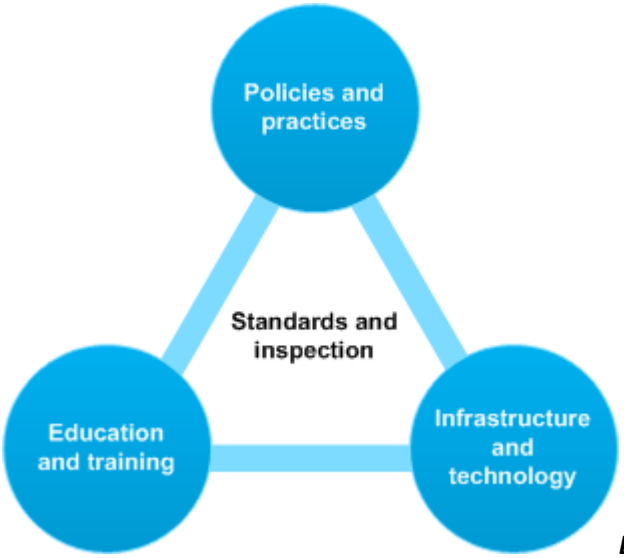
E-Safety Policy & Procedures

The internet itself will be a powerful resource in widening access to education, information and opportunity. So awareness of e-safety is now a necessity if we are to avoid a digital divide between those who are confident internet users and those who are not.

A framework for e-safety



Becta PIES model

Becta[1], formerly the agency promoting ICT in schools, developed a PIES model for approaching safeguarding within education. The PIES model encompasses:

- Policies and practices (P)
- Infrastructure and technology (I)
- Education and training (E)
- Standards and inspection (S)

[1] https://www.gov.uk/government/organisations/british-educational-communications-and-technology-agency

The model describes e-safety as a combination of policies, secure technology infrastructure, education and training, all underpinned by standards and inspection. This policy has adopted the good practice recommended by Becta as the underlying principles within this document, policy and procedures.

1.0 Scope of the Policy

1.1 This policy applies to all users interacting with ICOM's digital systems, including any online or blended learning environments. It addresses data protection, acceptable use, and online safety for both staff and students across virtual platforms, aligning with the MFHEA guidelines on Domain 4: Resources, which emphasize secure infrastructure and data protection..

1.2 ICOM withholds the right to instigate disciplinary procedures for inappropriate use / behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of college, but are linked to ICOM.

1.3 ICOM will deal with such incidents within this policy and associated use / behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of college.

2.0 Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the college.

2.1 The ICOM SMT

- SMT has a duty of care for ensuring the safety (including e-safety) of members of the college community, although the day to day responsibility for e-safety will be delegated to the E-Safety Officer.
- SMT and another designated member of the senior management team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff
- SMT is responsible for ensuring that the E-Safety Officer and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- SMT will ensure that there is a system in place to allow for monitoring and support of those who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

- SMT must ensure regular cyclical reviews of e-safety policies in the context of online and blended learning programmes, as specified by MFHEA guidelines (Domain 3). This includes ensuring that adequate resources and budget are allocated to digital security and e-safety measures.
- SMT and senior management team are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by receiving regular information about e-safety incidents and monitoring reports.
- SMT will ensure training and policies reflect the changing landscape of online learning, with a focus on preventing and responding to cyberbullying, hacking, and data breaches that may arise in online settings

2.2 E-Safety Officer (**stefano.ceriani@nexto.eu**)

The E-safety Officer will:

- Lead e-safety
- Take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the e-safety policy
- Ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provide training and advice for staff
- Update on the latest in online teaching environments and threats to e-learning infrastructure, ensuring the application of MFHEA's Domain 6: Assessment and Integrity requirements .
- Liaise with the Local Authority / relevant body
- Liaise with technical staff
- Receive reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- Maintain digital records of all e-safety incidents that occur online, with periodic reports submitted to senior management.
- Meet regularly with Designated Safeguarding Lead and f IT Services to discuss current issues and review incident logs
- Attend relevant meetings
- Report regularly to the senior management team
- Where safeguarding concerns exist they co-ordinate with external agencies
- Ensure that students complete, as part of their induction programme, activities designed to promote E-safety.
- Ensure that the tutorial programme includes activities to promote and remind students of e-safety and that they complete an on-line module designed to reinforce and confirm their understanding via a test.

2.3 Head of IT Services

The Head of IT Services is responsible for ensuring that:

- The colleges technical infrastructure is secure and is not open to misuse or malicious attack
- The college meets required e-safety technical requirements
- Users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- They keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- The use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Officer for investigation / action / sanction
- Monitoring software / systems are implemented and updated.

