Acceptable Use Policy
(Staff and Volunteers)

Why have an Authorised Acceptable Use Policy?

An Authorised Acceptable Use Policy is about ensuring that you, as a member of staff/volunteer/School Governor at Scole CEVC Primary School can use the Internet, email and other technologies available at the school in a safe and secure way. The policy also extends to out of school facilities e.g. equipment; printers and consumables; Internet and email, managed learning environment and websites.

An Authorised Acceptable Use Policy also seeks to ensure that you are not knowingly subject to **identity theft** and therefore **fraud**. Also that you **avoid cyber-bullying** and just as importantly, you **do not become a victim of abuse**. Certain sites which put the school network at risk are blocked by security software.

Scole CEVC Primary School strongly believes in the educational value of computing and recognises its potential to enable staff and volunteers in delivering and supporting the curriculum. Scole CEVC Primary School also believes that it has a responsibility to educate its pupils; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the Internet and other related technologies. To this end the expectation of Scole CEVC Primary School is that both staff and volunteers will play an active role in implementing school Internet safety polices through effective classroom practice.

Scole CEVC Primary School recognises that for staff and volunteers to effectively deliver and support the curriculum they must be able to make use of the ICT facilities of the school and have the opportunity to expand and develop the teaching material associated with their work. However, Scole CEVC Primary School expects that both staff and volunteers, will at all times, maintain an appropriate level of professional conduct in their own use of the school's ICT facilities.

Listed below are the terms of this agreement. Staff, School Governors and volunteers are expected to use the ICT facilities of the school in accordance with these terms. Violation of these terms by staff is likely to result in disciplinary action in accordance with school and local authority Disciplinary Procedures. Where the policy is breached by either volunteers or governors the school will seek advice and support from the Local Authority in order to manage the situation in a fashion that safeguards the school population.

Please read this document carefully and sign and date it to indicate your acceptance of the terms herein.

1. Equipment

1.1 School Computers

All computers and associated equipment are the property of Scole CEVC Primary School and must be used in accordance with this policy which adheres to the Computer Misuse Act 1990 and the Data Protection Act 1998 (see Glossary). The School assumes responsibility of maintenance of all hardware and software. Mis-use of equipment includes, but is not limited to the following:

- Modification or removal of software
- Unauthorised configuration changes
- Creation or uploading of computer viruses or other malware
- Deliberate deletion of files.
- The uploading of computer files to the school's network that are not related to work

Any of these actions reduces the availability and reliability of computer equipment, puts other users' data at risk and increases downtime caused by repairs, thus delaying other essential work such as upgrades or enhancements.

1.2 Laptop Computers

Laptop computers that have been distributed to staff remain the property of Scole CEVC Primary School at all times, and their usage is subject to the following guidelines:

- The equipment remains the property of Scole CEVC Primary School at all times and must be returned to the school at the end of the lease agreement or contractual period.
- The laptop computers may be taken home by staff but should only be used by the member of staff and solely for professional purposes.
- Maintenance of the equipment is the responsibility of Scole CEVCP. All maintenance issues must be referred to the headteacher.
- All installed software MUST be covered by a valid license agreement held by Scole CEVCP.
- All software installation MUST be carried out in accordance with the relevant license agreements.
- No software should be removed, uninstalled or disabled under any circumstances. Any software problems should be reported through the usual support channels.
- Antivirus software must be updated regularly. For laptop computers, it will be necessary to connect them to the school network to update the antivirus software. This should be done at least weekly.
- The user of the equipment is responsible for all personal files and data stored on the equipment. Backup of the data is the responsibility of the user. It is strongly recommended that all data is regularly backed up, either to a memory stick or to the Scole CEVC Primary School network. Where removable media is used the user must ensure that these mediums have not been used to download materials that are at risk of damaging the network.
- The user of the equipment must not encrypt any data or password protect any files so as to ensure future usage of the equipment.
- Scole CEVC Primary School cannot be held responsible for loss of data in the event of either a hardware or software failure or user error.
- From time to time, it may be necessary for the school to perform software updates and maintenance for which the equipment must be made available in School when reasonably requested.

1.3 Use of Removable Storage Media

Whilst staff may use flash memory devices to transfer files between home and school, Scole CEVC Primary School cannot guarantee the correct operation of any removable media or the integrity of any data stored on it.. Scole CEVC Primary School cannot guarantee the correct operation of flash memory devices on the system, although every effort is made to ensure that this facility is available.

1.4 Printers and Consumables

Printers are provided across the school for educational or work-related use only. All printer usage can be monitored and recorded.

- Proof-read your document on-screen and use the 'Print-Preview' facility to check the layout before printing.
- Do not print unnecessarily or waste ink or paper.
- Avoid printing directly from the Internet where possible. Internet pages are often not suitably formatted for printing and may cause wastage of paper and other consumables.

1.5 Data Security and Retention

All data stored on the Scole CEVC Primary School network is backed up daily and backups are stored for up to at least two weeks[1]. If you should accidentally delete a files or files in your folder or shared area, please inform the headteacher immediately so that it can be recovered. Generally, it is not possible to recover files that were deleted more than 2 weeks previously.

2. Internet and Email

2.1 Content Filtering

Scole CEVC Primary School provides Internet filtering, designed to remove controversial, offensive or illegal content. However, it is impossible to guarantee that all controversial material is filtered. If you discover any websites containing inappropriate or offensive content, please report these to theHeadteacher so that they can be filtered.

