SHREWSBURY COLLEGES GROUP

ONLINE SAFETY POLICY

Contents

Policy Overview....1
1. Introduction....1
2. Online Safety College Statement....1
3. Policy Scope....1
4. Roles and Responsibilities....2
5. Education and Training....4
6. Remote working guidance....6
7. Filtering & Monitoring - Responding to Online Safety Concerns....6
8. References....8
9. Links with other policies and practices....8
Appendix A – Guidance for staff working remotely with students....10

SHREWSBURY COLLEGES GROUP

ONLINE SAFETY POLICY

Policy Overview

The purpose of this policy is to safeguard and protect all members of the college community 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 and visitors who have access to, and are users of, our digital technology systems both on and off campus.

1. Introduction

Online safety in education is of paramount importance. As the online world evolves, so do both the online risks facing members of the college community and the relevant legislation and guidance 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 approach to online safety is adopted and that all stakeholders are aware of their responsibilities and duties in relation to keeping students, particularly where they are children, safe online.

2. Online Safety College Statement

Shrewsbury Colleges Group sees online safety is an essential element of its statutory duty to safeguard children and adults and undertakes to do all that it can to protect students and staff from online harms.

We believe that all students should be supported to build resilience and to develop strategies to recognise and respond to online risks as well as to provide an environment where they are directly protected from the risks as they occur.

3. Policy Scope

This policy lays out the ways in which the college discharges the statutory and other requirements around online safety set out in Keeping Children Safe in Education (2024) and the associated guidance and legislation listed in section 8 of this policy.

The policy outlines the expectations of all members of the college community with regards to online safety relating to governance, oversight, safeguarding practice, education and conduct. It relates to online safety on and off campus and using equipment owned by the college as well as that which is privately owned.

The policy seeks to cover the use of all online mediums including, but not restricted to:

- The internet
- Mobile phones

- Systems designed to support learning used in college such as Microsoft Teams
- Social media
- Text messages and messaging apps
- Email
- Online chats
- Online gaming
- Live streaming sites

There are a number of areas of abuse and concern that our approach and policy seeks to cover. The below list is not exhaustive but includes:

- Online bullying and harassment
- Relationship abuse
- Sharing of nudes and semi-nudes
- Cyber Crime (as both potential victim and perpetrator)
- Emotional abuse
- Grooming (including into exploitation and radicalisation
- Access to inappropriate content including pornography
- Risk taking behaviour such as online gambling
- Online reputation and digital footprint

4. Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of stakeholders across the college community.

4.1. Staff

All members of staff have a responsibility to protect students online.

All staff need to:

- Always act in the best interests of students.
- Act in accordance with professional boundaries as set out in the college Safe Working Practice Guidance and Social Media Policy, upholding professional behaviour and conduct at all times.
- Be aware of, and adhere to, all policies in college which support online safety and safeguarding.

- Support in the taking of responsibility for the security of systems and the data accessed.
- Model good practice when using technology and managing the use of mobile phones in lessons, whilst being able to use them for educational reasons where appropriate.
- Play a key role in the monitoring of student use of technology in college. This includes direct supervision when in the classroom and, in line with usual safeguarding practice, being alert to student safety in other contexts. This includes challenging inappropriate use when witnessed and reporting concerns.
- Know and follow the process for making referrals and reporting concerns relating to safeguarding.
- Know how to recognise, respond and report signs of online abuse and harm.
- Engage in mandatory safeguarding and Prevent training.
- Be responsible for their own continuing professional development in online safety.

4.2. The Lead Safeguarding Governor

The lead governor should support online safety by:

- Promoting online safety as a safeguarding issue which is embedded across the whole college culture.
- Liaising with the Senior Designated Safeguarding Lead to ensure online safety policies and practice adhere to the appropriate guidance, including Keeping Children Safe in Education (2024).
- Reporting assurance around matters relating to online safety to the college governing body.
- Ensuring that the college has appropriate filters and monitoring systems in place and attending the Annual Review of these processes to ensure that the college meets the standards stipulated in the digital and technology standards for schools and colleges.

4.3. Senior Designated Safeguarding Lead (DSL)

The Senior DSL is responsible for:

- Promoting online safety as a safeguarding issue which is embedded across the whole college culture.
- Ensuring online safety policies and practice adhere to the appropriate guidance, including Keeping Children Safe in Education (2024).
- Reviewing, auditing and risk assessing online safety processes in the college to ensure that the requirements of statutory and other guidance

are met. This is to include the Annual Review process for the Filtering and Monitoring standards.

- Working with the Vice Principal – Apprentices, Quality and Information to ensure that appropriate technical systems are procured and implemented to keep students and staff safe online.
- Maintaining own training levels to ensure an up to date knowledge of the requirements around online safety.
- Ensuring appropriate education for students following the framework of Education for a Connected World.
- Providing appropriate information and support for parents and carers to enable to help them with their duty to keep their children safe online.
- Ensuring there are robust and accessible reporting channels for staff and student concerns.
- Facilitating effective record keeping and the reporting and monitoring of all online safety concerns.

