Online Safety Policy

Policy number:	SA002	**Policy Owner:**	Head of Safeguarding, Support and Inclusion
EIA Status:	Compliant	**EIA meeting date:**	03/02/2025
Approved by:	SLT	**Date approved:**	October 2025
	Committee		
	Board		
Review frequency:	Annually	**Next review due:**	01/10/2026
External website:	Yes	**Status:**	Active
Linked policies/ documents	• Safeguarding Policy • Positive Behaviour Policy • Staff Code of Conduct • Student Code of Conduct • Privacy Notices • Student learning agreements		

Policy Summary

Newbury College and the University Centre Newbury (UCN) have established a comprehensive Online Safety Policy to protect and educate their community—including students, staff, volunteers, governors, and other stakeholders—on the responsible use of digital technology. The policy aims to safeguard all users from online risks, promote respectful online behaviour, and ensure a safe digital environment both on and off college premises. It also sets clear expectations and procedures for incident management, compliance, and continuous improvement in online safety practices

Online Safety Policy

1. Policy Statement and Purpose

Newbury College and the University Centre Newbury (UCN) (hereinafter referred to as 'the College') are committed to ensuring the online safety of all members of our community, including students, staff, volunteers, and governors. This policy outlines our approach to safeguarding against the risks associated with the use of digital technology, ensuring that online behaviour is safe, responsible, and respectful.

The College aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
- Identify and support groups of students that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole college community in its use of technology, including mobile and smart technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- Set out expectations for all college community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the college gates and college day, and regardless of device or platform
- Facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of todays and tomorrow's digital world, to survive and thrive online

Purpose

The purpose of this policy is to provide a clear framework for protecting and educating the college community on the use of technology, addressing the four key categories of online risk:

- **Content**: Being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism.
- **Contact**: Being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying.
- **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

Scope

This policy applies to all members of the college which include staff, students, governors, volunteers, parents/caregivers, visitors, and community users) who have access to and use college digital systems, both on-site and remotely. It also governs the use of personal digital devices on college premises where permitted.

2. Definitions

- **Online Safety:** The practice of safeguarding users of digital technology, including the internet and electronic communication devices, from harm, such as cyberbullying, inappropriate content, and online predators.
- **Filtering Systems:** Technology used to block access to inappropriate or harmful online content while allowing access to necessary and educational material.
- **Monitoring Systems:** Tools and processes used to track and review the use of digital devices and internet access to ensure compliance with online safety policies.
- **Acceptable Use Policy (AUP):** A set of rules and guidelines that outlines the appropriate use of the college's IT systems and internet access, which all users must agree to and follow.
- **Cyberbullying:** Bullying that occurs online or through digital communication, often involving the repetitive and intentional harm of an individual or group through social media, messaging apps, or gaming platforms.
- **Digital Technology:** Any electronic tools, systems, devices, or resources that generate, store, or process data, including computers, smartphones, tablets, the internet, and social media platforms.
- **Safeguarding:** The action of protecting children and vulnerable adults from abuse, harm, and neglect, ensuring their well-being and safety.
- **GDPR (General Data Protection Regulation):** A regulation that sets guidelines for the collection and processing of personal information from individuals who live in the European Union (EU), ensuring data privacy and protection.
- **Radicalisation:** The process by which an individual or group adopts increasingly extreme political, social, or religious ideals and aspirations, potentially leading to terrorist activities.
- **Nudes/semi nudes:** The act of sending or receiving sexually explicit messages or images, typically between mobile devices.
- **Vulnerable Adults:** Individuals over the age of 18 who are at increased risk of harm or exploitation due to factors such as age, disability, illness, or personal circumstances.

3. Responsibilities

Corporation Board:

- Ensure online safety training for all staff as part of safeguarding training.
- Oversee the effectiveness of filtering and monitoring systems.
- Review the policy and associated procedures annually.

Principal:

- Implement and monitor the consistent application of this policy.

Designated Safeguarding Lead (DSL):

- Lead on online safety within the institution.
- Ensure incidents are logged, reviewed, and reported appropriately.
- Provide training and updates to staff and students on online safety.

IT Manager:

- Implement and maintain secure IT systems, including filtering and monitoring.
- Regularly review and update security measures.

Online Safety Group:

- Provides a consultative group that has wide representation from within the college community.
- Responsibility for issues regarding online safety and monitoring the Online Safety Policy including the impact of initiatives.

