.

3. Do not use language that could be calculated to incite hatred against any ethnic, religious or other minority group or encourage radicalism.

4. Privacy – do not reveal any personal information (e.g. home address, telephone number) about yourself or other users. Do not trespass into other users' files or folders.

5. Passwords – do not reveal your password to anyone. If you think someone has learned your password then contact the Computing subject leader.

6. Electronic mail – is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Do not send anonymous messages.

7. Disruptions – do not use the network in any way that would disrupt use of the network by others or stop the school from providing its core duty.

8. Pupils will not be allowed access to unsupervised and/or unauthorised chat rooms and should not attempt to gain access to them.

9. Staff or students finding unsuitable websites through the school network should report the web address to the Computing Subject Leader.

10. Do not introduce flash drives or external hard drives into the network without having them checked for viruses.

11. Do not attempt to visit websites that might be considered inappropriate. (Such sites would include those relating to illegal activity, all sites visited leave evidence in the county network if not on the computer). Downloading some material is illegal and the police or other authorities may be called to investigate such use.

12. Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.

13. Files held on the school's network will be regularly checked by the Headteacher.

14. It is the responsibility of the User (where appropriate) to take all reasonable steps to ensure compliance with the conditions set out in this policy document, and to ensure that unacceptable use of the Internet/Intranet does not occur.

15. Staff must not use their own personal phone, iPad or other digital device to take pictures of children or activities at school.

UNACCEPTABLE USE

Examples of unacceptable use include but are not limited to the following:

- Users must login with their own user ID and password, where applicable, and must not share this information with other users. They must also log off after their session has finished.
- Users finding machines logged on under other users username should not continue to use that machine until they have logged off then logged on using their username.
- Accessing or creating, transmitting, displaying or publishing any material (e.g. images, sounds or data) that is likely to cause offence, inconvenience or needless anxiety. (The County Council have filters in place to block e-mails containing language that is or may be deemed to be offensive.)
- Accessing or creating, transmitting or publishing any defamatory material.
- Receiving, sending or publishing material that violates copyright law. This includes through Video Conferencing and Web Broadcasting.
- Receiving, sending or publishing material that violates Data Protection Act or breaching the security this act requires for personal data.
- Transmitting unsolicited material to other users (including those on other networks).
- Unauthorised access to data and resources on the school network system or other systems.
- User action that would cause corruption or destruction of other users' data, or violate the privacy of other users, or intentionally waste time or resources on the network or elsewhere.
- Downloading software onto a school machine that is not for school use.

Additional guidelines

- Users must comply with the acceptable use policy of any other networks that they access.
- Users must not download software without approval from the Computing subject leader

SERVICES

There will be no warranties of any kind, whether expressed or implied, for the network service offered by the school. The school will not be responsible for any damages suffered while on the system. These damages include loss of data as a result of delays, non-deliveries, or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the network is at your own risk.

NETWORK SECURITY

Users are expected to inform the Computing Subject Leader immediately if a security problem is identified. Do not disclose this problem to other users. Users must login with their own user id and password, where applicable, and must not share this information with other users. Users identified as a security risk will be denied access to the network.

PHYSICAL SECURITY

Staff users are expected to ensure that portable IT equipment such as laptops, digital still cameras, iPads, and video cameras are not left in view when the school is unoccupied e.g. overnight or at weekends. Any portable IT equipment e.g. encrypted memory sticks or laptops must be registered and signed out to known member of staff. Signing for a piece of equipment means that the person has agreed to follow this policy and will endeavour to keep the piece of equipment protected and safe.

WILFUL DAMAGE

Any malicious attempt to harm or destroy any equipment or data of another user or network connected to the school system will result in loss of access, disciplinary action and, if appropriate, legal referral. This includes the creation or uploading of computer viruses. The use of software from unauthorised sources is prohibited.

MEDIA PUBLICATIONS

Named images of children (e.g. photographs, videos, web broadcasting, TV presentations, web pages etc.) must not be published under any circumstances. Written permission from parents or carers will be obtained before photographs of pupils are published on the school web site.

Also refer to the E-safety policy for further information about the internet and working with children.