THE WILLOWS PRIMARY SCHOOL

E-SAFETY POLICY

Author:	ICT Co-ordinator
Date:	January 2024
Review Date:	January 2026
Date approved:	
Signed :	

Our E-Safety Policy reflects the need for children and adults to be aware of safety issues surrounding Internet use. It has been agreed by the staff and approved by governors.

The Importance of the Internet

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience. Many pupils use the internet widely outside of school and will need to learn how to evaluate internet information and to take care of their own safety and security. Internet access is an entitlement for pupils who show a responsible approach to its use.

The Benefits to Education

Staff and pupils can use the internet to access many resources that benefit learning. These include access to world-wide educational resources including museums and art galleries, educational and cultural exchanges between pupils world-wide and access to experts in many fields. In addition, it provides professional development for staff through access to national developments, educational materials and effective curriculum practice.

Internet access is planned to enrich and extend learning activities. Access levels are reviewed to reflect the curriculum requirements and age of pupils. Staff guide pupils in on-line activities that support the learning outcomes planned for the pupils' age and maturity. Pupils are educated in the effective use of the internet in research, including the skills of knowledge location and retrieval.

To ensure safety, internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils. Pupils are taught what is acceptable and what is not acceptable and given clear objectives for internet use.

Teaching pupils to evaluate online content

Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. They are taught to acknowledge the source of information and to respect copyright when using online material in their own work. These skills are part of every subject and are taught across the curriculum. If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Headteacher or ICT co-ordinator. These sites will be reported to RM SafetyNet, who manage our filtering and will ensure that they are blocked.

Maintaining the security of information systems

Internet access is managed through RM Unify who provide virus protection and filtering services. The ICT coordinator and IT technical can access, add and amend the blocked sites as and when required. Staff are required to sign an Acceptable Use Policy which outlines the rules for use of the network in order to ensure the safety of both school systems and themselves. Parents are asked to sign a similar Acceptable Use Policy for home loan of school devices.

Website content

The school has a website which is hosted by blue level at www.thewillowsprimary.org The school website is an essential information resource for parents and others. Items on this site are public. The point of contact on the website is the school address, school e-mail and telephone number. Staff and pupils' work and personal information / e-mail addresses are not published.

The Headteacher takes overall editorial responsibility and ensures that content is accurate and appropriate. The copyright of all material is held by the school or attributed to the owner where permission to reproduce it has been obtained.

Publishing pupils' images and work

Photographs that enable pupils to be identified will be selected carefully and only be of those children whose parents have given permission via our Photographic Consent Form. Pupils' full names will not be used anywhere, particularly associated with photographs. Permission to display photographs is obtained as part of the registration process for new pupils with the signing of the Photographic Consent Form

Social networking, social media and personal publishing

Pupils do not have access to social media in school. Pupils will be taught the advantages and pitfalls of social networking. Content will include advice relating to keeping personal details safe. Examples of personal details include: real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc.

Cyberbullying

Cyberbullying is defined as bullying that takes place using electronic technology. Electronic technology includes devices and equipment such as mobile phones, computers, and tablets as well as communication tools including social media sites, text messages, online chat forums and websites.

Cyberbullying can be a form of child on child abuse.

Examples of cyberbullying include inappropriate text messages or emails, rumours sent by email or posted on social networking sites, and embarrassing pictures, videos, websites, or fake profiles. Cyber bullying can happen at all times of the day, with a potentially bigger audience.

Teachers should be aware that, because children have limited access to social media or phones in school, cyberbullying incidents occur most commonly outside of school but that these incidents can have an impact in school if they are continued on site.

E-safety sessions are taught in every year group and are a regular focus in both class and whole school assemblies. Additional information on age appropriate use of social media is regularly shared with parents and advice on restricting and adding parental controls to a variety of mobile devices is shared regularly. Further information on how any kind of bullying is dealt with and how pupils are supported both in and out of school can be found in our Anti Bullying Policy.

Home Learning

Where a class, group or small number of pupils needs to isolate as the result of a pandemic, other extreme event or if there is a local lockdown requiring pupils to remain at home, school has the capacity to offer immediate remote education. Further information on how we ensure that remote/ online learning is as safe as possible can be found in our Remote Learning Policy.

Managing emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Pupil mobile phones cannot be used in school. **Smart watches which connect to a mobile device will not be allowed in school.**

Authorisation of Internet access

The pupils have access to a highly filtered internet. Children may work independently but are always supervised by an adult close by. Under no circumstances will pupils be allowed access to the Internet without supervision by a staff member. This includes break times, lunchtimes and after school.

Consequences for inappropriate use of ICT equipment and the internet in school

Teachers will share the **Rules for Responsible Internet Use** (see appendices)

Any breach of the rules for internet use will be referred to the ICT coordinator and the Headteacher. A record will be kept of what has happened, and possibly one or more of the following actions will occur:

☹ A letter will be sent to parents explaining how the rules have been broken.

☹ Pupils may be banned from using the Internet and other ICT equipment,

☹ Any further action decided by the Headteacher.

Risk assessment

Some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor West Berkshire Council can accept liability for the material accessed, or any consequences of Internet access. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Methods to identify, assess and minimise risks are reviewed regularly.

To minimise the risk of inadvertent access to unsuitable sites, unfiltered web-wide search engines are not be used by children. Suitable websites should be found by the teacher before the lesson and links made available. Search skills can be taught by using “closed” searches within checked sites eg bbc.co.uk/schools.

