Coppice Junior School

Acceptable internet use Policy

Policy ratified and adopted by Full Governing Body:	October 2022
Review frequency:	Annually
Policy due for renewal:	October 2023

Headteacher	Mark Knowles		Date
Chair of Governors	Jo Bromige		Date

1) Rationale and Entitlement

The purpose of the Internet access in school is to raise or develop the achievement and skills of pupils, to support the professional work of staff and to enhance the school's management information and business administration systems. We recognise that technologies such as the internet and e-mail have an increasingly profound effect on teaching and learning.
Access to the Internet is a necessary tool for all staff and students irrespective of gender, race, religion, culture or ability. It is an entitlement for students who show a responsible and mature approach with the intention to gain useful or entertaining resource.
The appropriate use of the Internet is providing a number of benefits to schools. These benefits include:-

Resources

•Providing access to documentation to aid in the development of teaching and learning resources
•Access to world-wide educational resources including museums and art galleries.
•Inclusion in government initiatives
•Information and cultural exchanges between students worldwide.
•Discussion with experts in many fields for pupils and staff.

Staff Professional Development

•Access to educational materials.
•Sharing good practice with colleagues.
•Communication with the advisory and support services, professional association and colleagues.

Administration

•More regular communication with schools and more immediate responses to inquiries.
•Improves access to technical support including remote management of networks.
•Method to publish information to schools that will free more resources for teaching and learning.
•Management of the school network from a single source, thus reducing the overall cost of performing this role.

Email

•Added value through access to Council IT systems (e.g. finance and payroll).
•Added value through the creation of a secure effective communication system between each other that can improve the transfer of information and data. Provision of a quick method of communication between pupils, staff, governors and officers of the authority.
•Provision of a centrally maintained email system that can give Coppice pupils an email address that will remain constant throughout their education.

Security

•Provision of a buffer between Solihull schools and the Internet designed to both protect users and enhance performance.
•Secure filtered Internet access.
•Filtered email for staff and pupils.
•Email anti-virus.
•Sophos anti-virus distribution – community license, supply software media and documented instructions to enable the School ICT Support to deploy and maintain Sophos anti-virus software on all its servers (however it is the school's responsibility to ensure their servers, laptops and workstations are constantly updated).
•Microsoft Critical Updates: distribution of Microsoft critical security updates services SUS and MSUS (school's responsibility to ensure computers are kept updated).
•Statutory UK ISK monitoring laws – records all Internet usage and email. The Headteacher will be informed when grooming or abuse is suspected.

Access to ICT resources is a privilege, not a right. It is the responsibility of the user (staff and, where appropriate, pupils) to take all reasonable steps to ensure compliance with the conditions set out in this document and to ensure that unacceptable use of technology (including the internet and the school networks) does not occur. Users are responsible for their behaviour and communications. Staff and pupils should use resources for the purposes for which they are made available. Users will accept personal responsibility for reporting any misuse of technology to the Headteacher. Users should take due care with the physical security of hardware. Users are expected to use ICT responsibly; it is impossible to set hard and fast rules about what is and is not acceptable, but the following provides some clear rules and guidance. Whether deliberate or accidental, failure to follow the policy's wider aims or specific points may result in disciplinary action.

There is a spare login for students on placement and supply teachers, so staff do not need to divulge their own login details; the spare login available at the School Office/ Headteacher. The password for the spare login will be periodically changed by the headteacher.

2. Aims

- To provide pupils with their entitlement as set out in the National Curriculum for computing.
- To use the Internet safety and effectively.
- To protect school from undesirable content.
- To raise the awareness of staff and students to the benefits of safe Internet access.

3. Objectives

- To develop strategies to use the Internet.
- To encourage suitable use through the implementation of a contract with users.
- To promote the use of the Internet as a learning tool.