All Staff, students and other IT users:

- Adhere to this policy and the Acceptable Use Policy (AUP).
- Report any online safety concerns or incidents to the DSL or IT manager.

4. Policy

Acceptable Use

- All users must agree to the College's IT Code of Conduct. The expectations for responsible use of digital systems are detailed within related documents such as learner agreements, code of conduct policies and staff handbooks. Any breach of this policy may result in disciplinary action.

Education and Training

- **Students:** Online safety education will be provided through the Personal and Pastoral Development (PPD) programme and during student induction. Information will be tailored to meet the needs of vulnerable students and those with SEND.
  Adult learners,19+, who are within adult provision will consider online safety during induction. Resources will be provided via Student Hub, and teaching will be who are within adult provision will consider online safety during induction, resources will be provided via Student Hub and teaching embedded throughout the programme.
  Further details can be found in the Learning Agreement.
- **Parents/Caregivers:** Provided with resources and information to support their children's/young people's safe use of the internet.
- **Staff:** Receive ongoing training on online safety, including recognising and responding to online risks.
- **Employers and other stakeholders:** All employers providing work experience or apprenticeships have access to key online safety education and are required to adhere to keeping young people safe online.

Monitoring and Reporting

- The College's digital systems are monitored to prevent access to harmful content.

- Filtering systems block harmful content while allowing necessary educational content.
- Any misuse is logged and addressed following the appropriate procedures, with serious incidents reported to the police if necessary.
- The College's digital systems adhere to Cyber Essentials Plus requirements.

Incident Management

- The College has clear procedures for managing online safety incidents, including those involving cyberbullying, sextortion, and online harassment.
- Any misuse of IT systems or online safety incidents will be managed according to the Behaviour Policy and Safeguarding Policy. In serious cases, incidents may be reported to the police.

5. Compliance and Enforcement

Compliance with this policy will be monitored through regular reviews, audits, and risk assessments conducted by the DSL and IT manager. Non-compliance may result in disciplinary action according to the relevant policies.

6. References

- Keeping Children Safe in Education – DfE
- Protecting children from radicalisation - DfE
- Education Act 1996
- Education Act 2011
- Education and Inspections Act 2006
- Equality Act 2010
- General Data Protection Regulation (GDPR) 2018
- Teaching online safety in schools
- Preventing and tackling bullying
- Preventing and tackling cyber-bullying
- Searching, screening and confiscation
- Meeting digital and technology standards in schools and colleges

7. Supporting Documents

- Safeguarding Policy
- Positive Behaviour Policy
- Student Code of Conduct
- Staff Code of Conduct
- Privacy Notices

8. Review and Monitoring

This policy will be reviewed annually to ensure its effectiveness and compliance with relevant legislation.

Reviewed: [Previous review dates]

Next review date due: July 2025

Appendix A: Procedure for maintaining online safety and preventing incidents

This procedure outlines the steps the College will take to prevent online safety incidents, including cyber-bullying, sharing inappropriate content, and exposure to extremist material. It supports the Online Safety Policy by providing detailed guidance on the actions required to safeguard students and staff in the digital environment.

Education and Awareness

(See Appendix B: Procedure for educating students and parents about online safety)

For Students

- Online safety education is embedded in the Personal and Pastoral Development (PPD) curriculum for the 16-19 programmes both on and off-site provisions. This is also included for all foundation learning programmes.
- Induction sessions include a focus on online safety and acceptable use of technology for all students across the College (long distance learning, apprenticeships, work experience (WEX), UCN students, Bootcamp provision, community-based/tailored learning and FENNS.
- Ongoing education through tutor time, and special events like Safer Internet Day/awareness days. Regular communications will be shared on the student hub and equivalent platforms off site provisions.

For Staff, Governors, and Volunteers

- All staff receive training on online safety, including cyber-bullying and the risks associated with digital technology, as part of their safeguarding training.
- Regular updates and refresher training are provided, ensuring staff are informed about the latest online safety risks and how to mitigate them.

For Parents/Caregiver

- The College provides resources and information to parents/caregivers through newsfeeds, the website, and during parent evenings.
- Parents/ care givers are encouraged to discuss online safety with their children and monitor their online activities.

For employers and external partners

- Employers and external providers should use our secure platforms, like Egress, One File, and Grofar, to share and discuss personal student information.
- Employers and partner agencies are encouraged to implement secure platforms and actively monitor online activities to ensure the safety of our students.