Further checks are made as part of the school’s monitoring and filtering policy, which sets out how routine filtering tests are made to ensure the robustness of our internet filters.

The ICT coordinator will ensure that the Internet policy is implemented and compliance with the policy monitored.

Complaints regarding e-safety

Complaints should be via the office email address and should be addressed to the Headteacher.

Staff

All staff must accept and sign the terms of the Acceptable Use Policy for Staff before using any network or Internet resource in school.

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. Staff should report any cases of misuse by children or other staff to the Headteacher. Misuse of the Internet or School Network by staff is a disciplinary matter.

Appendices: Rules for Responsible Internet Use
Acceptable Use Policy for Staff

See also: Anti Bullying Policy
Remote Learning Policy
Monitoring and Filtering Policy

The Willows Primary School
Rules for Responsible Internet Use

Our school has iPads, netbooks and desktop computers with internet access to help our learning.

These rules will help keep us safe and help us be fair to others.

Using the iPads, netbooks and computers:

- I will not access other people's files;
- I will not bring in portable data sticks or CDs from outside school and try to use them on the school computers.

Using the Internet:

- I will ask permission from a teacher before using the Internet;
- I will report any unpleasant material to my teacher immediately because this will help protect other pupils and myself;
- I understand that the school may check my computer/files and may monitor the internet sites I visit;
- I will not complete and send forms without permission from my teacher;
- I will not give my full name, my home address or telephone number when completing forms.

When using e-mail:

- I will immediately report any unpleasant messages sent to me because this would help protect other pupils and myself;
- I understand that e-mail messages I receive or send may be read by others;
- The messages I send will be polite and responsible;
- I will only e-mail people I know, or my teacher has approved;
- I will only send an e-mail when it has been checked by a teacher;
- I will not give my full name, my home address or telephone number;
- I will not use e-mail to arrange to meet someone outside school hours.

The Willows Primary School

Acceptable Use Policy for ICT (Staff)

Aims

- To allow all users to access and use the Internet and ICT equipment in all forms across the school
- To provide a mechanism by which staff and pupils are protected from sites, information and individuals which would undermine the principles and aims of the school.
- To provide rules which are consistent and in agreement with both GDPR regulations and the Data Protection Act.
- To provide a framework of rules which are consistent with the acceptable procedures commonly used on the internet.
- To ensure accountability for any breach of the rules.

Conditions

1. Personal use of the Internet is only permitted outside 'directed time'.
   This is to include, writing personal e-mails and visiting sites such as social networking, e-bay, holiday companies, insurance companies and ticket agencies.

1. You must not disclose passwords and log-in names to anyone, other than the persons responsible for running and maintaining the system.
   Log-in details should remain personal to avoid compromises in security.

2. You must not disclose personal addresses, telephone numbers, school network log-ins or e-mail log-ins of any staff or pupil.
   Privacy should be respected at all times.

3. You must not use names, photographs, video, web cam images or recorded material of pupils without written permission from parents or carers.
   This is recorded on the Parental Consent Form.

4. You must not download, use or upload any material which is copyright. Do not plagiarise other people's work. Permission should be sought from the owner.
   If in doubt do not use the material.

~~5.~~ Under no circumstances should you view, upload or download any material which is likely to be unsuitable for children. This applies to any material with violent, dangerous, discriminatory or inappropriate sexual content.

6. Be polite and respect other people's views. The use of strong or inappropriate language or aggressive behaviour is not allowed.
   This applies generally, but also in stored work, e-mails or the school website.

7. The use of chat rooms is forbidden.
8. Illegal activities of any kind are forbidden.
9. Always respect the privacy of files of other users. Do not enter file areas of other staff without their permission.

10. You must log off when you have finished using a computer. There are separate access passwords for pupils and staff to access the computers. Where remote access to the school network is available it is vital to log off and protect log-in details.
    This is to avoid unauthorised access to sensitive or shared material and to protect the school network from outside access by unauthorised users.
11. Under **no** circumstances allow pupil access to the Internet without supervision by a staff member. This includes break times, lunchtimes and after school.
12. Ensure that all pupils have followed the correct procedures before, during and after the session, in accordance with the Acceptable Use Policy for Pupils.
13. Report any incident which breaches the Acceptable Use Policy to the Headteacher.
14. In the event of any pupil reporting misuse of e-mail to you, please **DO NOT** delete any offending messages. You must report the details to Headteacher or ICT coordinator who will investigate further and log the incident.
15. Only use portable storage devices when absolutely necessary. Encrypted data sticks, e-mail or transfer between laptop and the school network are the preferred methods.
16. Hall projectors and classroom screens **must** be switched off when not in use. Please refer to the Health & Safety Policy.
17. Mobile telephones must not be used during 'directed time' for personal calls or texts unless in emergency.
18. You must not allow pupils to use a computer (desktop or laptop) while it is logged in as a teacher or adult working in school.
19. Refer to Acceptable Use Policy for School Laptops.
20. Refer to Acceptable Use Policy for Pupils.

Declaration:

I understand and agree to abide by the provisions and conditions of this policy.
I understand that any breach of the above rules may result in disciplinary action.
I agree to report any misuse of the system to the Headteacher.

Name (Block Capitals) ___________________________

Signed __________________________ Date ______________________