4.4. Students

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

- Adhere to the Acceptable Use of IT policy (AUP).
- Be aware that whilst they are permitted to bring their mobile phones or other smart devices to college they are to not to use them in lessons without permission of the teacher.
- Be aware of how to access the Safeguarding Team, report concerns and seek report when needed.
- Engage with the online safety education provided following the Education for a Connected World framework and other sources as appropriate such as Cyber Choices
- Behave respectfully towards others online including in their use of mobile phones.
- Take responsibility for keeping themselves and others safe online.

5. Education and Training

The college carefully plans education and training for students, staff and parents and carers to ensure a comprehensive and up to date understanding of risks surrounding online use and how to help mitigate those risks.

The college is a member of the National College which provides resources and materials which underpin the approach that we take in this important area.

A broad outline of this approach is given below for the key audiences.

5.1. Students

The college approaches educating students on online safety through:

- Making sure that students understand the college approach to acceptable use as they enrol to the college and reinforcing this message with each log on to college systems.
- Providing education regarding safe and responsible use and access of the internet, including the educational and personal dangers associated with excessive mobile phone use.
- Including online safety in Tutorial session.
- Reinforcing online safety messages during curriculum delivery.
- Informing all students of monitoring and filtering in place.
- Making clear expectations around online conduct, including legalities around the sharing of images, relationship abuse, hate speech and harassment/ bullying.
- Raising awareness of online risks related to radicalisation, in the context of local and national risk.
- Ensuring risks around online scams, hoaxes and activities such as gambling are understood.
- Implementing peer support strategies with an element of students educating and supporting each other.
- Using alternative, complementary support where needed, such as referral to CEOP, Cyber Choices and Prevent.
- Following our safeguarding or SEND risk assessment of individual students to put in place additional support and education for vulnerable students as appropriate. This may be a formal aspect of the support in an EHCP, Early Help or care plan and may also include the restriction of access to college IT systems.

5.2. Staff

To ensure staff are equipped to help keep students safe on the college will:

- Provide guidance on how to report concerns as part of the new staff induction
- Provide ongoing online safety training in order to ensure staff are up to date with online threats and any legislative and statutory changes.
- Ensure Raising Awareness training includes recognition of risks and how to respond to concerns.
- Inform staff of monitoring and filtering processes and their responsibility to help keep students safe online.

- Make staff aware that their online conduct outside of work can impact upon their professional role and responsibilities.
- Provide access to enhanced training in relation to online safety that is based upon the specifics of their role, for example as a designated safeguarding lead or member of the safeguarding team.

5.3. Parents and carers

To support parents and carers to keep their children safe we will provide information to help:

- Recognise and cultivate the essential role parents and carers have in fostering safer online safety practices in young people.
- Develop their knowledge of what to do if they need to support their child to report online content and/ or have it removed.
- Provide access to resources, support and advice.
- Advise of how and when to raise concerns with college and how to access support when they have concerns

6. 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 and updated and communicated to staff and students as appropriate.

See Appendix A – Guidance for staff working remotely with students.

7. Filtering & Monitoring - Responding to Online Safety Concerns

Aims

The college takes measures to provide a safe environment to learn and work online. Filtering and monitoring are both important parts of safeguarding students and staff from potentially harmful and inappropriate online material.

This work is guided by the standards listed in Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk).

Filtering and Monitoring processes in the college are, as Senior Designated Safeguarding Lead, the responsibility of the Vice Principal – Students.

Decisions about filtering and monitoring are made considering the stipulations mentioned in the standards. Namely:

- The context of the college in terms of our staff and student population as well as local and national risks

- The digital resilience of students and the levels of vulnerability of specific students such as those with SEND and those with identified safeguarding needs.
- The balance between restriction and the processes related to effective teaching and learning. Systems should block harmful and inappropriate content but not unreasonably impact teaching and learning.

In order to achieve the above the college adopts an approach to filtering that means that a high level of assurance is given that content cannot be accessed on college systems or equipment that is contrary to what is expected in the standards. This includes for the filtering and monitoring of devise such as mobile phones using the BYOD facility.

Where a risk assessment indicates the need, a higher level of restriction is placed on some students in order to keep them safe.

Where a study programme, in order to be studied effectively, needs access to resources that are legitimate but are blocked by the filter, temporary or permanent exceptions can be made so that the content can be accessed. There is a process in place whereby this is authorised by the Vice Principal – Students and Vice Principal – Apprentices, Quality and Information.

Where new safeguarding risks emerge the changes to the block list for the college commercially procured system are dynamically updated. However, this is supplemented, especially around local risks, with local testing of the filter against identified search terms giving an added level of assurance.