Technology and Monitoring

Filtering and Monitoring

- The College employs filtering and monitoring systems to block access to harmful content and to monitor the use of college IT systems.
- Regular audits of filtering logs and alerts are conducted by the Online Safety Lead (DDSL) and IT Manager to ensure compliance.
- All off site provisions comply with the venue's broadband systems. We are working towards improving the filtering and monitoring activities.

Use of Personal Devices

- Clear guidelines are provided regarding the use of personal devices on campus.
- Students and staff are informed of the acceptable use policy, and any misuse is subject to disciplinary action.

Reporting and Responding to Incidents

Reporting Mechanisms

- Students and staff are encouraged to report any online safety concerns via the "See Something, Say Something" portal, directly to the safeguarding team, or through the safeguarding email.
- Incidents are logged and reviewed by the Designated Safeguarding Lead (DSL) and appropriate action is taken based on the severity of the incident.
- We provide information to secure platforms where students may wish to report any concerns directly to the platform such as Facebook, WhatsApp, Instagram. We will promote the 'Report and Remove' tool across the college on out student hub and messaging.

Incident Response

- **Cyber-bullying:** Incidents are managed according to the Behaviour Policy. Illegal content or harmful material spread among students will be contained, and the DSL will report to the police if necessary.
- **Radicalisation:** Any exposure to extremist material is immediately reported to the DSL, who will work with external services and follow the Prevent policy for the appropriate referral/response.
- **Nudes and Sextortion:** Any incidents involving the sharing of nudes, semi-nudes, or sextortion are escalated to the DSL and dealt with in line with the guidance from the Department for Education (DfE) and UK Council for Internet Safety (UKCIS). We wil follow the actions in this guidance and the flowchart below (extracted from the guidance).

Searching and Confiscation

(See Appendix C: Procedure for examining electronic devices)

- Staff authorised by the principal, are permitted to search and confiscate electronic devices if they have reasonable grounds to suspect they contain harmful material. Searches must follow the DfE guidelines, and any illegal content is reported to the police.

Responsibilities

Governing Board

- **Overall Accountability:** The Corporation board has overall responsibility for monitoring the Online Safety Policy and holding the principal accountable for its implementation.

All governors will:

- Ensure they have read and understand this policy.
- Agree to and adhere to the terms on acceptable use of the College's IT systems and the internet.
- Ensure online safety is integrated into the college's safeguarding policies and procedures.
- Ensure that online safety education is adapted for vulnerable children, victims of abuse, and students with special educational needs and/or disabilities (SEND) where necessary, recognising that a 'one size fits all' approach may not be suitable.

Principal

- **Policy Implementation:** The principal is responsible for ensuring that staff understand the Online Safety Policy and that it is being implemented consistently across the College.

Designated Safeguarding Lead (DSL)

- **Policy Implementation:** The DSL ensures that the Online Safety Policy is effectively implemented across the organisation, supporting the Principal and other staff.
- **Policy Review:** Annually reviews the Online Safety Policy with the Principal and governing board, ensuring updates are incorporated as necessary.
- **System Oversight:** Takes the lead in understanding and managing the filtering and monitoring systems on college devices and networks.
- **Collaboration:** Works closely with the IT Manager and other relevant staff to address any online safety issues or incidents promptly.
- **Incident Management:** Manages all online safety incidents according to the Safeguarding Policy, ensuring they are logged and resolved appropriately.
- **Cyber-bullying:** Ensures that incidents of cyber-bullying are logged and managed in line with the Behaviour Policy.
- **Training Delivery:** Updates and delivers online safety training to staff, conducting self-audits as needed to assess training needs.
- **Liaison:** Coordinates with external agencies and services when necessary to support online safety.
- **Reporting:** Provides regular reports on online safety issues to the Principal and/or governing board.

- **Risk Assessment:** Conducts annual risk assessments to identify and address the risks students face online.
- **Communication:** Ensures the Online Safety Policy and updates are accessible to all staff via SharePoint page and the College website.

