Engineering UTC Northern Lincolnshire

E-Safety Policy

March 2026

Approved by the ENLUTC Governing Body
March 2026

Document Control Table

Document Title:	**E Safety Policy**
Author (Name & Job Title):	**Anesta McCullagh, Principal**
Acknowledgement:	
Version Number:	**V4 November 2020**
Date Approved:	**Approved March 2026**
Approved By:	**Approved by UTC Board**
Date of Review:	**March 2027**

Document History

Version	Date	Author	Note of revisions
2	30 Sept 2018	As above	Amendments included: dates/name changes additional elements from Network Manager
3	November 19	J. Emmett	2,5 forward reports to DSL & SLT
4	13/10/2023	C.Reet	2.8 Change to wording as students do not sign a paper ICT policy.

1. Policy Document

1.1 This policy applies to all members of the college community (including staff, students, volunteers, parents/carers and visitors) who have access to and are users of the college's ICT systems, both in and out of the college.

1.2 The Principal is empowered, to such extent as is reasonable, to regulate the behaviour of students when they are off the college site and staff are empowered to impose disciplinary penalties for inappropriate behaviour.

1 This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of college, but is still linked to membership of the college. The college will deal with such incidents within this policy and associated behaviour and inappropriate e-safety behaviour that take place out of college. Parents/carers may be informed of concerns via telephone or letter.

2 Roles and Responsibilities

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

2.2 Governing Body

Governors are responsible for the approval of the e-safety Policy and for reviewing the effectiveness of the policy.

2.3 Principal and Senior Leaders

- The Principal is responsible for ensuring the safety (including e-safety) of members of the college community.
- The Principal and senior leaders are responsible for ensuring that relevant staff receive suitable training and development to enable them carry out their e-safety roles and to train other colleagues, as relevant.
- The principal and senior leaders will ensure that there is a system in place to allow for the monitoring and support of those in college who carry out the internal e-safety monitoring role. This is to provide a safety net and also to support those colleagues who take on important monitoring roles.
- The college's senior leadership team (SLT) will receive information regarding any e-safety incidents which will be logged and reviewed during SLT meetings.

2.3 Member of SLT with responsibility for e-safety

- Take day to day responsibility for e-safety issues and oversee the sanctions for breaches of rules relating to e-safety.
- Ensure that all staff are aware of the procedures that need to be followed in the event of an esafety incident taking place.
- Provide training and advice to staff.
- Liaise with the Local Authority Designated Officer (LADO) or Police as appropriate.
- Liaise with the college's ICT technical staff.
- Receive reports of e-safety incidents as part of behaviour monitoring.
- Provide information to the Governing Body as appropriate.

2.5 ICT Staff

- Ensure that the college and its ICT infrastructure is secure and is not open to misuse or malicious attack and that all aspects of the college's ICT systems are secure, in line with its guidance and policies.
- Manage, run, and forward reports of e-safety incidents to the DSL and necessary members of SLT.

2.6 Teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of current college e-safety policy and practices;
- They have read and understood the appropriate ICT agreements;
- They report any suspected misuse or problem to a member of SLT;
- Digital communications with students are only on a professional level and carried out using official college systems;
- It is understood that social media can play an important part in communication between the college and students, parents/carers; however, there is also a need to ensure it is used in an appropriate and safe way. Before any member of staff set up a resource such as a student blog space, they must seek permission from the Principal and they should ensure that appropriate steps are taken to make such social media 'private' so that only people they approve can access it. The member of staff will then be responsible for the posts made on the site and for moderating the content from other users/contributors;
- E-safety issues are embedded in all aspects of the curriculum and other college activities;
- Students understand and follow the college's e-safety and Acceptable Use Policy;
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor ICT activity in lessons, extra-curricular and extended college activities;
- They are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current best practice 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 to deal with any unsuitable material that is found in Internet searches.

2.7 Designated Safe-guarding Person (and Deputy)

Should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate on-line contact with adults/strangers
- Potential or actual incidents of grooming
- Cyber-bullying

2.8 Students

- Are responsible for using the college's ICT systems in accordance with college policy, which they are agreeing to follow by logging into the college systems.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand college policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand the college's policies on the taking/use of images and on cyber-bullying.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of college and realise that the college's E-Safety Policy covers their actions out of the college, if related to their membership of the college.

2.9 Parents/Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the Internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The college will therefore take every opportunity to help parents understand these issues through college communications and the website.

Parents and carers will be responsible for:

- Endorsing the college policy
- Accessing the college website in accordance with the relevant Acceptable User Policy.