4. Key principles and definitions

Coppice junior School owns the ICT system to which this policy refers; 'ICT system' means all computers, associated equipment and technical resources (eg printers, digital cameras) belonging to the school, whether part of the school's integrated network, stand-alone, or taken offsite. For the purposes of this policy, the same guidance applies to communications (e.g. text messages) made to colleagues and peers from hardware not belonging to school.

Professional use of the ICT system is characterised by activities that provide children with appropriate learning experiences or allow adults to enhance their own professional development. Resources must not be used for any personal reasons with one exception: staff may check personal emails. For those staff with a laptop on loan, personal use is allowed within the parameters set out below. Equipment on loan to a member of staff (eg laptop) should be used solely by the member of staff; it is not acceptable to loan the equipment to someone else.

All children must be made aware through class discussion of all the important issues relating to acceptable use of physical resources and the internet**.**

5. Responsibilities

The role of the Headteacher is to ensure that all staff are:

- Given opportunities to discuss the issues associated with Internet access and develop appropriate teaching strategies.
- Given appropriate training.
- Aware of, that the monitoring of Internet access takes place for both staff and pupils.
- Provided with or have access to the Internet Access Policy and its importance explained.
- Activity reports are mentioned regularly, and action taken as necessary.
- Parents' attention will be drawn to the policy in newsletters, the school brochure and on the school website.
- A module on responsible Internet use (e-safety) will be included in the ICT curriculum for all year groups covering both school and home use.
- New facilities will be thoroughly tested before pupils are given access.
- The policy is implemented and reviewed as necessary.

The role of the all staff is to ensure that:

- Rules for Internet access are posted near computer systems.
- There is equality of access within the classroom.
- They inform the Computing subject leader of any problems when they arise.
- They supervise pupils at all times when they access the Internet.
- They use the Internet in a responsible manner

The role of the pupils:

- To read and understand the rules for responsible use guidance 'Think then Click' or have them explained by a teacher where necessary.
- To access the Internet in a sensible manner. (See Appendix B)
- To report to an adult any material when they receive that they consider offensive in inappropriate.
- To refrain from giving their name, address or contact numbers to any person without permission from a parent, carer or teacher.

The role of the governors:

- Ensure an Internet Usage Policy is written.
- All staff have been given the opportunity to discuss the policy.
- The policy is ratified and reviewed as necessary: **bi-annually**.

6. Equal Opportunities

To make sure that all pupils receive the National Curriculum entitlement, it is essential that opportunities are provided for pupils to access the Internet, regardless of gender, race, religion, ethnic group, culture or ability. It is equally important that all staff are given the opportunity to access the Internet.

7. Special Educational and Additional Needs

It can be a positive tool for children with Special Educational and Additional Needs. Access to the Internet is therefore a vital link with which communication to the outside world can be achieved. Access to the Internet can also stimulate children to develop their ideas and research independently.

8. Safeguarding

Children must not be given unsupervised access to the internet. At Coppice Junior School, 'supervised' here means ensuring the user is regularly, frequently monitored by a responsible adult. The teaching of internet safety is included in the school's computing teaching, but all teachers within all year groups should be including internet safety issues as part of their discussions on the responsible use of the school's computer systems. Most importantly, all children must understand that if they see an unacceptable image on a computer screen, they must shut the laptop or turn of the device and report immediately to a member of staff.

9. Resources

It is expected that resources will be used from the Internet for teaching and learning materials. It is vital schools acknowledge the origination of resources, authenticate the author, examine the target audience and discriminate between what is fact and fiction.

10. Copyright

Copyright of materials must be respected. When using downloaded materials, including free materials, the intellectual property rights of the originator must be respected and credited. All material saved on the school's network is the property of the school and making unauthorised copies of materials contained thereon maybe in breach of the Data Protection Act, Individual Copyright or Intellectual Property Rights.