IT Manager and Executive Director, Corporate Services

- **Security Measures:** Implements and regularly reviews security measures, including filtering and monitoring systems, to safeguard students from harmful online content.
- **System Monitoring:** Regularly monitors the college's IT systems, reporting any misuse to the appropriate manager or safeguarding lead.
- **Incident Logging:** Ensures all online safety incidents are logged and addressed according to the Behaviour Policy.
- **Cyber-bullying:** Reports any incidents of cyber-bullying to the appropriate manager, ensuring they are handled according to policy.
- **Technical Security:** Maintains the technical infrastructure to prevent misuse or malicious attacks, ensuring that all users have secure usernames and passwords.
- **User Management:** Keeps an up-to-date record of users and their access credentials, requiring users to change their passwords every six months.

HR Manager & Safeguarding Manager

- **Filtering & Monitoring:** Regularly monitors the filtering and monitoring reports, following college procedures as required. Escalating concerns to the DSL and/or DDSL for staff as appropriate.

Staff and Volunteer

- **Policy Adherence:** All staff and volunteers must understand and implement the Online Safety Policy consistently.
- **Acceptable Use Compliance:** Ensure compliance with the terms of IT Code of conduct of college IT systems and the internet, guiding students to do the same.
- **Incident Reporting:** Report any incidents related to filtering and monitoring systems to the DSL or IT services for appropriate action.
- **Educational Support:** Assist students in understanding appropriate online behaviour, reporting any concerns regarding misuse or inappropriate content. Tailor education support for vulnerable children, including those with SEND, seeking advice where required.
- **Cyber-bullying Response:** Manage any incidents of cyber-bullying according to the Behaviour Policy, ensuring a prompt and appropriate response.
- **Increased Vigilance:** Remain vigilant during lessons, particularly when students are conducting free research, and report any misuse to IT services or the safeguarding team.

Online Safety Group

- **Policy Review:** Assists the DSL in reviewing and monitoring the Online Safety Policy and associated documents.
- **Education Provision:** Maps and reviews online safety education, ensuring it covers relevant areas and provides adequate progression.

- **Monitoring Logs:** Reviews network, filtering, and monitoring logs where possible, encouraging learner contributions to online safety awareness.
- **Stakeholder Consultation:** Engages with staff, parents, and caregivers to gather feedback and improve online safety measures.
- **Improvement Monitoring:** Monitors the implementation of actions identified through self-review tools, ensuring continuous improvement.

All Users

- **Policy Awareness:** Anyone who use the college's IT systems must be made aware of the Online Safety Policy and expected to follow it.
- **Acceptable Use Agreement:** Where relevant, visitors must agree to the terms of acceptable use as outlined in the IT Code of Conduct.

Appendix B: Procedure for examining electronic devices

Procedure for the lawful examination and potential confiscation of electronic devices at the College in accordance with the Department for Education (DfE) guidance on Searching, Screening, and Confiscation.

1. Authorised Personnel

- **Principal:** Holds the authority to permit the examination of electronic devices.
- **Senior Leadership Team (SLT) and Curriculum Leadership Team (CLT) Members:** May be authorised by the principal to conduct searches.
- **Designated Safeguarding Lead (DSL):** Involved in decisions regarding the examination and potential erasure of data on electronic devices.

2. Conditions for Examination

An authorised staff member may search and confiscate an electronic device if they have reasonable grounds to suspect that the device:

- Poses a risk to staff or students.
- Is identified in the Behaviour Policy as a banned item.
- Contains evidence related to an offence, such as illegal or undesirable material, including but not limited to sexual images, pornography, violence, or bullying.

3. Procedure for Conducting a Search

3.1 Assessment of Urgency

- Determine the urgency of the search.
- If the situation is not urgent, seek advice from the principal and/or the DSL.

3.2 Communication with the Student

- Explain to the student the reason for the search, the process, and address any questions they may have.
- Seek the student's cooperation for the search.

3.3 Examination of Device

Authorised staff may examine, and in exceptional circumstances, erase data or files on the device where there is a 'good reason' to do so.

Good reasons include:

- The device has or could be used to cause harm.
- The device could undermine the safe environment of the college or disrupt teaching.
- The device contains evidence of an offence.

4. Handling Inappropriate Material

If inappropriate material is found:

- The DSL, Principal, or another senior leader will determine the appropriate response.
- If the material poses a risk to any person, consider the necessary safeguarding response.

4.1 Erasure of Data:

Staff may erase data if:

- The continued existence of the material is likely to cause harm.
- The student and/or their parent/caregiver refuses to delete the material.
- If the material is suspected to be evidence of an offence, it should not be deleted. Instead, the device must be handed to the police as soon as possible.

