WINDHILL PRIMARY SCHOOL

FLYING HIGH FOR EXCELLENCE

Acceptable Use Policy

Person responsible for policy:	Donna Howard
Approved by:	Lynn Mathers Se tembe 2018
Role:	Chair of Governors
Last Reviewed:	November 2022
Next review due by:	November 2024

Introduction

Windhill Primary School recognises that access to technology in the school gives students and teachers greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work and life. We are committed to helping students develop 21st-century technology and communication skills.

This Acceptable Use Policy outlines the guidelines and behaviours that users are expected to follow when using school technologies.

- The network is intended for educational purposes only.
- All activity over the network or using district technologies is monitored. Misuse of school resources can result in disciplinary action.
- Students are expected to follow the same rules for good behaviour and respectful conduct online as offline.
- Users of the network or other technologies are expected to alert IT staff immediately of any concerns for safety or security.

Your ICT contact in the school is Mr M Hedar.

Technologies Covered

Windhill Primary School may provide Internet access, desktop computers, mobile computers or devices, videoconferencing capabilities, online collaboration capabilities, message boards, email, and more.

As new technologies emerge, Windhill Primary School will attempt to provide access to them. The policies outlined in this document are intended to cover all available technologies, not just those specifically listed.

Web Access

Windhill Primary School provides its users with access to the Internet, including web sites, resources, content, and online tools. That access will be restricted in compliance with the school's policies. Web browsing may be monitored and web activity records may be retained indefinitely.

Users are expected to respect that the web filter is a safety precaution, and should not try to circumvent it when browsing the Web. If a site is blocked and a user believes it shouldn't be, the user should follow protocol to alert an IT staff member or submit the site for review.

Email

Windhill Primary School may provide users with email accounts for the purpose of school-related communication. If users are provided with email accounts, they should be used with care. Users should not send personal information; should not attempt to open files or follow links from unknown or untrusted origin; should use appropriate language; and should only communicate with other people as allowed. Email usage may be monitored and archived.

On-line learning platforms

Windhill Primary School provides all children with log-in details for on-line learning platform, Microsoft Teams. This should only been used for the purpose for which it is intended and should not be used by staff or pupils for any other reasons. Staff and learners will only use school managed, professional accounts with learners and/or parents/carers. The use of any personal accounts to communicate with learners and/or parents/carers is not permitted.

Users should not share their log-in details or passwords with others.

Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Posts, chats, sharing, and messaging may be monitored. Users should be careful not to share personally-identifying information online.

Social / Web 2.0 / Collaborative Content

Recognising that collaboration is essential to education, Windhill Primary School may provide users with access to web sites or tools that allow communication, collaboration, sharing, and messaging among users.
Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Posts, chats, sharing, and messaging may be monitored. Users should be careful not to share personally-identifying information online.

The school has an official Twitter page which is managed by Senior Leadership Team. Staff members who have not been authorised to manage or post to the account must not access, or attempt to access the account.

The school has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

Mobile Devices Policy

Windhill Primary School may provide users with mobile computers or other devices to promote learning both inside and outside of the classroom. Users should abide by the same acceptable use policies when using school devices off the school network as on the school network. Users are expected to treat these devices with extreme care and caution; these are expensive devices that the school is entrusting to your care. Users should report any loss, damage, or malfunction to IT staff immediately.

Security

Users are expected to take reasonable safeguards against the transmission of security threats over the school network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin. If you believe a computer or mobile device you are using might be infected with a virus, please alert IT. Do not attempt to remove the virus yourself or download any programs to help remove the virus.

Plagiarism

Users should not plagiarise (or use as their own, without citing the original creator) content, including words or images, from the Internet.

Users should not take credit for things they didn't create themselves, or misrepresent themselves as an author or creator of something found online. Research conducted via the Internet should be appropriately cited, giving credit to the original author.

