ONLINE SAFETY POLICY

DATE ADOPTED: DECEMBER 2023

1. RATIONALE

Online learning, creative and collaborative resources enrich students' experiences of learning in dramatic ways. In addition, the modern young person is a "digital native" in that they use a myriad of online and mobile tools with great confidence, enthusiasm and flair to communicate, record, document their lives and entertain themselves.

With this familiarity comes risk. There are horrific crimes being committed online, including cyberbullying, child pornography, child abuse, child trafficking and fraud. Many young people are not experienced enough to fully understand the risks of using online tools and the consequences their actions may bring. This policy provides a framework for the college to take measures to protect our students and other stakeholders from these risks and to support them in becoming confident, online safe citizens.

The Online Safety Policy is an integral part of the college's day to day practice and relates to other policies including those for ICT, bullying and for child protection.

2. ROLES

EXECUTIVE PRINCIPAL (KIM EVERTON)

2.1. Takes ultimate responsibility for Online Safety Policy and practice within college.
2.2. Communicates with Board of Trustees on online safety matters.
2.3. Supports Online Safety Coordinator in the implementation of the policy.
2.4. Ensures any instances of ICT misuse are dealt with in the appropriate manner.
2.5. Supports the Online Safety Coordinator in the implementation of incident management protocols.
2.6. Advises the Online Safety Coordinator on trends in students' ICT use that they become aware of.
2.7. Develops and maintains a knowledge of current online safety related issues.
2.8. Develops and maintains a knowledge of current online safety related issues, with particular regard to how they might affect vulnerable people.
2.9. Liaises with parents of students with SEN on online safety matters.
2.10. Develops procedures to support students who are identified by staff as needing support, as well as those who self-refer.

BOARD OF TRUSTEES

2.11. Supports the Executive Principal and other designated staff with regard to online safety related matters.
2.12. Ensures funding is available to implement and maintain online safety.
2.13. Reviews reports on online safety.

MAT-WIDE / ONLINE SAFETY COORDINATOR (RYAN PERRENS) / ICT OPERATIONS MANAGER (ARON V DAVIES)

2.14. Reports to / updates the Executive Principal.
2.15. Communicates with other key members on online safety related matters.
2.16. Responsible for development and maintenance of online safety policies.
2.17. Responsible for implementation of incident management protocols.
2.18. Leads staff professional development in online safety knowledge.
2.19. Liaises with outside agencies (e.g. Safeguarding Adults, Local Authority [LA]).
2.20. Ensures that the technical infrastructure is in place, maintained and updated to support online safety (e.g. firewall, backup, Internet monitoring, filtering systems).
2.21. Stays up to date with technical trends and issues concerning the ICT infrastructure and online access.

WHOLE COLLEGE COMPUTING COORDINATOR (AMBER WOOD)

2.22. Works with college staff on subject-specific issues regarding online safety (e.g. filtering of resource sites) and training needs.
2.23. Ensures a uniform approach to online safety within the college.
2.24. Encourages the development of an online safe set of online resources for use within the department.
2.25. Responsible for coordinating online safety curriculum programme.
2.26. Responsible for parental contact and information regarding online safety.

ALL STAFF

2.27. Implement the Online Safety Policy.
2.28. Develop and maintain a knowledge of current online safety related issues.
2.29. Ensure online safety and copyright messages are reinforced in ICT activities.
2.30. Check resources and links when planning ICT activities to ensure that inappropriate material is not inadvertently viewed.
2.31. Report breaches of ICT security through the relevant channels.
2.32. Maintain professional conduct when online, both inside and outside college.

STUDENTS

2.33. Strive to uphold the Online Safety Policy.
2.34. Develop skills of critical review and working safely, both on technical and personal levels.
2.35. Report any ICT misuse to a teacher.
2.36. Report any inadvertent viewing of inappropriate content to a teacher.
2.37. Seek help from an adult if they face problems.
2.38. Discuss / educate parents / carers about online safety issues.

3. ACCEPTABLE USE

3.1. The college declares that all students and staff can use the ICT equipment for legitimate purposes, acting within a remit appropriate to their professional / student status, employ online safe practices consistently and follow procedures regarding online safety.
3.2. Staff are required to sign an AUP before being granted access to the college's ICT infrastructure and portable devices. AUPs are reviewed annually by the ICT Operations Manager to ensure that they

are fair, up to date and take account of the latest technological advances and Best Practice from ICT advisory bodies.

