


Author | Matthew Nolan
Contributors |
Version | 3
Pages | 12
Publication Date | Autumn 2025
Next Review Date | Autumn 2026



Online Safety Policy

Policy overview

The purpose of this policy is to safeguard and protect all members of Richard Huish College by providing a framework to promote and maintain a safe, effective, and responsive online safety culture. The policy is applicable to all members of the college. This includes staff, students, volunteers, parents/carers, visitors, and community users who have access to and are users of The College digital technology systems, both internally and externally.

Other related policies

Equality and Diversity Policy
Health and Safety Policy
Acceptable Use Policy
Whistle Blowing Policy
Staff Code of Conduct
Safer Recruitment & Procedure
Social media and online software expectations
Artificial Intelligence Policy

Contents

1. Introduction
2. Online Safety Statement
3. Policy Scope
4. Roles and Responsibilities
5. Education and Training
6. Cultivating a Safe Environment
7. Remote working guidance
8. Responding to Online Safety Concerns
9. Responding to Complaints

1. Introduction

As the online world evolves, so do both the online harms and risks facing our young people and the relevant legislation, both statutory and non-statutory, which directs and guides how colleges should meet their online safety requirements.

College staff and governors play a vital role in setting an example for the whole college and are central to implementing policy and process. It is imperative that a whole college community approach to online safety is adopted and that all stakeholders are aware of their responsibilities and duties in relation to keeping children safe online. This will support a robust online safety ethos and ensure that colleges are providing the best online safety provision they possibly can.

This policy is applicable to all members of Richard Huish College. This includes staff, students, volunteers, parents/carers, visitors, and community users who have access to and are users of the Richard Huish College digital technology systems, both internally and externally within the home and community setting.

2. College Online Safety Statement

Richard Huish College asserts that online safety is an essential element of safeguarding and duly acknowledges its statutory obligation to ensure that all students and staff are protected from potential online harm. The college adheres to the Online Safety Act and will make changes to this policy and the college practice when required.

Richard Huish College believes that the internet and associated devices are an integral part of everyday life.

Richard Huish College affirms that all students should be empowered to build resilience and to develop strategies to recognise and respond to online risks.

3. Policy Scope

Online safety is a universal topic which requires recurrent regulatory review and places a stringent duty of care on us all. This policy supports the college in meeting statutory requirements as per the Department of Education (DfE) guidance under Keeping Children Safe in Education (KCSIE). Effective, timely and robust online safety is fundamental to protecting young people in education and it is a significant part of the safeguarding agenda.

High quality online safety provision requires constant vigilance and a readiness to act where abuse, exploitation or neglect is suspected. The landscape of safeguarding is constantly evolving, and the college must endeavour to embrace and shape their key priorities in support of this. Education has a vital role to fulfil in protecting young people from forms of online abuse whilst demonstrating a concerted obligation to respond with haste and flexibility to concerns as they arise. Above all, staff foster dedication to ensuring that they listen to the voices of the vulnerable and act upon what is heard. Safeguarding is everyone's responsibility.

Defining online abuse: "Online abuse is any type of abuse that happens on the web, whether through social networks, playing online games or using mobile phones" (NSPCC, 2019).

Hidden harms - types of online abuse may include:

- Cyberbullying
- Emotional abuse
- Grooming
- Sexting
- Sexual abuse
- Sexual exploitation
- Sexual harassment

The types, patterns and different circumstances of significant harm and abuse should be considered within the categories identified for children in the Children Act 1989/ 2004. These are:

- Neglect
- Sexual
- Physical
- Emotional

Technology can facilitate a world of learning and development in addition to help yield a range of opportunities. However, the reality is that it can also present a window to potential and actual harm and abuse. It can elicit and support an array of illegal abusive behaviours including, but not limited to:

- harassment
- stalking
- threatening behaviour
- creating or sharing child sexual abuse material
- inciting a child to sexual activity
- sexual exploitation
- grooming
- sexual communication with a child
- causing a child to view images or watch videos of a sexual act.

Artificial Intelligence is a powerful tool that can be used to support and enhance student experience, but it is important that it is used ethically and responsibly both within the context of our college and with a view to the future.

Potential harms related to safeguarding include:

- Disinformation, bias or discrimination
- Sexual abuse of children
- Lack of an ethical framework
- Data protection and privacy issues

- Lack of regulation
- Cybercrime and fraud

This policy should be read alongside the relevant policies relating to safeguarding of children and in addition to the associated statutory legislation and guidance.

4. Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of all stakeholders across the online community at Richard Huish College

4.1 Staff

All members of staff (teaching and non-teaching) have a responsibility to protect young people online. All staff must always act in accordance with their own professional boundaries, upholding professional behaviour and college code of conduct.

All staff need to:

- Be aware of and adhere to all policies in college which support online safety and safeguarding.
- Support in the ownership and responsibility for the security of systems and the data accessed.
- Model good practice when using technology.
- Know the process for making referrals and reporting concerns.
- Know how to recognise, respond, and report signs of online abuse and harm.
- Receive appropriate online safety/safeguarding training.
- Always act in the best interests of the young person
- Be responsible for their own continuing professional development in online safety.
- Have a basic understanding of how Artificial Intelligence can be used by young people.

It is the responsibility of the member of staff to inform their line manager if they are being investigated in relation to children, young people or adults at risk with respect to protection concerns outside of work. They should also report if their own children/stepchildren/children they are living with become subject to child protection matters or an adult related to them or living with them become subject to adult protection matters. The line manager must report this to the DSL, Principal or Chief People Officer.

4.2 Governors and Senior Leadership Team

A governor's role for online safety in college includes:

- Upholding online safety as a safeguarding issue which is embedded across the whole college culture.
- Ensuring that young people are provided with a safe environment in which to learn and develop.
- Ensuring that the college has appropriate filters and monitoring systems in place.
- Ensuring the college has effective policies and training in place.
- Carrying out risk assessments on effectiveness of filtering systems.
- Auditing and evaluating online safety practice.
- Ensuring there are robust reporting channels.

4.3 The Designated Safeguarding Lead (DSL)

With respect to online safety, it is the responsibility of the DSL to:

- Ensure students are being appropriately taught about and know how to use the internet responsibly.
- Ensure teachers and parents are aware of measures to keep young people safe online through relevant training provision.
- Take responsibility for all safeguarding matters, including online safety.
- Facilitate effective record keeping and the reporting and monitoring of all online safety concerns.
- Promote online safety and the adoption of a whole college approach.
- Maintain own training and learning needs, ensuring they are up to date with all matters relating to online safety.

4.4 Students

With respect to online safety in college, students need to:

- Know the college Safeguarding Team
- Engage in age-appropriate online safety education opportunities.
- Read and adhere to online safety policies.
- Respect the feelings of others, both off and online.
- Take responsibility for keeping themselves and others safe online.
- Know where and how to find help with any online incidents or concerns.
- Know how, when, and where to report concerns and when to seek help from a trusted adult.

The college aims to equip students for digital life. The college aims to educate all students on the following topics:

- Self-image and identity
- Online relationships
- Online reputation

- Online bullying
- Managing online information
- Health, wellbeing, and lifestyle
- Privacy and security
- Copyright and ownership
- Artificial Intelligence

4.5 Parents and carers

Parents and carers need to understand the risks that students face online to protect them from online dangers. Parents/carers need to:

- Read and adhere to all relevant policies.
- Be responsible when taking photos/using technology at college events.
- Be aware of the college safeguarding team.
- Know how to report online issues.
- Support online safety approaches and education provision.
- Be a role model for safe and appropriate behaviour.
- Identify changes in students' behaviour that could indicate they are at risk of online harm or abuse.
- Understand the uses of AI.

To ensure parents and carers can respond appropriately the college shall:

- Recognise and cultivate the essential role parents and carers have in fostering safer online safety practices in students.
- Ensure provision of resources, support and advice.
- Ensure provision and adherence to online safety policies and other policies of relevance.
- Advise of how and when to raise concerns.
- Provide details of all relevant contacts (for example, the DSL).

5. Education and Training

Safeguarding activity across the United Kingdom (UK) continues to intensify in volume and intricacy with national influences relating to political uncertainty, a rise in poverty, an increase in the ageing population, sustained funding pressures and increased demand for child and adult services.

Furthermore, a commitment to ensuring the provision of an integrated and highly robust safeguarding service for all ages is essential. Effective online safety provision and promotion of the welfare of children and young people relies on constructive relationships that are conducive to robust multi-agency partnership working. This can only be effective when all staff are knowledgeable, confident, and equipped with the skills to deal with processes and procedures when concerns arise relating to online abuse or harm.