11. Parental Involvement

Due to the high level of Internet use in homes, the school will try to increase the involvement of parents/guardians in developing safe Internet practices. The school may be able to help parents plan appropriate, supervised use of the Internet at home, thereby raising parental awareness of the dangers that pupils may face when access to the Internet in unrestricted. Information and advice is shared with parents via the school Facebook page and emails.

Strategies

- A careful balance between informing and alarming parents will be maintained.
- Demonstrations and practical IT sessions for parents will be organised to encourage a partnership approach.
- Joint home/school guidelines on issues such as safe Internet use will be established.
- Suitable educational and leisure activities that make responsible use of the Internet will be developed with parents.

Community Use

Internet use in the local community is avalible. In addition to the home, access may be available at the local library, youth hub, adult education centre, community use sites or supermarket. The school will liaise with the local community to promote a united approach to internet access for pupils.

12. Use of hardware at Coppice Junior School

ICT resources are provided to enhance pupils' education and staff's professional activities.

Guidelines:

- Equipment may be in the care of a specific individual, but it is expected that all staff may wish to benefit from their use; access should be negotiated, and any difficulties should be referred to the Headteacher.
- Certain equipment will remain in the care of particular personnel and may be booked out for use according to staff requirements. Once equipment has been used, it should be returned to the designated storage area.
- Equipment such as laptops is encouraged to be taken offsite for use by teaching staff and certain other personnel in accordance with this policy. All equipment must be treated with care and staff will be responsible for replacement if damaged or lost. Our school insurance policy provides cover for equipment taken offsite temporarily, provided it is looked after with due care, i.e. not left in view on a car seat etc.
- The school reserves the right to examine or delete any files that may be held on its computer systems or to monitor any internet sites visited.
- Any costs generated by the user at home, such as phone bills, printer cartridge etc. are the responsibility of the user (unless the user has gained prior agreement from the Headteacher and only in exceptional circumstances).
- Where a member of staff is likely to be away from school through illness, professional development (e.g. secondment) or maternity leave, arrangements must be made for any portable equipment in their care to be returned for school. In the event of illness, it is up to the school to collect the equipment if the individual is unable to return it.

- If an individual leaves the employment of the school, any equipment must be returned.
- Staff should be aware that the use of USB pens (memory sticks), re-writeable CDs, etc. to transfer data from external computer systems can lead to problems with viruses. Where information has been downloaded from the internet, or copied from another computer, wherever possible, it should be emailed to school to ensure that it undergoes anti-virus scanning.
- The installation of software or hardware unauthorised by the school, whether legitimately licensed or not, is expressly forbidden without prior consent of the Headteacher.
- Use of materials stored on the school's curriculum network for personal use is not permitted.
- Users must not use the network in any way that would disrupt use of the network by others.
- All teachers within all year groups should ensure they actively teach how to use safely and sensibly ICT resources.

13. Email at Coppice Junior School

Email has become an essential means of communication. As part of the National Curriculum, pupils need to use email. Pupils need to be taught that the content of email should be something that they would not mind being read aloud. This should prevent content of an undesirable nature being written and sent. Email addresses are monitored by the SLT, designated Child Protection staff and the Technology support team.

Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received. Due regard should be paid to the content. Be polite – never send or encourage others to send abusive messages. Use appropriate language – users should remember that they are representatives of the school on a global public system.

Neither the school nor the council will be liable under any circumstances for any injury, distress, loss or damage to the pupil or parents, which may arise directly or indirectly from the pupils' use of unauthorised use of those facilities or email.

Guidelines

- Email must only be used in school for educational purposes.
- Staff email addresses (@coppice.solihull.sch.uk) should not be divulged to children unless part of a learning requirement agreed by a member of SLT. Personal email addresses should never be shared with parents or pupils.
- Pupils will be given an individual email account. This assumes a high level of trust and pupils will be regularly reminded of the 'Think then Click e-safety rules'.
- In-coming and outgoing email will be regarded as public and will be monitored.
- Messages sent using the school domain name should be regarded in the same way as messages written on school headed paper. Do not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
- The forwarding of chain letters will be banned, as will the use of chat lines.
- The sending of any sensitive personal data, for example home address, photographs or telephone numbers relating to the user or any other person is forbidden.
- Users will be held responsible for email sent from their account.