4. ONLINE SAFETY EDUCATION / TRAINING

All ICT users are at risk of crimes such as cyberbullying, grooming, extremism, stalking and identity fraud through the illegal use of information and channels found online.

Students are taught:

4.1. That there are many risks to disclosing personal data online.
4.2. To carefully consider what personal information to put online and what it may be used for.
4.3. About the consequences and impact of Cyberbullying, and what to do about it.
4.4. About the techniques some people employ to extract information for illegal use.
4.5. Procedures when involved in online safety incidents, at home and in college.
4.6. How to ensure their personal data is kept safe from technological threats such as viruses and Trojans.
4.7. Not to trust information from unverified sources and unknown people.
4.8. How to critically review and verify any information found online.
4.9. About extremism and how online platforms can be used to radicalise.
4.10. About copyright law, how it protects everyone, how to work within the law when collecting and using digital information.

5. INFORMAL TEACHING OPPORTUNITIES

5.1. It is important to consider that effective teaching of online safety skills in students is not simply a matter of “covering units”. All staff should be aware of online safety issues and build them into their teaching wherever possible, even as an informal class discussion. Advantage should be taken of students’ own experiences to discuss online safety with them.

6. FOR STUDENTS

There is a coordinated curriculum of online safety awareness:

6.1. The core elements of online safety are covered at an appropriate level to ensure students are prepared for the dangers they could face online.
6.2. Students progressively learn more about online safety with more elements being introduced and further detail being added to core elements to ensure students have a solid understanding of all dangers and how to cope with them.

The online safety curriculum is reviewed annually as part of normal scheme reviews.

7. FOR PARENTS / GUARDIANS

7.1. This document is available to parents on the college website. This ensures that Parental information on the college's ICT provision, expectations of students and online safety are shared.

8. FOR STAFF

8.1. New staff are trained in online safety matters as part of the induction programme. In addition, support and guidance are available from the Online Safety Coordinator.
8.2. For existing staff, online safety training is delivered annually as a standalone session and is also incorporated into the whole-college INSET programme as part of the Child Protection training.
8.3. The staff curriculum is based on the programme delivered to the students, covering the same points. In addition, staff are trained on classroom management techniques to minimise risks to students and themselves.

9. ASSESSMENT

9.1. Assessment of online safety education and policy effectiveness is conducted as an integral part of their education. Students are taught about the subject at least once a year and work is assessed and feedback is given to reinforce understanding and knowledge.

10. CLASSROOM REINFORCEMENT

10.1. Whenever ICT is used in the classroom, all adults need to be aware of the potential for online safety incidents and breaches of ICT security. To minimise the risk of online safety incidents, staff should all adhere to the following classroom management protocols concerning online safety.
10.2. Always research web links before a lesson - can a student easily find themselves on inappropriate materials in a few clicks from your recommended site? Is all material suitable for the age range of the students?
10.3. Be active in the ICT rooms and do not allow unsupervised use - tour the room, looking for signs of secrecy. This normally means some illicit activity going on.
10.4. Be aware of phrases being used like LMIRL (lets meet in real life) and ASL (age, sex, location), and also students using web-based chat facilities (which should be blocked anyway).
10.5. If an incident occurs, determine its severity rating:
  10.5.1 **Minor** (games, emailing, general web surfing, storing / viewing images in the “silly” category)
  10.5.2 **Major** (viewing / storing / printing legal pornography, distasteful material, cyberbullying)
  10.5.3 **Extreme** (viewing / storing / printing illegal pornography, scenes of extreme violence, rape, torture; criminal activity such as fraud, hacking)
10.6. Follow the appropriate action in the Classroom Management section of this document. Please note the importance of not allowing anyone to use the computer after an extreme incident - Police may wish to check the computer for evidence. DO NOT attempt to email, re-view or print the content, as this is an offence in itself.
10.7. Students use online communications facilities (email, instant messaging, texting, Twitter, blogs, YouTube, social networking sites) as part of their everyday lives.
10.8. You should ensure that you keep yourself safe by:
  10.8.1 Not divulging personal information online.
  10.8.2 Carefully managing social networking profiles.
  10.8.3 Using ONLY the facilities provided by the college to communicate with students and parents / guardians - DO NOT use personal email or other unauthorised methods.
  10.8.4 Considering your position as a professional, acting accordingly when online.

11. PROTECTION OF PERSONAL DATA

11.1. Students undergo an online safety lesson throughout the academic year, part of this covers protection of personal data.

