ONLINE REVIEW

ORIGINATOR: Alexandra Emmerson

September 2023

Overview

Children today are firmly part of the digital age and, as such, often use a wide range of devices, both inside and outside of the College day. When used correctly, technology can be a fantastic learning and social tool, but students need to have a clear understanding of expectations and rules surrounding its use. The College is committed to providing this education through a number of contributing factors which help students to stay safe online and not fall foul of the myriad of risks and threats which can occur.

Policies and Procedures

The College has robust online safety policies and procedures which show how to safeguard against and respond to online safety incidents. All stakeholders have been made aware of these.

The policies and procedures for online safety follow legislation and guidance for child protection in schools. Policies also include the Government's Prevent Duty guidance (April 2019 updated September 2023) regarding online safety and radicalisation. The following policies contain information pertaining to online safety:

- Federation Safeguarding Policy
- Federation ICT Code of Conduct Policy
- Catmose College Behaviour Management Policy
- Federation Close Personal Relationships at Work Policy
- Federation Data Protection Policy

All policies are available on the College and RDSF websites and are reviewed annually.

The named person for online safety is the Designated Safeguarding Lead, currently Alex Emmerson, supported by the safeguarding team.

Teaching Online Safety

The College ensures that online arrangements are robust by teaching its students, through the tutorial programme and computing curriculum, a number for topics which fall under these headings:

Content: illegal, inappropriate and harmful material

Students are taught to critically assess content in order to make a safe choice. Key thinking is around:

- 'Online reputation' and 'digital footprints': What does yours say about you? How could this affect you in the future?
- The risk of online behaviour – both positive and negative.
- The risks and benefits of sharing information online, with whom and when.
- Secure passwords and internet security.
- How to protect personal data.

Contact: harmful online interactions with advertising or individuals

Students are taught to understand that not everything they see online is true, valid or acceptable, and that sometimes people are not who they say they are, or are not sharing real information. Key questions students are taught to ask are:

- Is this content, website, link or email fake?
- What information am I sharing?
- Is this fact or opinion?
- Why am I being sent this?
- Should I share this?

Conduct: personal online behaviour which can cause harm

Students are taught techniques to recognise persuasive content and avoid manipulation. They are also taught to recognise and respond appropriately to malicious or detrimental activity or requests.

- Am I being asked to do something I am not comfortable with?
- Am I being asked sensitive or personal information?
- Is this service/product/advert legitimate?
- Do I want to keep engaging in this game or with this individual?

Reporting, monitoring and seeking support: how and where

Students are challenged to think and understand what is acceptable and unacceptable behaviour and how to realise that the same standards of behaviour and honesty apply both online and offline. Key discussions in the curriculum are around:

- Why people behave differently online (anonymity and invisibility)
- How emotions can be intensified online
- How arguments and disagreements can be defused
- What constitutes banter and what is abuse
- How to deal with negative, racist, homophobic or misogynistic language online

The computing curriculum draws from DfE guidance 'Teaching Online Safety in Schools' (June 2019, updated January 2023). In addition, it also addresses topics contained within the 'Education for a Connected World' (February 2018, updated June 2020).

The curriculum has a deliberately planned online education programme which is taught across all year groups and progresses as students grow and develop. It builds on the skills learnt at primary school and uses the limited information of the National Curriculum to further students' skills. Within the GCSE course there is a unit of work dedicated to consequences of computing, which includes online safety content such as privacy, data protection and cyber security. In order for staff to stay up-to-date with new specifications they are continually undertaking Continued Professional Development through exam boards and their own inquisitive development of their skills. A recommendation would be for teachers of Computer Science to undertake more formal training, with qualifications where applicable, in order to deepen their already established knowledge.

The spiral curriculum across KS3 embeds and develops strategies for navigating the online world and prepares students for KS4. A key skill needs analysis at KS4 also helps to shape and navigate the KS3 curriculum intent and implementation. A good example of this is the understanding required at KS4 around the ethical use and preparing students accordingly for this. Therefore, within KS3 members of staff have ongoing conversations with students about the benefits and dangers of the internet and create an open environment for students to ask questions and raise concerns. This open dialogue leads to the opportunity for students to make informed choices about their actions online. Age-appropriate conversations also allow students to recognise the dangers of misinformation, illegitimate and criminal activities such as online grooming. This ethos of open and mutual communication creates an environment where trust is established and this means staff are able to manage and mitigate risk for students with positive successes. The following example demonstrates the impact this has had: a young student was concerned about the welfare of a peer who had posted photographs online. The student emailed their concerns to the Client Services team including copies of the information/photographs. This was then followed up in the appropriate safeguarding manner. This clearly identifies the learning and student's ability to make good choices to keep their peer safe.

In addition, checkpoints and key assessments in all year groups directly monitor the impact of students' knowledge and understanding of their learning in this topic.

The tutorial programme supports the teaching within the computing curriculum. It provides opportunities for students to reflect on topics and equip them with further knowledge of how to respond, report concerns and make positive choices. Topics such as online grooming, sexting, peer-pressure and relationships are explicitly taught using Child Exploitation Online Portal (CEOP) workshop material provided by the Home Office, the Brecks Last Game video and My Digital Footprint. Recent assemblies on conspiracy and understanding the use of 'cookies' has generated discussion amongst the College population with many students and staff claiming that, prior to this teaching, they had little understanding of what cookies actually did. Workshops led by Leicestershire Police, the Relate counsellor and Knife Crime provided by the Youth Offending Service further complement and support the work of tutor-led sessions. These examples of external agencies work together are critical in ensuring staff and students have the most up-to-date information to help them stay safe in the everchanging digital world.

Supporting parents also helps keep students safe online. The College provides tips, advice, guides and resources through its termly safeguarding newsletter ensuring that parents are kept informed with the current hot topics and trends. In addition, all parents were given an opportunity to attend three sessions delivered by Souster Youth as part of its iGeneration programme. These were:

1. Digital Technology
2. Emotional Health

3. Relationships and Sex

Below is a quote from a parent regarding these sessions:

> *''Thank you so much for the informative and excellent workshop. I thought I was rather tech-savvy; however, I gained a wealth of knowledge from the session on digital technology! I feel better informed how I can support my children with the use of technology and apps on their smartphones.''*

Monitoring and assessment of need is driven by information reported through our normal safeguarding arrangements on Child Protection Online Management System (CPOMS). Online concerns are followed up through the same procedures as all other safeguarding concerns; practice is parallel. Intervention and support are bespoke to the individual concern raised. Weekly intervention and safeguarding meetings look for patterns and emerging trends within the community in order for more support to be delivered to target particular groups of students or year groups. A good example of this is the Leicestershire Police workshop on Criminal Exploitation which specifically worked with a group of students who had been identified as vulnerable in the area. In addition, DSLs also regularly attend Rutland County Council exploitation meetings and forums to ensure their knowledge and skills in dealing with this topic are current. The DSL is also Prevent Level 2 qualified.

Recommendations

- Teachers of Computer Science to attend further CPD or undertake further qualifications to deepen their knowledge of this topic.
- Teachers of Computer Science to lead a CPD to upskill all staff on current online topics.
- Teachers of Computer Science to create three assemblies linked to conspiracy, misinformation and privacy to share with all students in tutorial.