2.4 Designated Safeguarding Lead

The Designated Safeguarding Lead is responsible for ensuring that:

- They share with the E-safety Officer, issues or concerns disclosed during safeguarding meetings with students.

2.5 Teaching, Safeguarding and Support Staff

Teaching, Safeguarding and Support staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters
- They have read, understood and signed the Staff Acceptable Use Policy
- They report any suspected misuse or problem to the E-safety Officer
- All digital communications with students / parents / carers should be on a professional level and only carried out using official ICOM systems
- E-safety issues are embedded in all aspects of the curriculum and other activities

- Students understand and follow the e-safety and acceptable use policies
- They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other activities and implement current policies with regard to these devices
- In lessons, where internet use is pre-planned, students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

2.6 Partners / Employers etc…

Users who access ICOM systems will be expected to sign an Acceptable Use Agreement before being provided with access to ICOM systems.

2.7 Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of ICOM's e-safety provision. Students need the help and support of the college to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- Key e-safety messages should be reinforced as part of a planned programme tutorial and other pastoral activities
- Students should be taught in lessons to be critically aware of the materials / content they access on-line and be guided 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
- Students should be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside ICOM
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites they visit

3.0 Education & Training

3.1 It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly
- All staff will receive updated training focused on e-safety in online learning environments, including data privacy, the appropriate use of digital tools, and responding to online incidents in compliance with MFHEA's Domain 2(Staffing Profile and Professional Development).
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the college e-safety policy and Acceptable Use Agreements
- The E-Safety Officer will receive regular updates through attendance at external training events
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings
- The E-Safety Officer will provide advice / guidance / training to individuals as required.
- Staff must understand their roles in safeguarding students' data and be trained to respond to incidents of misuse of virtual learning environments (VLE), cyber-attacks, or breaches in the integrity of digital assessments

4.0 Technical – infrastructure / equipment, filtering and monitoring

4.1 It is the responsibility of the Head of IT Services to carry out all the e-safety measures.

4.2 The Head of IT Services will be responsible for ensuring that the college IT infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- Technical systems will be managed in ways that ensure that ICOM meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of the college technical systems

- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to technical systems and devices
- All users will be provided with a username and secure password. The Head of IT Services will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be requested to change their password every six months
- ICOM will ensure that its technical infrastructure supports safe online learning environments, ensuring protection against malware, unauthorized access, and breaches of data security. This aligns with Domain 4: Resources of the MFHEA guidelines .
- The "master / administrator" passwords for the IT infrastructure must also be made available to the President
- The Head of IT Services is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users and content lists are regularly updated and internet use is logged and regularly monitored
- ICOM technical staff regularly monitor and record the activity of users on the college IT systems and users are made aware of this in the Acceptable Use Agreement
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the IT Help Desk
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of college systems and data. These are tested regularly. The college infrastructure and individual workstations are protected by up to date virus software.
- An agreed protocol is in place for the provision of temporary access of "guests"
- An agreed protocol is in place that allows staff to download executable files and installing programmes on college devices
- An agreed protocol is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on ICOM devices. Personal data cannot be sent over the internet or taken off site unless safely encrypted or otherwise secured.
- Mandatory training for staff to effectively manage e-safety in digital and blended learning contexts.
- Regular audits of e-learning platforms to ensure security and compliance.
- Implementation of secure authentication methods for all digital learning platforms.

5.0 Bring Your Own Device (BYOD)

Students will receive guidance during induction on levels of secure access, data protection measures, and monitoring use to ensure compliance with college e-safety and acceptable use policies. Students using personal devices for learning must adhere to institution-defined BYOD guidelines, ensuring compliance with e-safety standards.

- ICOM has a set of clear expectations and responsibilities for all users
- ICOM adheres to the Data Protection Act principles
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the college's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Mandatory training is undertaken for all staff
- Students receive training and guidance on the use of personal devices
- Regular audits and monitoring of usage will take place to ensure compliance
- Students and staff must be made aware that their usage while on college premises is monitored to ensure compliance.
- Risks and safe practices for participating in online learning.
- Guidelines on the ethical use of generative AI and other digital tools.
- Information about reporting inappropriate behaviour or breaches of online safety protocols.

6.0 Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

ICOM will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites
- Staff are allowed to take digital / video images to support educational aims, but must follow college policies concerning the sharing, distribution and publication of those images
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere, that include students will be selected carefully and will comply with good practice guidance on the use of such images
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of students are published on the college website
- Students' work can only be published with the permission of the student and parents or carers.