5. Special Considerations

5.1 Indecent Images of Children

- Staff must not view any images suspected to be indecent images of a child (nude or semi-nude).
- If nudes or indecent images are found, staff can confiscate the device immediately and report the incident to the DSL.
- The DSL will follow the DfE and UK Council for Internet Safety (UKCIS) guidelines on handling such incidents.

6. Coordination with Police and External Agencies

For students aged 19+, or in cases involving serious offences, the college will liaise directly with the police and relevant external agencies to determine the appropriate course of action.

7. Complaints and Appeals

Any complaints regarding the search, examination, or deletion of data from a student's electronic device will be handled through the college's complaints procedure.

Appendix D: Procedure for the acceptable use of digital devices and systems

This procedure outlines the acceptable use of digital devices and systems owned by the College to ensure the safety and integrity of the college's IT resources and its users.

Acceptable Use Guidelines

- **Educational Purpose:** Use of the college's digital devices and systems is strictly for educational purposes or activities that fulfil the user's role within the college.
- **Monitoring and Compliance:** All internet usage will be monitored to ensure compliance with this procedure. Access to certain websites may be restricted through filtering systems.

Digital Content (inc. images and video)

- **Image Use:** Staff and students may use digital content to support educational objectives. However, they must ensure that content used responsibly and ethically, avoiding any actions that might cause harm or embarrassment.
- **Consent:** Written consent is required before taking, using and/or publishing images or video of others.
- **Publication:** When publishing images, ensure that students are appropriately dressed and avoid using full names to protect their privacy.

Social Media

- **Guidelines:** Staff engaging with social media must follow the college's Code of Conduct and related polices, ensuring that no personal information about students or staff is shared, and professional boundaries are maintained.
- **Training:** The college provides training on the risks associated with social media use and how to mitigate these risks.

System Security

- **Incident Reporting:** Any technical incidents or security breaches must be reported immediately to the IT Help Desk.
- **Security Measures:** The college's systems are protected by security measures, including firewalls, virus protection, and regular security checks. Users must not attempt to breach or circumvent these measures.

Communication Technologies

- **College Platforms:** Communication between staff and students must take place only on official college platforms (e.g., college email or Teams).
- **Professionalism:** All communications must be professional in tone and content. Personal devices should not be used for college communications unless specifically authorised.

Use of Personal Devices

- **Students**: Students are allowed to bring mobile phones to college for emergency use or during lunch breaks. Care should be taken not to capture images of other students. Photos and videos should not be uploaded to social media without the consent of those identifiable in the content. During lessons, phones must not be used unless the teacher has given express permission for their use as part of a lesson. Unauthorised use during lessons or the taking of inappropriate photographs or videos will result in disciplinary action as per the Positive Behaviour Policy, including the potential withdrawal of mobile privileges.
- **Staff:** Staff should keep mobile phones on silent during work hours and only use them in private staff areas. Staff should not download student or staff data onto personal devices.
- **Volunteers, Contractors, and Governors:** If the use of a mobile device is necessary (e.g., to take photos of equipment or buildings), permission must be obtained from a member of the Senior Leadership Team (SLT) or the principal, and the action should take place in the presence of a staff member.
- **Parents and Visitors:** Permission should be sought before taking any photos, and care should be taken not to capture images of other students. Photos should not be uploaded to social media without the consent of those identifiable in the images.

Off-Site Use of College Devices

- **Security:** Staff must ensure that work devices remain secure when used off-site, including using strong passwords, encryption, and keeping software up to date.
- **Exclusive Use:** College devices must only be used for college-related activities and should not be shared with family or friends.

Use of Generative AI Tools

Generative AI tools (e.g., ChatGPT, Google Gemini, Microsoft Copilot, etc) may be used to support educational activities, including research, content generation, and problem-solving. However, users must adhere to the following guidelines:

- **Appropriate Content:** AI-generated content must be appropriate for the educational environment. It should not include or promote harmful, offensive, or misleading information.
- **Originality:** AI tools should not be used to create content that will be submitted as original work unless it is properly cited and acknowledged. Students and staff must ensure that AI use aligns with academic integrity policies.
- **Privacy:** Personal information must not be entered into AI tools, and any sensitive data must be handled in accordance with the college's data protection policies.
- **Ethical Use:** The use of AI must align with ethical guidelines, including avoiding deepfakes, AI-generated harassment, or other forms of misuse.