Online safety has a high emphasis on a competent well-established workforce, up to date policies and procedures, robust governance arrangements and collaborative practices.

Types of online risk usually fall under one of four categories:

Contact: Contact from someone online who may wish to bully or abuse the young person. This could also include online grooming, online harassment, or activities of a commercial nature, including tracking and harvesting person information.

Content: Inappropriate material available to children online including adverts, spam, sponsorship, personal info, violent or hateful content, pornographic or unwelcome sexual content, biased materials, racist materials, and misleading information or advice.

Conduct: The child may be the perpetrator of activities including illegal downloading, hacking, gambling, financial scams, bullying or harassing another child. They might create and upload inappropriate material or provide misleading information or advice.

Commerce: risks associated with online gambling, phishing or financial scams The college seeks to support students who are affected by these issues and educate students so that incidents are minimised in and outside of college.

5.1. Students

Richard Huish College promotes safe and responsible internet use:

- Education regarding safe and responsible use and access of the internet.
- Include online safety in Tutorial sessions.
- Reinforce online safety messages during curriculum delivery.
- Acceptable use information when a student logs into any college computer (see acceptable use policy <https://www.huish.ac.uk/wp-content/uploads/2023/05/RHT-Acceptable-Use-Policy.pdf>).
- Informing all students of monitoring and filtering in place.

5.2. Vulnerable students

Vulnerable young people who need our help the most are not only missing out on opportunities to flourish online but are often experiencing the very worst that the online world can be.

Richard Huish College recognises that some students are more vulnerable due to a range of factors. Those young people may be:

- Receiving statutory care or support.
- Known to have experienced specific personal harm.
- With a disability, ill-health or developmental difficulties.
- In households or families with characteristics or locations that indicate higher potential likelihood of current and future harm.

- Vulnerable or of concern by virtue of their identity or nationality.
- At risk in relation to activity or institutions outside the home.
- Caring for others.

Richard Huish College will ensure the effective and safe provision of tailored online safety education and obtain input and advice from specialist staff/agencies as deemed necessary.

5.3. Vulnerable students

To ensure staff can respond appropriately the college shall:

- Ensure provision of robust policies and practices as part of induction and ongoing training provision.
- Provide up to date online safety training at least annually or more in line with legislative and statutory changes and/or online safety incidents arising.
- Ensure training will include recognition of risks and responding to concerns.
- Inform of monitoring and filtering processes.
- Make staff aware that their online conduct outside of work can impact upon their professional role and responsibilities.
- Advise of appropriate resources.
- Ensure that all staff are aware of procedures to follow in recognising, responding and reporting online safety concerns.

6. Cultivating a safe environment

All staff should be aware of indicators, which may signal that young people are at risk from or are involved with serious violent crime. These may include increased absence from college, a change in friendships or relationships with older individuals or groups, a significant decline in performance, signs of self-harm or a significant change in well-being, or signs of assault or unexplained injuries. Unexplained gifts or new possessions could also indicate that children have been approached by, or are involved with, individuals associated with criminal networks or gangs.

Young people should be educated in an age-appropriate way around:

- How to evaluate what they see online.
- How to recognise techniques for persuasion Their online behaviour.
- How to identify online risks How and when to seek support.
- How to safely use Artificial Intelligence.

6.1 Evaluate: How to evaluate what they see online

This will enable students to make judgements about what they see online and not automatically assume that what they see is true, valid, or acceptable.

The college will help students in tutorial; curriculum sessions consider questions including:

- Is this website/URL/email fake? How can I tell?
- What does this cookie do and what information am I sharing?
- Is this person who they say they are?
- Why does someone want me to see this?
- Why does someone want me to send this?
- Why would someone want me to believe this?

6.2 Recognise: How to recognise techniques used for persuasion

This will enable students to recognise the techniques that are often used to persuade or manipulate others. A strong grasp of knowledge across many areas makes people less vulnerable to these techniques and better equipped to recognise and respond appropriately to strongly biased intent or malicious activity.

The college will help students to recognise:

- Online content which tries to make people believe something false is true and/or mislead (misinformation and disinformation).
- Techniques that companies use to persuade people to buy something.
- Ways in which games and social media companies try to keep users online longer (persuasive/sticky design)
- Criminal activities such as grooming.

6.3 Online Behaviour

This will enable students to understand what acceptable and unacceptable online behaviour looks like. The college will teach students that the same standard of behaviour and honesty applies online and offline, including the importance of respect for others. The college will also teach students to recognise unacceptable behaviour in others.

