Hawthorn Primary School

Creating Life Long Learners

SOCIAL MEDIA AND ACCEPTABLE USE POLICY FOR STUDENTS

Date Published: Dec. 2017	Review Date: Dec. 2018
Compiled by: Miss Robinson Mr Godley	Authorised By:

Elmham Road, Cantley, Doncaster DN4 6LQ
Tel: 01302 535906
Fax: 01302 371192
Email: admin@hawthorn.doncaster.sch.uk
Headteacher: Mrs Diane Wakefield
Chair of Governors: Mr H Fraser
Website: www.hawthorn.doncaster.sch.uk

Social Media and Acceptable Use Policy for Students

Introduction

Hawthorn Primary School recognises that access to technology in the education establishment 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 education establishment technologies.

- The network is intended for educational purposes only.
- All activity over the network or using district technologies is monitored. Misuse of education establishment 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 education establishment are: Mrs Wakefield, Amy Robinson and Mr Godley.

Technologies Covered

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

As new technologies emerge, Hawthorn Primary 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

Hawthorn Primary 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 education establishment'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

Hawthorn Primary may provide users with email accounts for the purpose of education establishment-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.

Social / Web 2.0 / Collaborative Content

Recognising that collaboration is essential to education, Hawthorn Primary 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.

Mobile Devices Policy

Hawthorn Primary 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 education establishment devices off the education establishment network as on the education establishment network.

Users are expected to treat these devices with extreme care and caution; these are expensive devices that the education establishment 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 education establishment 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 the adults in the classroom. 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 (parent if you're using the device at home) immediately.

- Users should never share personal information, including phone numbers, address, education establishment 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.

Radicalisation

- Web access will be restricted in compliance with the education establishment's policies. Web browsing may be monitored and web activity records may be retained indefinitely.
- Users should report and suspicious behaviour.
- See personal safety section for more information.

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.

Examples of Acceptable Use

I will:

- Use education establishment technologies for education establishment-related activities and research.
- Follow the same guidelines for respectful, responsible behaviour online that I am expected to follow offline.
- Treat education establishment 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 education establishment 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 education establishment resources.

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

Examples of Unacceptable Use

I will not:

- Use education establishment 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 education establishment's safety measures and filtering tools.
- Use education establishment 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 education establishment 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 education establishment 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 education establishment and education establishment-related activities
- Legal action and/or prosecution
-

I have read and understood this Acceptable Use Policy and agree to abide by it:

____
(Student Printed Name)

____
(Student Signature and date)

____

I have read and discussed this Acceptable Use Policy with my child and have a full understanding of social media acceptable usage

____
(Parent Printed Name)

____
(Parent Signature and date)

____