2.2 Acceptable use of the Internet

Use of the Internet should be in accordance with the following guidelines:

- Personal use of the internet will not normally be allowed except with the prior permission of the headteacher.
- Transmission of any material in violation of any United Kingdom or other national laws is prohibited. This includes, but is not limited to, copyrighted material, threatening or obscene material or material protected by trade laws
- Only access suitable material – using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.
- Respect the work and ownership rights of people outside the school. This includes abiding by copyright laws.
- Do not access Internet chat sites. These represent a significant security threat to the school's network.
- Staff should be mindful of using social networking sites. Privacy settings should be set to 'high' and staff should not be sharing information of a sensitive nature about aspects of school.
- The use of online gaming sites is prohibited. These consume valuable network resources that may adversely affect the performance of the system.
- If you wish to use content from websites, consider using the copy and paste facility to move it into another application, copyright permitting.

[1] The duration of data being stored on the school network is an issue that the school ICT Co-ordinator will need to decide upon in conjunction with the Headteacher and other members of he school leadership team.

- Do not attempt to download or install software from the Internet. The headteacher assumes responsibility for all software upgrades and installations.

- Staff are reminded that ALL Internet access is logged and actively monitored and traceable.

3.0 Privacy and Data Protection

3.1 Passwords

- Never reveal your password to anyone else or ask others for their password.

- When choosing a password, choose a word or phrase that you can easily remember, but not something which can be used to identify you, such as your name or address. Generally, longer passwords are better than short passwords. It is advisable to use a 'strong' password. A strong password is one which contains a combination of upper and lower-case letters, numbers and other punctuation characters. You can substitute numbers and letters for other characters that look similar, such as '3' for 'E', '1' for 'I' or '@' for 'O', '!' for '1' etc. This will help to make your password much more difficult to guess. Remember that passwords are case-sensitive.

- If you forget your password, please request that it be reset via the computing technician

- If you believe that a student may have discovered your password, then change it **immediately**.

3.2 Security

- Never attempt to access files or programs to which you have not been granted authorisation. Attempting to bypass security barriers may breach data protection regulations and such attempts will be considered as hack attacks and will be subject to disciplinary action.

- You should report any security concerns immediately to the Headteacher.

- Any user identified as a security risk will be denied access to the system and subject to disciplinary procedures as stated previously.

4.0 Mobile Technologies

For reasons of safety and security staff, governors and volunteers should not use their mobile phone or any other technology in a manner that is likely to bring the school into disrepute or risk the welfare of a child or young person. Staff and volunteers should not accept social network friends who are pupils and be mindful of friend requests from parents.

The development of mobile technology is such that mobile phones and other similar devices connected to mobile networks have enhanced features which include: picture messaging; mobile access to the Internet; entertainment in the form of video streaming and downloadable video clips from films, sporting events, music and games etc. The capabilities of 4G mobile phones also means that adults working within the school environment may be sent inappropriate images or videos, or be encouraged to send back images or video of themselves using integrated cameras.

In order to reduce the opportunity for those behaviours that could possibly cause upset, it is advisable that staff, governors and volunteers working with children and young people within the school setting, limit their use of mobile technologies to necessary communication during specified breaks during the school day.

If you are sent inappropriate material e.g. images or videos **report it immediately**.

Glossary

- Computer Misuse Act

  The Computer Misuse Act makes it an offence for anyone to have:-

  - Unauthorised access to computer material e.g. if you find or guess another user's password and use it.
  - Unauthorised access to deliberately commit an unlawful act e.g. if you guess another user's password and access their learning account without permission
  - Unauthorised changes to computer material e.g. if you change the desk-top set up on your computer or introduce a virus deliberately to the school's network system.

- Data Protection Act 1998

  The Data Protection Act ensures that information held about you is used for specific purposes only. These rules apply to everyone in the school.

  The Act covers the collection, storing, editing, retrieving, disclosure, archiving and destruction of data held about individuals in the school. The Act not only applies to paper files it also applies to electronic files.

  The Principles of the Act state that data must be:

  - Fairly and lawfully processed
  - Processed for limited purposes
  - Adequate, relevant and not excessive
  - Accurate and up to date
  - Kept no longer than necessary, in line with statutory guidance
  - Processed in accordance with data subject's rights
  - Secure
  - Not transferred to other countries without adequate protection

- RIPA – Regulation of Investigatory Powers Act 2002
  If a request for authorised access is made to the school they will provide the appropriate access to your ICT records and files. The Act legislates for using methods of surveillance and information gathering to help the prevention of crime, including terrorism. RIPA makes provision for:
  - the interception of communications
  - the acquisition and disclosure of data relating to communications
  - the carrying out of surveillance
  - the use of covert human intelligence sources
  - access to electronic data protected by encryption or passwords

  If a request for authorised access is made to the school, we will provide the appropriate access to your computing records and files.

Agreed by governors	
Date of review	
Signature of Chair	

REQUIRED SIGNATURE

MEMBER OF STAFF/VOLUNTEER

I understand and agree to the provisions and conditions of this agreement. I understand that any violations of the above provision may result in disciplinary action and revocation of privileges. I also agree to report any misuse of the system to the Headteacher. I agree to use the Internet and electronic communications systems in compliance with the terms outlined in this document and understand that my Internet access and any electronic communications may be logged or monitored.

NAME ____

SIGNATURE ____

DATE ____