14. Web Publishing

The school wishes the school's website to reflect the diversity of activities, individuals and education that can be found at Coppice Junior School. However, the school recognises the potential for abuse that material published on the internet may attract, no matter how small this risk may be. Therefore, when considering material for publication on the internet, the following principles should be borne in mind:

- **Images:** photographs of children should not be published without the written consent of the parent / carer and the child's own verbal consent.
- **Names:** surnames of children should never be published, or forenames with photographs.
- **Addresses:** no link should be made between an individual and any home address, including simply street names.
- **Child protection:** serious consideration must be taken as to whether images and names may be published or not where the person publishing material suspects that there may be child protection issues at stake; in the case of anonymous pupil work, this may well be fine, but images / names of that child should not be published; if in any doubt at all, refer to the Designated Child Protection Officer.

The school or the council will not be made liable under any circumstances for any injury, distress, loss or damage to the pupil or parents who may arise directly or indirectly from the publishing of information on the website.

- The Headteacher may delegate editorial responsibility to a member of staff or other responsible person(s) to ensure that content is accurate, and quality of presentation is maintained.
- The website will comply with the school's guidelines for publications.
- Pupils will be made aware that the quality of their work published on the web needs to reflect the diversity of the audience.
- All material must be the author's own work, or where permission to reproduce has been obtained, clearly marked with the copyright owner's name.
- The point of contact on the website should be the school address and telephone number. Home information or individual email identities will not be published.
- Photographs of displays of children's learning or scanned examples of children's learning can be used on the website. Children's full names will not be used anywhere on the website, and no name should be used alongside photographs.

15. Internet Access

How will the school ensure Internet Access is Safe?

The internet may be accessed by staff and children during school hours and at home if a staff member has a school laptop on loan. All internet activity should be appropriate to staff professional activities or the children's education. Access to appropriate information should be encouraged and Internet access must be safe for all members of the school community from youngest pupil to teacher and administrative officer.

Authorised users are given a unique username and password generated by a central body, outside of school. Individuals will be responsible for their own password security. For security reasons, staff must use their '@coppice.solihull.sch.uk' email addresses for work purposes. Users must login with their own authorised user ID and password and must not share this information with other users. All web activity may be monitored, including the content of e-mail, therefore it is the responsibility of the user to ensure that they have logged off the system when they have completed their task. Users finding machines logged on under other users' username should log off the machine whether they intend to use it or not.

Through using the Microsoft package, the following strategies are used to try to ensure staff and pupils are protected, content reviewed, and sites blocked.

The filtering software used as part of the school contains a number of lists or categories of URLs (Uniform Resource Locator- the best-known example of the use of URLs is for the addresses of web pages on the World Wide Web) that can be marked as allowed or denied. These lists are updated frequently.

Some of the categories are listed below:

- Alcohol
- Alternative Lifestyles
- Criminal Skills
- Extreme
- Gambling
- Hast Speech
- Host as an IP Address (Internet Protocol address or host name, may or may not identify a specific computer. An IP address is something with which all computers accessing the internet are automatically allocated at point of connection.)
- Humour
- Match Making
- Network Timeout
- Network Unavailable
- New URL
- Occult
- Phishing (Phishing is a way of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. It is typically carried out by e-mail or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.)
- Pornography
- Profanity
- Proxy Anonymizer
- Safe Search
- Search Keywords
- Sex Education
- Substance Abuse
- Weapons
- Web Chat
- Web email

Teachers might need to research areas including drugs, medical conditions, bullying or harassment. In such cases, legitimate use must be recognised, and the user protected from possible accusation of inappropriate use.