11.2. Students are reminded about the importance of protecting personal data through discussions, posters or presentations.
11.3. The college's network filtering systems are configured to prevent student access to many of the sites which pose risks in terms of students posting personal data (these include Facebook, Instagram, etc.
11.4. Staff are required to adhere to the Mobile Phone Policy, which reminds staff that posting personal data on social networking sites or using instant messaging services may put them at professional and personal risk.

12. PUBLICITY PROTOCOLS (PHOTO / VIDEO OF STUDENTS)

UPLOADING IMAGES TO ONLINE PUBLIC SYSTEMS

12.1. Since the college's website is a publicly accessible source of information, information must be carefully checked to ensure it complies with online safety standards before publication (decency, non-identifiable students etc.
12.2. All materials for web-site publication are reviewed and approved by the ICT Operations Manager before being uploaded.
12.3. No materials should be added to any public-facing information source (including the website) without approval by the Executive Principal.

PHOTOGRAPHY / IMAGES / VIDEO

12.4. Students have their personal photographs taken for inclusion on the college's system. They are only to be used for this purpose and assessment walls, but must not be copied to shared areas, staff folders.
12.5. Students are at risk of identification if photographic images or videos are publicised along with name data. Care should be taken that no photographs / videos of students in combination with names are available on any public system.
12.6. It is preferable to publish group photos rather than individuals.
12.7. Care should also be taken to ensure that, in informal settings (e.g. college trips) the same standards of privacy, decency and non-identifiability are adhered to.
12.8. Before photographing / videoing any student in scenarios that may be publicised, referral should be made to the "opt out" list held in the college office.

13. INCIDENT MANAGEMENT

13.1. Incidents concerning breaches of ICT security or cyberbullying will fall into several classes of severity. A definition of these, and the actions to be taken, are given in the subsections below.
13.2. For all incidents of online safety an entry should be made on our incident recording system CPOMS with the relevant category selected (online safety) and a description of the event including the severity of the incident.

MINOR

13.3. Minor incidents (such as using personal devices during lessons) should result in the equipment (if mobile / personal) being confiscated and the matter referred to the form tutor, Executive Principal or Online Safety Coordinator.
13.4. The Online Safety Coordinator will evaluate the incident for evidence of modifications needed, and will liaise with the relevant managers as appropriate.
13.5. Form tutors will deal with the incident under the college's discipline procedures.

MODERATE

13.6. Moderate incidents (such as: viewing or saving pornography / other offensive material, Cyberbullying by texting, emailing, taking unsolicited photos / videos) should be referred to the Online Safety Coordinator through the normal channels.

13.7. The Executive Principal will evaluate the incident for evidence of modifications needed.

13.8. The Executive Principal will deal with the incident under the college's discipline procedures.

13.9. The IT Department will be responsible for providing evidence from the monitoring system.

EXTREME (ILLEGAL)

13.10. Extreme incidents (such as viewing or saving of illegal material or activity such as fraud, hacking) have criminal implications and the procedure below must be followed immediately such an incident is discovered:

UPON DISCOVERING THE INCIDENT

13.10.1 For extreme incidents the device should be isolated immediately from all users, screens turned off and the ICT Operations Manager and Online Safety Coordinator informed immediately.

13.10.2 The password for the user concerned will be changed to lock down the machine to preserve evidence.

13.10.3 The Online Safety Coordinator or Executive Principal will notify the appropriate agencies (LA / Police) for further advice.

13.10.4 It is VITAL that any ICT equipment used to commit an illegal act is not tampered with in any way, to preserve evidence.

13.10.5 The ICT Operations Manager will produce a report of the incident to the Executive Principal and liaise with staff on preserving evidence.

13.10.6 The Executive Principal will review impact of security breach on current Online Safety Policies.

13.10.7 The Executive Principal will liaise with the appropriate external authorities (Police / Internet Watch Foundation).

13.10.8 Throughout this procedure, reference should be made to the "Appendix " flowchart "Flowchart for Responding to Online Safety Incidents", from Becta publication Online Safety: Developing whole-college policies to support effective practice.

INCIDENTS IMPLICATING STAFF

13.11. Extreme incidents involving staff should be dealt with using the same protocols as students.

13.12. Generally the Executive Principal will take the lead in incidents minor / moderate severity, liaising with IT staff as necessary.

13.13. Once evidence has been collected, the college's Disciplinary Policy will be implemented.

ACCIDENTAL VIEWING OF INAPPROPRIATE CONTENT

13.14. In these instances, these points shall be followed:

STUDENTS

13.14.1 Students should report the incident to the nearest member of teaching staff.

13.14.2 The teacher should then notify ICT Operations Manager who should lock the appropriate machine and user account and use the monitoring software to provide evidence of the security breach.

