Online Safety Policy

This policy outlines our commitment to maintaining a safe online environment for all users. It is based on best practices and statutory guidelines, including those from the NSPCC and from KCSIE (2021) which introduced the 4Cs online safety framework that categorises online safety risks into four groups: content, contact, conduct and commerce. The 4Cs framework allows educators with a systematic method to identify, understand and tackle potential online dangers.

Author: Dave Strudwick - Head of Education
Quality Assured: Nicki Lorenzini - Head of Wellbeing
Date Approved: April 2025
Date to be reviewed: April 2026
DSL: Dave Strudwick
DDSL: Nicki Lorenzini

Purpose

The Hummingbird Learning Lab works with children and families.The purpose of this policy statement is to:

- ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices.
- provide staff and volunteers with the overarching principles that guide our approach to online safety
- ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.
- protect individuals from online risks and harm.
- outline procedures for reporting and addressing online safety concerns.

Key Principles

The new RSE guidance gives clear support and direction for educators. For example:
“Schools should be aware that for many young people the distinction between the online world and other aspects of life is less marked than for some adults. Young people often operate very freely in the online world and by secondary school age some are likely to be spending a substantial amount of time online. Where topics and issues outlined in this guidance are likely to be encountered by pupils online, schools should take this into account when planning how to support them in distinguishing between different types of online content and making well-founded decisions.

More broadly, the internet and social media have other important characteristics which young people should be aware of in order to help them use them discriminatingly. For example, social media users are sometimes prepared to say things in more extreme, unkind or exaggerated ways than they might in face to face situations, and some users present highly exaggerated or idealised profiles of themselves online. Some platforms attract large numbers of users with similar, sometimes extreme, views, who do not welcome dissent or debate. Young people should be aware that certain websites may share personal data about their users, and information collected on their internet use, for commercial purposes (in other words, to enable targeted advertising). In addition, criminals can operate online scams, for example using fake websites or emails to extort money or valuable personal information. This information can be used to the detriment of the person or wider society. Schools should take these factors into account when planning teaching of these subjects and consider the overlap with their wider curriculum to ensure pupils know how to keep themselves and their personal information safe.”

We want all children and young people to be safe online. The online world provides everyone with many opportunities; it can also present risks and challenges.

- The online world changes quickly and we will act thoughtfully in relation to this
- We will provide an appropriate filter system
- We will monitor use effectively through the small group size and adult ratios
- We have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online

- We have a responsibility to help keep children and young people safe online, whether or not they are using hummingbird's network and devices
- Working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety
- All children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse
- Respect and responsibility: Users are expected to treat others with respect and act responsibly online. Bullying in any form is not acceptable.
- Learning to be safe: Users should learn how to stay safe and this includes protecting their personal information and taking steps to ensure online security.
- Reporting concerns: Any concerns about online safety should be reported promptly.

Wider Framework

- This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England relating to online abuse, bullying, child protection and safeguarding.
- This policy connects to other policies including
    - Behaviour Policy (including consequences and rewards)
    - Safeguarding policy
    - Anti bullying Policy
    - Relationships and Sex Education Policy

Guidelines for Online Behavior

In practice this means we:

1. Consider if the use of technology enhances learning.
2. Be respectful and considerate of others online.
3. Do not share personal information with unknown individuals.
4. Use strong passwords and keep them confidential.
5. Be cautious of clicking on links or downloading files from unknown sources.
6. Report any online abuse, harassment, or inappropriate content.
7. The DSL has an online safety responsibility.
8. Expect our behaviour code to provide direction to staff and volunteers about life at Hummingbird.
9. Support and encourage parents and carers to do what they can to keep their children safe online.
10. Develop an online safety agreement for use with young people and their parents or carers.
11. Develop clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child or young person.
12. Review and update the security of our information systems regularly.

13. Ensure that user names, logins, email accounts and passwords are used effectively
14. Keep personal is held securely and shared only as appropriate.
15. Ensure that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given.
16. Provide supervision, support and training for staff and volunteers about online safety.
17. Examine and risk assess any social media platforms and new technologies before they are used within the organisation.

Educating Students about Online Safety

In practice this means we:

1) Foster our students' critical thinking and maintain open communication between them and our staff about the content they encounter, particularly regarding misinformation, disinformation (e.g. fake news), and conspiracy theories.
2) Empower students to question sources, check for emotional triggers, and use fact-checking tools before believing or sharing information found online
3) Actively address with students topics like: personal information privacy, identifying and reporting, understanding their digital footprint, using privacy settings correctly, creating strong passwords, and knowing how to interact with others respectfully and safely online.
4) Actively educating students about how to protect themselves from the 4 areas of online risk outlined in KCSiE:
   Content: being exposed to illegal, inappropriate or harmful content, including: pornography, fake news, racisim, misogyny, self-harm, suicide, and anti-religious, radical or extremist content
   Contact: being subjected to harmful online interaction with other users; including: peer to peer pressure, adults posing as young people for the purposes of grooming children.
   Conduct: personal online behaviour that increases the likelihood of, or causes, harm, including: making, sending and receiving explicit images; sharing others explicit images, and online/cyber bullying.
   Commerce: the risks associated with the financial and commercial aspects of the internet, including: online gambling, inappropriate advertising, phishing, financial scams, and in-app purchases.
   Ref: The 4C's of Online Safety from Child Protection by Horizons
   Ref: The 4 Cs of online safety: online safety risk for children from NSPCC Learning

Reporting Procedures

Any concerns about online safety should be reported to the DSL using a Safeguarding Concern Form on our website