Sites that are within disallowed categories are blocked automatically. This mechanism provides an additional 'safety' check. It also allows for many more sites than it would conventionally be available using the simple 'allowed list' system used by other filtering applications.

None of these systems can be completely effective in isolation therefore a combination of approached is used. It is acknowledged that adequate supervision is essential.

Guidelines

- Pupils will be informed that Internet use will be supervised, and sites selected will be monitored.
- Users will inform the ICT subject leader if their password is being used by another person or has been lost.
- The school will work in partnership with parents/carers, SMBC, DfE and the service providers to ensure systems to protect pupils are reviewed and improved.
- Senior staff will ensure that occasional checks are made to ensure that the filtering methods selected are effective in practice.
- If staff or pupils discover unsuitable sites, the URL and content will be reported to the Solihull helpdesk via the ICT / Computing Subject Leader, appropriate measures will be used to ensure the process to select appropriate material is adequate.
- 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 local authority network if not on the computer. Downloading some material is illegal and the police or other authorities may be called to investigate such use.
- Use of the school's internet connection for personal financial gain (including the use of online auction sites), gambling, political purposes, or advertising is forbidden.
- Illegal activities of any kind are strictly forbidden.
- Staff or students finding unsuitable websites through the school network should report the web address to the Headteacher.
- The use of the internet, e-mail, or any other media to access inappropriate materials relating to pornography, racism, extremist religion or any other offensive material is forbidden.
- As well as this policy, users must comply with the acceptable use policy of websites and other networks that they access.
- Activity that threatens the integrity of the school's computer systems, or that attacks or corrupts other systems, is prohibited.
- Users must not access data and resources to which they have no authorisation or acceptable purpose.
- Users must avoid the 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.

Security

In common with other material such as magazines, books and videos, some material available via the Internet is unsuitable for pupils. The school will supervise pupils and take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear on a terminal.

Neither the service providers nor SMBC can accept liability for the material accessed, or any consequences thereof:

- The use of computer systems without permission or of purposes not agreed by the school could constitute a criminal offence under the computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed.
- Staff, parents, governors and advisers will work to establish agreement that every reasonable measure is being taken.
- The headteacher will ensure that the policy is implemented effectively.
- The school will abide by the Data Protection Act 2018.

How will the Security of School ICT Systems be maintained at Coppice Junior School?

The Service Providers has put in place a system of logins that encourages users to be responsible for their own Internet access. It is essential that users log out, and this needs to be reinforced as good practice whenever possible. Maintaining security of the school systems is of paramount importance as sensitive data is stored within it. Internet access and email content will be automatically monitored and regular reports will be produced to the headteacher.

Guidelines

- Security strategies as discussed with the LA will be implemented.
- The ICT co-ordinator/network manager will ensure that the system has the capacity to take increased traffic caused by Internet use.
- The security of the whole system will be reviewed with regard to threats to security from Internet access.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Virus protection will be installed and updated regularly.
- Use of email to send attachments such as system utilities will be reviewed.

Monitoring

As a summary of the above, users must not access or create, transmit, display or publish any material that is illegal or likely to cause offence, inconvenience or needless anxiety. This includes any defamatory material, material that violates copyright law (this includes through video conferencing and web broadcasting), and material that violates Data Protection Act. Internet activity is monitored through Solihull ICT services and issues will be reported to the Headteacher. Any transgressions (i.e. those listed above) will be responded to quickly and could lead to removal of internet access rights, ICT system access rights or disciplinary action (staff or pupils), in accordance with the severity of the offence and related policies.

Social networking sites

Social networking sites (e.g. Facebook, MySpace) can blur the distinction between school and home. In order to avoid placing themselves in vulnerable situations, staff should not respond to or attempt to establish contact with pupils or parents.

Likewise, staff are encouraged to be sensitive to colleagues' needs to be 'detached' from school – some people may prefer not to communicate with colleagues, and this should be taken simply as the desire to 'switch off' from anything work-related.