7.0 Data Protection and GDPR

7.1 Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure storage of data in cloud systems that comply with international data protection standards.
- Prohibition of data sharing without explicit consent and appropriate safeguards

7.2 ICOM will ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing"
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood procedures and routines for the deletion and disposal of data
- There is a procedure for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.
- All personal data stored or transmitted during online learning must be encrypted, ensuring compliance with GDPR and MFHEA' s guidelines on data security

7.3 Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- Transfer data using encryption and secure password protected devices.

7.4 When personal data is stored on any portable computer system, memory stick or any other removable media:

- The data must be encrypted and password protected

- The device must be password protected (memory sticks / cards and other mobile devices cannot be password protected)
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device, in line with college policy (below), once it has been transferred or its use is complete

7.5 Incident Reporting and Follow-Up

Real-time incident reporting tools must be integrated into e-learning platforms. Staff are required to document and escalate e-safety breaches immediately using a centralized reporting system managed by the E-Safety Officer

8.0 Communications

8.1 A wide range of rapidly developing communications technologies has the potential to enhance learning. General principles are outlined below.

8.2 When using communication technologies ICOM considers the following as good practice:

- The college email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the college email service to communicate with others
- Any digital communication must be professional, using official ICOM channels. Unauthorized use of social media for academic communication is strictly prohibited
- Users must immediately report the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- Any digital communication between staff and students must be professional in tone and content. These communications may only take place on official systems. Personal email addresses, text messaging or social media must not be used for these communications
- Staff should not give out their personal home or mobile telephone number to students.
- Students should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies

- Personal information should not be posted on the college website and only official email addresses should be used to identify members of staff.

8.3 Staff and students must use AI tools responsibly, ensuring that their use supports, rather than undermines, ethical learning practices. Any coursework that incorporates AI assistance must include a statement of AI usage, as per the Academic Integrity Policy.

9.0 Social Media - Protecting Professional Identity

9.1 General principles are outlined below.

9.2 ICOM provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the college through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

9.3 Staff should ensure that:

- No reference should be made in social media to students or staff
- They do not engage in online discussion on personal matters relating to members of the college community
- Personal opinions should not be attributed to ICOM

10.0 Unsuitable / Inappropriate Activities

10.1 ICOM considers that the activities referred to in the following section would be inappropriate in a college context and that users, as defined below, should not engage in these activities on site or outside college using college property / networks. The college policy restricts usage as follows:

10.2 Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- Child sexual abuse images
- Grooming, incitement, arrangement or facilitation of sexual acts against
- Youth produced sexual imagery (formally known as sexting)

- Criminally racist material in UK – to stir up religious hatred
- Pornography
- Promotion of any kind of discrimination
- Threatening behaviour, including promotion of physical violence or mental harm
- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of ICOM's or brings the college into disrepute
- Using college systems to run a private business
- Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the college
- Infringing copyright
- Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Unfair usage (downloading / uploading large files that hinders others in their use of the internet)
- On-line gaming other than for educational purposes
- On-line gambling
- On-line shopping / commerce
- File sharing
- Use of social media
- Use of messaging apps
- Use of video broadcasting
- Students and staff must be made aware that their usage while on college premises is monitored to ensure compliance.

11.0 Responding to incidents of misuse

11.1 This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

11.2 Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to E-safety Officer

11.3 Other Incidents

It is hoped that all members of the college community will be responsible users of digital technologies. However, there may be times when infringements of the policy

could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported. Complete E-safety incident log form (Appendix 1)
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded.
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the investigation form. For cases where pornography is involved, do not print the image. Instead, write an account of the photograph.
- Once this has been completed and fully investigated the E-safety Officer will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement of an external agency
    - Police involvement and/or action
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
- Incidents of 'grooming' behaviour
- The sending of obscene materials to a child
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

11.4 It is important that all of the above steps are taken as they will provide an evidence trail for the College and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

12.0 College Actions & Sanctions

12.1 Students

The following points represent general principles in deciding if any actions or sanctions will be taken. In all cases, refer to the student disciplinary policy in the first instance.

- Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)
- Unauthorised use of non-educational sites during lessons
- Unauthorised use of mobile phone / digital camera / other mobile device
- Unauthorised use of social media / messaging apps / personal email
- Unauthorised downloading or uploading of files
- Allowing others to access the college network by sharing username and passwords
- Attempting to access or accessing the college network, using another student's account
- Attempting to access or accessing the college network, using the account of a member of staff
- Corrupting or destroying the data of other users
- Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature
- Continued infringements of the above, following previous warnings or sanctions
- Actions which could bring the college into disrepute or breach the integrity of the ethos of ICOM
- Using proxy sites or other means to subvert the college's filtering system
- Accidentally accessing offensive or pornographic material and failing to report the incident
- Deliberately accessing or trying to access offensive or pornographic material
- Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.

12.2 Staff

The following points represent general principles in deciding if any actions or sanctions will be taken. In all cases, refer to the staff disciplinary policy in the first instance.

- Deliberately accessing or trying to access material that could be considered inappropriate
- Inappropriate personal use of the internet / social media / personal email
- Unauthorised downloading or uploading of files
- Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account
- Careless use of personal data e.g. holding or transferring data in an insecure manner
- Deliberate actions to breach data protection or network security rules
- Corrupting or destroying the data of other users or causing deliberate damage to hardware or software
- Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature
- Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students
- Actions which could compromise the staff member's professional standing
- Actions which could bring the college into disrepute or breach the integrity of the ethos of the college
- Using proxy sites or other means to subvert the college's filtering system
- Accidentally accessing offensive or pornographic material and failing to report the incident
- Deliberately accessing or trying to access offensive or pornographic material
- Breaching copyright or licensing regulations
- Continued infringements of the above, following previous warnings or sanctions

13.0 Development / Monitoring / Review of this Policy

13.1 This E-Safety Policy has been developed by:

- Designated Safeguarding Lead
- E-safety Officer
- Head of IT Services

13.2 The implementation of this E-Safety Policy will be monitored by the following:

- Designated Safeguarding Lead
- E-safety Officer
- Head of IT Services

13.3 The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.

13.4 The SMT will receive regular reports on the implementation of the E-Safety Policy (which will include anonymous details of e-safety incidents).

13.5 Review Cycle: This policy will undergo an annual review to remain responsive to evolving technologies and threats. Reviews will incorporate:

.• Results from learning analytics and incident logs

- Monitoring logs of internet activity (including sites visited)
- Feedback from staff, students, and external stakeholders

13.6 Professional Development

The institution will provide ongoing training for staff in:

- Data protection and cybersecurity.
- E-safety in online and blended learning environments.
- Addressing emerging threats and tools, such as the misuse of AI technologies.

14 **Implementation Plan (Section 14)**

Monitoring and Evaluation The E-Safety Officer, in collaboration with the IT Department, will:

- Conduct regularaudits of digital systems to ensure adherence to policy standards.
- Provide regular reports to the Senior Management Team on e-safety incidents and trends.

Stakeholder Communication Staff and students will receive regular updates on e-safety protocols through institutional communication channels and training sessions.

Appendix 1

ICOM E-safety incident log

Name and contact details of person reporting incident	
Name and contact details of person investigating incident	

Date and time of incident	
Details of incident	
Where did the incident occur	
Date and time of reporting incident	
Names and contact details of those involved	
Classification of type of incident	☐ bullying or harassment ☐ online bullying or harassment (cyberbullying) ☐ sexting (self-taken indecent imagery) ☐ deliberately bypassing security or access ☐ hacking or virus propagation ☐ racist, sexist, homophobic religious hate material ☐ terrorist material ☐ other (please specify) _____
Details of any attachments / evidence	
Did the incident involve material being	☐ created ☐ viewed ☐ printed ☐ shown to other ☐ transmitted to others ☐ distributed
Could this incident be considered as	☐ harassment ☐ grooming ☐ cyberbullying ☐ sexting (self-taken indecent imagery) ☐ breach of AUP ☐ other (please specify)

Action taken	**staff** incident reported to Head of College /senior manager advice sought from children's social care incident reported to police incident reported to CEOP incident reported to Internet Watch Foundation incident reported to IT disciplinary action to be taken e-safety policy to be reviewed/amended
Action taken	**student** incident reported to member of staff (specify) incident reported to social networking site incident reported to IT student's parents informed disciplinary action taken student debriefed e-safety policy to be reviewed/amended
Outcome of incident/ investigation	
Police/CEOP	
Organisation	
Individual (staff member/student)	
Other (HR/legal etc)	
Learning from the case	

Date and people involved in reviewing the case and making recommendations	
Key learning point 1	
Key learning point 2	
Key learning point 3	
Recommendations and timescales to implement	
Recommendation 1	
Recommendation 2	
Recommendation 3	