13.14.3 The ICT Operations Manager will then notify the Online Safety Coordinator and Executive Principal and will review the security breach.

13.14.4 It is important that students feel supported and not criminalised in this instance, as doing so would dissuade them from reporting incidents of this type, with the consequent risks of further security breaches later on.

STAFF

13.14.5 Staff should follow the above procedure if they accidentally view inappropriate content from within college. The procedure will be the same, but the ICT Operations Manager will report the matter to the Executive Principal.

14. CREATING A SAFE ENVIRONMENT

14.1. The college will employ such technologies and policies as it sees fit to ensure the security of:

- 14.1.1 ICT infrastructure (e.g. virus protection);
- 14.1.2 Protection against data against loss / corruption (backup strategies);
- 14.1.3 Protection of personal data against unauthorised publicity, transfer and use;
- 14.1.4 Users against being exposed to inappropriate / damaging material.

FILTERING

14.2. The college employs 2 levels of internet filtering system:

- 14.2.1 ISP - filtering. This is provided as part of the online connectivity package. The system is configured by Link2ICT with some guidance from our ICT Operations Manager (Online Safety Coordinator). This provides limited customisable filtering.
- 14.2.2 College level filtering. Using the locally installed Impero monitoring system, staff can request the additional filtering of websites. The ICT Operations Manager manages and implements changes.

14.3. Staff can request for filtering to be applied to ensure the college adapts to the changing dangers posed by the internet. Conversely staff can also request the removal of certain filters to allow them to access resources they require for a lesson. In this case it is carefully considered by the Online Safety Coordinator in consultation with other members of the ICT team.

MONITORING

14.3.1 Students' and staffs' on line activities are monitored using the Impero system mentioned before. The monitoring software is used in active mode, with the detection of key words resulting in the immediate locking of students' screens. In the event of an incident being escalated, Impero can also be consulted later for evidence which is then supplied to the appropriate member of staff dealing with the incident. The monitoring system observes any activity on a user's screen and captures screen shots when specified words are detected on the screen. This can then be used as evidence in the event of an incident.

ANTI-VIRUS / FIREWALL

- 14.3.2 The college subscribes to the ISP provided Anti-Virus package. Automatic updates are set to operate on all end-user workstations, laptops and file servers.
- 14.3.3 Laptops are protected by the Anti-Virus package even when offline.
- 14.3.4 The college employs ISP firewalls and uses on-site firewalls where deemed most appropriate.
- 14.3.5 Patches and updates to programs and operating systems are regularly applied to ensure security integrity is maintained at all times.
- 14.3.6 The college does not allow any unauthorised devices to be connected to its networks or other ICT Infrastructure. Wireless networks are encrypted by default, with security details known only to the relevant technical staff.

SOCIAL NETWORKING OR MOBILE DEVICES

14.4. There are specific college policies for Social Networking and Mobile devices. A summary of key points follow below.

STUDENTS

14.4.1 Social networking sites and newsgroups will be blocked unless a specific use is approved.

14.4.2 Students are advised never to give out personal details of any kind which may identify them or their location. Examples would include their real name, address, mobile or landline phone numbers, college, IM address, e-mail address, names of friends, specific interests, clubs, etc.

14.4.3 There is to be no communication with staff members in or outside of college, unless there is circumstance where this is not possible, e.g. College Trip, Residential, and Emergency Situation.

14.4.4 Communication with other students outside of college hours should be monitored by parents. If a situation arises, such as bullying the Executive Principal can be contacted.

STAFF

14.4.5 Staff must never give out their personal details to students or parents.

14.4.6 Communication with other staff members outside of college via social networking is the responsibility of the end user. However, references to college and staff, students or parents, if of an offensive nature, may be subject to disciplinary investigation. Staff must be aware that anything posted online is in the public domain and may potentially be seen by anyone including non-intended recipients.

14.4.7 Communication with current students or parents, such as having them as a friend on social media, and messaging is not allowed by college. Uploading or sharing photos or videos with students in is also forbidden.

14.4.8 All staff must be aware that the posting of inappropriate pictures, videos and comments may be viewed as bringing the college into disrepute by association, which could be considered a disciplinary issue.

14.4.9 Staff must not share their contact details with current students or parents unless agreed by the College Principal. We also advise that staff do not share their contact details with past students or parents, as there is usually still a link to college through current students and parents.