The same need for sensitivity applies to photos of colleagues taken at or after school events: some staff will prefer not to have electronic images displayed and verbal consent should be sought each time.

As well as this policy, users must comply with the acceptable use policy of websites and other networks that they access; this is particularly important with social networking sites. Facebook, for example, has a minimum age limit of 13yrs and so no staff member should in any way encourage or condone a child at our school to use Facebook (this includes responding to Facebook messages).

Users should not reveal any personal information (e.g. home address, telephone number) about themselves or other users.

Any expression of a personal view about the school or Local Authority matters in any electronic form of communication must be endorsed to that effect. Any act that would bring the name of the school or Local Authority into disrepute is not allowed.

<u>Complaints or Problems</u>

How will Complaints Regarding Internet use be handled?

Prompt action will be required if a complaint is made. The facts of the case will need to be established, for instance whether the issue has arisen through Internet use inside or outside school. The school will need to discuss procedures for dealing with transgressions and these may be linked to the school's behaviour policy. Transgressions of the rules may be minor, whereby a temporary ban on Internet use will be adequate or major where a permanent ban may be required. Serious cases may necessitate the involvement of the policy or a local authority officer.

Guidelines

- Responsibility for handling incidents will be given to senior members of staff.
- Pupils and parents will be informed of the complaint's procedures.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- As with drugs issues, there may be occasions when SMBC needs to be informed. Early contact will be made to establish the legal position and discuss strategies.
- A pupil may have email, Internet or computer access denied for a period of time depending on the nature of the incident.

Appendix A

Staff purpose and use of Internet and email at Coppice Junior School:

Always remember you have a professional responsibility in terms of personal confidentiality; especially communication with parents' i.e. social networking; email; instant messenger. (If anyone is concerned about privacy, or doesn't know how privacy settings work on certain websites see the ICT subject leader.)

The internet at school can be used for:

- Any activity which supports the curriculum
- Search engines
- Online educational resources
- @coppice.solihull.sch.uk - email.

The internet at school can not be used for:

- Online gaming/gambling
- MSN or other instant messaging services
- Pornography
- Online dating
- Personal email/social networking (Facebook).

Our School email system can be used for:

- Any activity which supports the curriculum
- To enable local, regional, national and international collaboration between staff and students
- To supply and share information with other schools or the LA
- To enable parents to contact school.
- To enable homework to be submitted/collected
- To make contacts between governors the LA
- To support school administration
- You tube – so long as it has been checked as a valuable teaching resource.

Our school email system can not be used or:

- Sending material which contains abusive or offensive language
- Sending messages which are bullying or threatening in nature
- Sending personal details- home address, home/mobile number
- Sending viruses, hoax letters or chain mail
- Participating in news groups/chat rooms/social networks that require an email address.

Appendix B :Children's purpose and use of Internet and email at Coppice Junior School to be displayed in the computer room.

Acceptable internet use for Coppice pupils

At Coppice Junior School pupils are expected to use the internet in a safe and sensible manner. You can only use the internet if a teacher is present and you have been given permission to do so.

The internet at school can be used for:

- Searching for information- Google
- Online educational resources e.g. Purple Mash, BBC bitesize, timestable rock stars and google classroom.
- @coppice.solihull.sch.uk email

The internet at school can not be used for:

- Online gaming
- MSN or other instant messaging services
- Social networking (this is illegal on many sites for under 14's)
- You tube; any you tube clips will have been vetted by staff to ensure secure content.

Our School email system can be used for:

- Emailing classmates
- Emailing pen pals which have been issued by school
- Children to submit homework
- Teaching of email techniques and etiquette
- Sending attachments agreed by the member of staff.

Our school email system can not be used or:

- Sending material which contains abusive or offensive language
- Sending messages which are bullying or threatening in nature
- Sending personal details or photographs
- Sending private information about another person
- Forwarding chain letters
- Sending attachments - unless agreed by staff.