The college will help students to recognise acceptable and unacceptable behaviour by:

- Looking at why people behave differently online. For example, how anonymity (you do not know me) and invisibility (you cannot see me) affect what people do.
- Looking at how online emotions can be intensified resulting in mob mentality.
- Teaching techniques (relevant on and offline) to defuse or calm arguments (for example, a disagreement with friends) and disengage from unwanted contact or content online; and
- Considering unacceptable online behaviours often passed off as so-called social norms or just banter. For example, negative language that can be used, and in some cases is often expected, as part of online gaming and the acceptance of misogynistic, homophobic, and racist language that would never be tolerated offline.

6.4 Identify: How to identify online risks

This will enable students to identify possible online risks and make informed decisions about how to act. This should not be about providing a list of what not to do online. The focus should be to

help students assess a situation, think through the consequences of acting in different ways and decide on the best course of action.

The college will help students to identify and manage risk by:

- Discussing the ways in which someone may put themselves at risk online.
- Discussing risks posed by another person's online behaviour.
- Discussing when risk taking can be positive and negative.
- Discussing "online reputation" and the positive and negative aspects of an online digital footprint. This could include longer-term considerations, i.e. how past online behaviours could impact on their future when applying for a place at university or a job for example.
- Discussing the risks vs the benefits of sharing information online and how to make a judgement about when and how to share and who to share with.
- Asking questions such as what might happen if I post something online? Who will see it? Who might they send it to?

6.5 How and when to seek support

This will enable students to understand safe ways in which to seek support if they are concerned or upset by something they have seen online.

The college will help students by:

- Helping them to identify who are trusted adults.
- Looking at the different ways to access support from the college, police, the National Crime Agency's and 3rd sector organisations, such as Childline and the Internet Watch Foundation.
- Helping them to understand that various platforms and apps will have ways in which inappropriate contact or content can be reported.

7 7 7. Remote working guidance

The college has guidance for staff delivering remote learning sessions with students along with a student code of conduct for accessing remote learning. This guidance is regularly reviewed, updated and communicated to staff and students.

8. Responding to Online Safety Concerns

The safety of the student is of paramount importance. Immediate action may be required to safeguard investigations and any other students/people. Any concern that children and young people may be at risk of harm or abuse must immediately be reported.

Reputational issues must be managed appropriately by discussion with the Senior Management Team.

Online safety is recognised as part of the education setting's safeguarding responsibilities - the DSL should take lead responsibility for online safety concerns which will be recorded and actioned.

The college utilises Smoothwall web filtering services to monitor internet use. The filters applied by Smoothwall are continuously updated to ensure emerging content concerns are appropriately filtered and reviewed. Instant notification reports enable an immediate response to any concerning use of the internet these are sent directly to the DSL as well as the college safeguarding email address which is monitored by the safeguarding team.

The college safeguarding team complete a termly filtering and monitoring test using both a student and staff account. This allows for any concerns or issues to be identified and addressed through communication with the college IT team.

9. Responding to complaints

There are several sources from which a complaint or allegation might arise, including those from:

- A child or young person
- An adult
- A parent/carer
- A member of the public (including a friend or relative)
- A colleague

There may be up to three components in the consideration of an allegation:

- A police investigation of a possible criminal offence.
- Enquiries and assessment by children's social care or adult social care relating to whether a child, young person or adult at risk needs protection or services.
- Consideration by an employer of disciplinary action in respect of the individual (including suspension).

Useful Documents

Sharing nudes and semi-nudes: advice for education setting working with children and young people.

[Sharing nudes and semi-nudes: advice for education settings working with children and young people \(updated March 2024\) - GOV.UK \(www.gov.uk\)](#)

NSPCC online safety and schools.

[Online safety \(e-safety\) and schools | NSPCC Learning](#)

Online Safety in Schools and Colleges.

[Online safety in schools and colleges: questions from the governing board - GOV.UK \(www.gov.uk\)](#)

Online Safety Act - [Online Safety Act: explainer - GOV.UK](#)

South West Grid for Learning (SWGfL)

[Online Safety for Schools | SWGfL](#)

JISC – Staying safe online
[Staying safe online - Jisc](#)

Use of artificial intelligence in education delivery and assessment
[Use of artificial intelligence in education delivery and assessment - POST \(parliament.uk\)](#)