

ONLINE SAFETY POLICY

Effective for applicants, employees, volunteers, governors, potential students and students on or after September 2025.

Policy Category:	Learners
Approved by:	SMT
Policy Owner:	Vice Principal Student Experience and DSL
Applicable to:	Applicants, staff, students
Effective From:	September 2025
Date of next review:	September 2026

Contents

	SECTION	PAGE
1.	INTRODUCTION	3
2.	POLICY STATEMENT	3
3.	SCOPE	4
4.	RESPONSIBILITIES	4
5.	PROCEDURE	5
6.	OTHER RELEVANT POLICIES	7
7.	REVIEW	6

1. INTRODUCTION

It has been recognised that 'children can be at risk of harm inside and outside of the school/college, inside and outside of home, and online' (Keeping Children Safe in Education 2025). With young people constantly 'connected', the UCS College Group seeks to protect its students from online abuse and raise awareness of the risks inherent in online activity. Staff and students will be advised about how to attend remote learning safely and appropriately and parents/carers supported in their awareness of the risks.

2. POLICY STATEMENT

2.1 College Group will seek to limit access to, and raise student and staff awareness of, the online safety risks. These are categorised into four key areas:

- **Content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- **Contact:** being subjected to harmful online interaction with other users; for example: 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:** online behaviour that increases the likelihood of, or causes, harm; for example, 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.

2.2 UCS College Group will seek to ensure that its own IT systems are sufficiently resilient to protect users from others accessing their personal data, and, through effective filtering and monitoring, minimise the possibility of accessing inappropriate sexualised, violent or offensive material in line with the DfE's Filtering and Monitoring Standards and Cyber Security Standards.

2.3 UCS College Group will also seek to ensure the effective filtering and monitoring of College devices when used off College premises in other Wi-Fi domains. The current system to monitor this is called Lightspeed. This system is managed jointly by the Student Experience Teams and Digital Transformation Teams in line with the DfE's Filtering and Monitoring Standards and Cyber Security Standards.

2.3 UCS College Group will take appropriate disciplinary action when students or staff are engaged in illegal online activities, threatening the reputation or safety of others through online activity, or engaged in online bullying or harassment.

2.4 UCS College Group will consider any SEND issues when dealing with student online activity.

3. SCOPE

- 3.1 The Online Safety Policy applies to all College Group staff, governors, and volunteers, and students in College Group and in the workplace.
- 3.2 The Policy applies to students on work experience and work placement programmes and those engaged in any College Group organised off site activity.
- 3.3 The Policy applies to working arrangements with other agencies to support the College Group's Online Safety Policy, including local education authorities, schools, support agencies, sub-contractors and employers.

4. RESPONSIBILITIES

4.1 Online Safety Lead – Vice Principal for Student Experience and DSL (Designated Safeguarding lead)

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the College online safety and Safeguarding policies.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Ensures that training and advice are provided for staff, students, parents/carers and others.
- Alongside the College DSLs, represents UCS College Group and where necessary, the sector, and keeps professionally up to date, through participation in Somerset DSL updates and Somerset Colleges Safeguarding Committee meetings.

4.2 College DSLs

- Support and advise students and staff in their area of UCS College Group on online safety matters.
- Create online safety Tutorials (for students) and training (for staff).
- Keep professionally aware and up to date on online safety matters through regular in house and external training.

4.3 The Head of Digital Transformation ensures that:

- The College's IT infrastructure is secure and is not open to misuse or malicious attack.
- The College has a filtering procedure which is updated on a regular basis, and effective monitoring is able to detect misuse of systems so that this can be followed up. The filtering procedure should be able to be lifted on request for specific resources needed for genuine curriculum purposes, but only for the period of study. Filtering and monitoring will seek to protect students against exposure to radicalising or terrorist material, in line with the Prevent Duty and with Meeting Digital and Technology Standards in Schools and Colleges (October 2024).
- IT staff are up to date with relevant technical information in order to ensure network security and protection for users.
- A UCS College Group self-assessment using the DfE's [Plan Technology for Your School tool](#) following merger, which will be reported on in the Safeguarding Committee in 25/26.