3. Education and Training

3.1 E-Safety education will be provided in the following ways:

- A planned e-safety programme will be provided as part of the ICT programme.
- Key e-safety messages will be reinforced as part of a planned programme of assemblies/tutorials and within the PSHE curriculum.
- Students will be taught whenever an opportunity occurs to be critically aware of the material/content they access on-line and be guided to validate the accuracy of information.
- Students will be encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside the college.
- Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- Staff will act as good role models in their use of ICT, the Internet and mobile devices.

3.2 Education and Training – Staff

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:

E-safety training for all staff is included as part of Level 1 child safeguarding training.

All new staff will receive e-safety training as part of their induction programme, ensuring they understand the E-safety Policy and Acceptable Use Policy.

3.3 Training – Governors

The college's online child safeguarding training covers the relevant elements of e-safety training. Governors are required to undertake the college's online training on their appointment.

4. Infrastructure, equipment, filtering and monitoring

The college will be responsible for ensuring that its infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. All users will have clearly defined access rights to college's ICT systems.

- All users will be provided with a username and password by ICT support who will keep an up to date record of users and their usernames. Users will be required to change their password regularly
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

-
- In the event of the IT Staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Principal.
- Requests from staff for sites to be removed from the filtered list will be considered by the IT Staff.
- ICT technical staff regularly monitor and record the activity of users on the college's ICT systems and users are made aware of this in the Acceptable Use Policy.
- Remote management tools are used by staff to control workstations and view users' activity
- An appropriate system is in place for users to report any actual / potential e-safety incident to SLT.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the college's systems and data.
- Guest users may be granted a temporary log in or guest account if agreed by the IT Staff
- Personal use of the college's ICT systems should be limited to what may be deemed reasonable. The services are provided predominantly for education purposes.
- Neither staff nor students should install programmes or other software on workstations, portable devices or servers, without the prior express, written permission of the college's IT Staff
- The college's ICT infrastructure and individual workstations are protected by up to date virus software.
- Personal data (as defined by the Data Protection Act) cannot be sent over the Internet or taken off the college site unless safely encrypted or otherwise secured by password or other means – please refer to the college's Data Handling Policy for further information.
- Where staff have email accounts and other college data on their phone or other mobile device, they must ensure that the device is locked with a password.

5. Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

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, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- Students should be taught in all lessons to be critically aware of the materials / content they access online 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.

6. Use of digital and video images -Photographic, Video

6.1 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 sharing images and with posting digital images on the Internet. Those images may remain available on the Internet forever and may cause harm or embarrassment to individuals in the short or longer term.

6.2 There are many reported incidents of employers carrying out Internet searches for information about potential and existing employees. The college 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. Those images should only be taken on college equipment, the personal equipment of staff should not be used for such purposes. They should also only be stored on the college's network and not on any personal device.
- 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 will be selected carefully and will comply with good practice guidance on the use of such images.
  Written permission from parents or carers will be obtained before photographs of students are published on the college website (this is covered as part of the agreement signed by parents or carers).
- Be aware that downloading, copying or printing images from the Internet may also breach copyright laws.

7. Data Protection

•

7.1 Personal data (as defined by the Data Protection Act - GDPR) 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.

7.2 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/ secure password protected devices or ensure that the file is password protected.

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

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected, if this is the case then each individual file will need to be password protected)
- the data must be securely deleted from the device, once it is no longer required

8. Communications

8.1 A wide range of rapidly developing communications technologies has the potential to enhance learning.

- Users need to be aware that email communications may be monitored.
- Users must immediately report, to a member of SLT, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students or parents / carers (email , eportal etc) must be professional in tone and content. These communications may only take place on official (monitored) college systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.

- Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the college website and only official email addresses should be used to identify members of staff.

9. Unsuitable / inappropriate activities

9.1 Some Internet activity e.g. accessing child abuse images or distributing racist material is illegal and is obviously be banned from the college and all other ICT systems. Other activities e.g. Cyber-bullying, use of electronic communications to radicalise children or others, is banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a college context, either because of the age of the users or the nature of those activities.

10. Responding to incidents of misuse

10.1 It is hoped that all members of the college community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

10.2 If any apparent or actual misuse appears to involve illegal activity i.e. child sexual abuse images, adult material which potentially breaches the Obscene Publications Act, criminally racist material, other criminal conduct, activity or materials and/or radicalisation of others, the Principal must be informed immediately. The Principal and any other relevant members of the SLT must inform the relevant authorities immediately of any concerns/ infringements. The steps taken must all be reported to the Chair of Governors.