Academy of Science Technology and Management

E-Safety Policy and Procedures

Originator:	Chief Operating Officer
Approved by:	SMT
Date Approved:	June 2020
Review Interval:	3 Years
Review Date:	June 2023

Introduction

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.

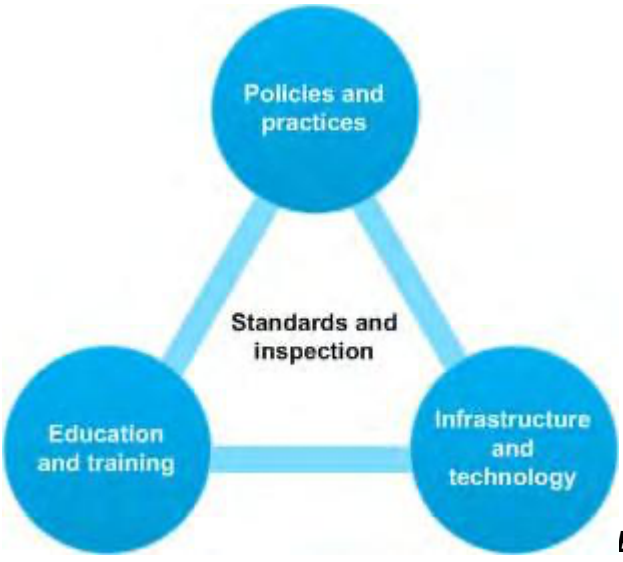
JULIA TAYLOR, FOREWORD TO NIACE E - SAFETY DIGITAL LEARNING GUIDES

E-Safety is about safe and responsible practice with technology and the sensible management of risks presented by the digital world.

There is a need to educate ourselves and others about the benefits and risks of using technology and to provide awareness, skills and safeguards to enable users to take responsibility for their own and others' online experience.

The JISC definition quoted above can be used as a starting point for learning about a vital part of ***living in a digital society***. Moreover, empowering people to take responsibility and be able to safeguard themselves and their personal information is something that needs to be developed and maintained throughout their life.

A framework for e-safety



Becta PIES model

Becta, 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)

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.

This policy is derived from a number of other college policies and repeated here for clarity including: Safeguarding, Student Disciplinary, Bullying & Harassment, ICT, Social Media, Data Protection. For specific information refer to the original policy.

1.0 Scope of the Policy

This policy applies to all members of Academy of Science Technology and Management, including staff, students, volunteers, parents / carers and visitors, who have access to or use the College's IT infrastructure.

1.1 Academy of Science Technology and Management 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 Academy of Science Technology and Management.

1.2 Academy of Science Technology and Management 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 Principal, Senior Management Team & Governing Body

- The COO / Directors has a duty of care for ensuring the safety (including e-safety) of members of the college community.
- The COO / Directors 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
- The COO / Directors 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.
- The COO / Directors 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.

- The COO / Directors 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.

2.2 E-Safety Officer (The COO)

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
- 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
- Attend relevant meetings
- Report regularly to the senior management team.

2.3 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 Academy of Science Technology and Management 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.

2.4 Parents / Carers

Parents / Carers play a crucial role in ensuring that their child understands the need to use the internet / mobile devices in an appropriate way. The college will take every opportunity to help parents understand these issues through, newsletters, letters, website and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the college in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at college events
- Their child's personal devices in the college.

2.5 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 Academy of Science Technology and Management'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 must be reinforced as part of a planned programme tutorial and other pastoral activities
- Students must 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 must be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students will be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside Academy of Science Technology and Management
- Staff must 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 must 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 must be vigilant in monitoring the content of the websites they visit
- It is accepted that, from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs or discrimination) that would normally result in internet searches being blocked. In such a situation, staff must request that IT Services temporarily remove those sites from the filtered list for the period of study. Any request to do so should be placed with the IT Helpdesk, with clear reasons for the need.

2.6 Parents / Carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the student's on-line behaviours. Parents may underestimate how often students come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

Academy of Science Technology and Management will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site, etc…
- Parents / Carers evenings / sessions
- High profile events / campaigns
- Education & Training

2.7 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 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.

2.8 Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by colleges of users bringing in their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include: levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring. This list is not exhaustive and a BYOD policy should be in place and reference made to it within all relevant policies.

- Academy of Science Technology and Management has a set of clear expectations and responsibilities for all users
- Academy of Science Technology and Management 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 must 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.

3 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. Academy of Science Technology and Management 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 must 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
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the college into disrepute
- 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 must be selected carefully and comply with good practice guidance on the use of such images
- Students' full names should not be used anywhere on a website or blog, particularly in association with photographs unless consent is obtained and comply with good practice guidance on use of such images
- Written permission from students / parents or carers must 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.

4 Data Protection

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
- Only transferred to others with adequate protection.

4.1 Academy of Science Technology and Management 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”
- It has a Data Protection Policy
- 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 policies and routines for the deletion and disposal of data
- There is a policy 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.

4.2 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.
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

5 Communications

5.1 A wide range of rapidly developing communications technologies has the potential to enhance learning. Refer to the Academy of Science Technology and Management Acceptable Use of Social Media policy for further advice. General principles are outlined below.

5.2 When using communication technologies Academy of Science Technology and Management 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 must therefore use only the college email service to communicate with others
- 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 must not give out their personal home or mobile telephone number to students. The college provides mobile phones for educational visits and this number should be given to students / parents.
- Students will 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 must not be posted on the college website and only official email addresses will be used to identify members of staff.

6 Social Media - Protecting Professional Identity

6.1 Please refer to The Acceptable Use of Social Media Policy. General principles are outlined below.

6.2 Academy of Science Technology and Management 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

6.3 Staff must ensure that:

- No reference will 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 must not be attributed to Academy of Science Technology and Management

7 Unsuitable / Inappropriate Activities

7.1 Academy of Science Technology and Management considers that the activities referred to in the following section would be inappropriate in a college context and that users, as defined below, must not engage in these activities on site or outside college using college property / networks. The college policy restricts usage as follows:

7.2 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 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 Academy of Science Technology and Management'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 (e.g. 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.

8 Responding to incidents of misuse

8.1 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 (see “User Actions” above).

8.2 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

8.3 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 must 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.
- 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 must 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 must 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.

8.4 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.

9 College Actions & Sanctions:

9.1 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 Academy of Science Technology and Management
- 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.

9.2 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 the college network by sharing username and passwords or attempting to access or accessing the college 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

10 Development / Monitoring / Review of this Policy

10.1 This E-Safety Policy has been developed by:

Chief Operating Officer and Board of Directors

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

- COO
- Board of Directors

10.3 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.