Monitoring takes place by reporting on a live, daily and weekly basis of the activity of students and staff as well as in person monitoring of online activity by staff. Where concerns are identified these are followed up according to the relevant college policy. For example, Safeguarding, Prevent, Conduct or Anti-Bullying. This includes the misuse, or concerns raised around risks related to the use of, mobile phones.

The filtering and monitoring processes are formally reviewed by the Lead Governor, Senior Designated Safeguarding Lead, Deputy Senior Designated Safeguarding Lead, Vice Principal –Quality, Apprenticeships and Information and the Head of Technical Services on an at least annual basis. This review is documented in an Annual Review Report based on resources issued by the Safer Internet Centre.

The process is also reviewed if there are significant changes to IT provision in the college or the safeguarding risk profile locally or nationally.

8. References

The following legislation and guidance is linked to the college approach to Online Safety.

Keeping children safe in education (2024) Keeping children safe in education 2024

Teaching online safety in schools Teaching online safety in schools - GOV.UK

Digital and technology standards in schools and colleges Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK

Education for a connected world Education for a Connected World - GOV.UK

Mobile phones in schools Mobile phones in schools - GOV.UK

UK Council for Internet Safety guidance Online safety in schools and colleges: questions from the governing board - GOV.UK

Harmful online challenges and online hoaxes Harmful online challenges and online hoaxes - GOV.UK

Children Act 2004

Communications Act 2003

Computer Misuse Act 1990

Criminal Justice and Courts Act 2015

Data Protection Act 2018

Education Act 2011

Education and Inspections Act 2006

Freedom of Information Act 2000

Malicious Communications Act 1988

Serious Crime Act 2015

Voyeurism (Offences) Act 2019

9. Links with other policies and practices

- Whistleblowing
- Anti-bullying
- Social Media
- Safeguarding Children and Adults with Care and Support Needs
- Prevent
- Acceptable Use Policies

- Student Conduct policy
- Safe Working Practices
- Complaints policy
- Data protection policy
- Guidance for staff working remotely with students

Appendix A – Guidance for staff working remotely with students.

This guidance is in place to ensure that you take all practicable steps to keep yourself and students safe whilst working remotely. It follows advice that has been given in, and linked to, Keeping Children Safe in Education.

The guidance applies to live or recorded content that staff are providing where students are accessing remotely.

It should be considered alongside the college polices on Information Technologies Acceptable Usage, Social Media, Home Working, Safe Working Practice and Safeguarding.

The college recommends that you use Microsoft Teams, Moodle or existing course-based Facebook Closed Groups to facilitate teaching and learning remotely.

Guides and training are available for staff and students to enable effective use of Microsoft Teams and we recommend that this is the medium used for live video conferencing with students.

Safeguarding yourself and your students

- DO use channels which are provided by the college e.g.) Teams, Moodle, Facebook Groups where students are secured by their college email and/or login
- DON'T contact students via means where they have to use their private email or contact details
- DO have a record of the conference/ live session timing and who participated, including those that arrived/departed early or late.
- DO feel able to use the video facility so that students can see you (though check that there is no personal information or artefacts visible in the background). NOTE – there is the facility in Microsoft Teams to blur the background and we recommend that you should do this if working from home.
- DO record your video session so that you have evidence of interaction (as a safeguarding check) and so it can be shared. This is especially important if the session is 1:1. Please make sure students are aware that this recording is taking place, the purpose of the recording and that they can opt out of recording by making the simple announcement below at the start of each recorded session;

  > "This session is being recorded (add where appropriate where it is to be shared with students in the class). All participants have now been informed of its use and have consented to being recorded. Any participant not wishing to be recorded can mute their audio and/or video at any time."

- DO dress professionally (as you would on campus) if video conferencing
- DO make clear to students that good behaviour (classroom standard) is expected and that inappropriate behaviour (including where this involves messages to other students) will be dealt with through the conduct policy.

- DO make sure that if a camera is used showing students at home, the background is blurred to protect the privacy of others in the room. The use of cameras by students shouldn't be compulsory and in most cases students should be asked to turn their cameras off.
- DO NOT under any circumstances provide students with your personal phone number, email or address
- DO only contact students within college hours (08.30-17.00 Monday to Friday) or normal delivery hours outside of this time for some Adult/ Higher Education students so as to manage expectations and ensure that you have support from the safeguarding team should concerns emerge.
- DO NOT arrange to meet with students even if in a public place or as a group
- DO NOT contact students on personal social media platforms. Be aware of invitations via Snapchat, Instagram, Facebook etc from students.

The Safeguarding Team are available 08.30-17.00 Monday to support with concerns or disclosures that may emerge whilst working remotely.

Safeguarding links are available on the college website for what to do if there is a safeguarding concern out of normal college working hours - Safeguarding | Shrewsbury Colleges Group (scg.ac.uk)