Personal Safety

If you see a message, comment, image, or anything else online that makes you concerned for your personal safety, bring it to the attention of an adult (teacher or staff if you're at a school; parent if you're using the device at home) immediately.

Users should never share personal information, including phone numbers, address, school name, birthdays any other private information online.

To ensure your safety, avoid talking about personal schedules or situations.

Users should recognise that communicating over the Internet brings associated risks, and should carefully safeguard the personal information of themselves and others.

Users should never agree to meet someone they meet online in real life.

Users should also remember not to post anything online that they wouldn't want parents, teachers, or future colleges or employers to see. Once something is online, it's out there - and can sometimes be shared and spread in ways you never intended.

Cyberbullying

Cyberbullying is bullying through the internet and will not be tolerated. Harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyberstalking are all examples of cyberbullying. Don't send emails or post comments with the intent of scaring, hurting, or intimidating someone else.

Engaging in these behaviours, or any online activities intended to harm (physically or emotionally) another person, can always be tracked down by CEOP. Cyberbullying can be a crime. Remember that your activities are monitored and retained.

Online Radicalisation and extremism

Online groups promoting self-harm, extreme weight loss, suicide and far right politics are a very real threat to impressionable individuals, such as school children, who are using the internet in isolated or unmonitored sessions. We cannot predict which form of extremism will pop up or what form it will take. We can and do educate our pupils and staff to look for signs of coercion and pressure online. We also combat these forms of abuse through the promotion of British values, community and emotional well-being in our school culture. We provide a safe environment in which to discuss concerns about these issues and explore points of view in our eSafety and PSHE teaching.

Sites or communications that cause us concern will be immediately reported to the police.

Handling of complaints

It is our duty of care to ensure that every child in our school feels safe, secure and confident online. However, due to the evolving nature of content on the internet, the scale of its use globally, the speed of changes and the sheer variety of methods of accessing the net it is unrealistic to imagine that unsuitable content will never appear on a school computer or mobile device. The school has taken all steps it currently feels necessary in order to secure the online safety of our pupils as much as reasonably possible however, the school accepts no liability for material accessed or consequence of internet use.

Any complaints about our precautions, their use or content accessed shall be:

- Logged by the SLT or Computing lead as appropriate
- Fed into future policy review

- Reported to school governors as necessary
- Forwarded to the Local Authority, CEOP or police as necessary

Monitoring

The headteacher, business manager and IT lead, Mr Hedar, monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every 2 years.

The governing board is responsible for approving this policy.

Examples of Acceptable Use

I will:

- Use school technologies for school-related activities and research.
- Follow the same guidelines for respectful, responsible behaviour online that I am expected to follow offline.
- Treat school resources carefully, and alert staff if there is any problem with their operation.
- Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
- Alert a teacher or other staff member if I see threatening/bullying, inappropriate, or harmful content (images, messages, posts) online.
- Use school technologies at appropriate times, in approved places, for educational pursuits only.
- Be cautious to protect the safety of myself and others.
- Help to protect the security of school resources.

This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

Examples of Unacceptable Use

I will not:

- Use school technologies in a way that could be personally or physically harmful to myself or others.
- Search inappropriate images or content.
- Engage in cyberbullying, harassment or disrespectful conduct toward others - staff or students
- Try to find ways to circumvent the school's safety measures and filtering tools.
- Use school technologies to send spam or chain mail.
- Plagiarise content I find online.
- Post personally-identifying information about myself or others.
- Agree to meet someone I meet online in real life.
- Use language online that would be unacceptable in the classroom.
- Use school technologies for illegal activities or to pursue information on such activities.
- Attempt to hack or access sites, servers, accounts or content that isn't intended for my use.

This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

Violations of this Acceptable Use Policy

Violations of this policy may have disciplinary repercussions, including:

- Suspension of network, technology, or computer privileges in extreme cases
- Notification to parents in most cases
- Detention or suspension from school and school-related activities
- Legal action and/or prosecution