4.4 Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of online safety matters, of current College online safety policy and practices, and of the College's filtering and monitoring

systems and procedures

- They have read, understood and accept the College Acceptable Use Policy when they log on to the network.
- They report any suspected misuse or problem to a DSL or Deputy DSL.
- Communications with students are carried out at a professional level – for example, they do not 'follow' students on personal social networking sites.
- Online safety issues are embedded in all aspects of the curriculum and other College activities.
- Students are supported to develop research skills and avoid plagiarism and uphold copyright regulations.

5 PROCEDURE

5.1 Staff guidelines for dealing with an online safety incident

When it becomes apparent that a young or vulnerable person has been the victim of bullying or harm through online activity and technology, the following steps should be taken:

- Ensure the young or vulnerable person is safe and no longer at risk of harm
- Check that others are not at immediate risk of harm from the same online safety issue
- Contact their College DSL or Safeguarding Officer.
- Work with the Safeguarding Officer, IT Services or Police investigation as required.
- Talk to your line manager if you feel in need of support following exposure to the incident.
- Consider what you and other staff can learn from the experience to reduce such incidents in future.

5.2 Education and training

Students

Online safety education will be provided in the following ways:

- Online safety awareness training will be offered at induction and via the Tutorial programme. This should aim to help students to understand and adopt safe and appropriate use of technology and social media both within and outside College, and develop resilience in the use of digital communication. For 2025/26 this will include an emphasis on Shore Space
- Students will be provided with a basic understanding of filtering and monitoring systems used by UCS College Group.
- Safeguarding and Prevent training will refer to related online safety risks.
- Students will be encouraged to be critically aware of content they access on-line and be helped to validate the accuracy of information
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet. Rules for use of IT systems will be accessible to students, for example on login screens.

Parents / carers

Many parents and carers have a limited understanding of online safety risks and issues, despite the amount of time that young people spend online. The UCS College Group will seek to provide information and enhance awareness for parents.

Opportunities will be taken to inform parents and carers:

- what their children will be asked to do online.
- with whom from the College they might be communicating online.
- how the College uses filtering and monitoring to protect young people online.

Staff

Online safety training will be offered:

- As a planned programme of formal online safety training.
- As part of the initial safeguarding training undertaken by all staff.
- In addition, other opportunities should be sought to enhance staff awareness of online safety, for example via newsletters and meetings.

Governors

- Governors will receive regular briefings on online safety, including updates on AI, misinformation, and cyber security, to support strategic oversight.
- Safeguarding Governors will be update on online safety and filtering and monitoring processes via Safeguarding Committee.

5.3 Social Networking

The College's policy on the use of social media sites is that:

- The College accepts that students will wish to access social media sites and appropriate access will, where possible, be provided. However, the College Group will reserve the right to limit access where this prevents others from using IT facilities for study purposes.
- Students will be warned of the dangers implicit in the use of social media, such as making 'friends' with strangers and the risks of grooming.
- Staff will be supported in understanding the privacy and location settings on Social Networking sites and using these to help avoid potential allegations.
- Staff will be told explicitly that they must not accept 'follow' requests from students on personal social media sites, including LinkedIn.

5.4 Use of digital images and video

Staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

- When using digital images, opportunities should be sought to educate students about the risks associated with the taking, use, sharing, publication and distribution of images, via social networking sites or messaging services ('sexting' for example).
- Students and staff must not take, use, share, publish or distribute images of others without their permission. Images of students should not be posted on individual staff members accounts (such as LinkedIn), unless they are being re-shared from Marketing.
- Photographs and videos of students published on the College website, or in printed media, will be selected carefully and will comply with good practice guidance on the use of such images. Where practicable written permission from students will be sought, and from parents or carers when photographs of students under 16 are published. Care should be taken when taking images that students are appropriately dressed and are not participating in activities that

might bring the risk of harm to individuals or bring the College into disrepute.

6 OTHER RELEVANT POLICIES AND DOCUMENTS

This policy should not be read in isolation but should be cross-referenced to other relevant College employment and student policies and procedures, including:

- [Safeguarding and Child Protection Policy and Procedure](#)
- [IT Acceptable Use Policy](#)
- [Mobile Device Policy and Procedure](#)
- [Staff Disciplinary Policy and Procedures](#)
- [Data Protection Policy and Procedure](#)
- [Keeping Children Safe in Education Part 1](#) (2024)

7 REVIEW

This policy will be reviewed annually, or earlier where new technological advancements suggest revision is necessary.