Suffolk New College

E-Safety Policy

Policy Title:	E-Safety Policy
Issue Date:	July 2019
Author(s):	Director of Quality, Teacher Development & Student Progress Director of Student Services, Safeguarding & Support
Approved by:	SMT
Last Review date:	01/12/2025
Date of Equality Assessments:	01/12/2025
Review date:	01/12/2026
Related Policies & Procedures:	IT Acceptable Use Policy Safeguarding & Child Protection Policy Learner Disciplinary Policy Use of AI Policy IT Cyber Security Policy

Equality Impact Assessment Tool

E-Safety Policy

		Yes/No	Comments
1	**Does the policy/guidance affect one group less or more favourably than another on the basis of:**		
	Race or ethnicity	No	
	Disability	No	
	Gender	No	
	Religion or belief	No	
	Sexual orientation	No	
	Age	No	
	Marriage and Civil Partnership	No	
	Maternity and Pregnancy	No	
	Gender Reassignment	No	
2	**Is there any evidence that some groups are affected differently?**	No	
3	**If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?**	N/A	
4	**Is the impact of the policy/guidance likely to be negative?**	No	
5	**If so, can the impact be avoided?**	N/A	
6	**What alternatives are there to achieving the policy/guidance without the impact?**	N/A	
7	**Can we reduce the impact by taking different action?**	N/A	

disability confident
COMMITTED

SUFFOLK NEW COLLEGE

E-Safety Policy

1 INTRODUCTION

The purpose of the e-Safety Policy is to safeguard and promote the welfare of all members of the Suffolk New College community when using technologies both on site and at home. Online safety is an essential part of safeguarding and the College has a duty to ensure that all learners and staff are protected from potential harm when using mobile technology and social media. This same duty applies in instances of potential risk of harm or abuse caused by AI-generated content.

Mobile devices, such as computers, tablets, mobile phones, smart watches and games consoles and social media, are an important part of everyday life, which present positive and exciting opportunities, as well as challenges and risks. Suffolk New College will empower our learners to acquire the knowledge needed to use the mobile technology, social media and generative-AI in a safe, considered and respectful way, develop high levels of digital skills and develop their resilience so they can manage and respond to online risks, as well as prepare for future learning opportunities and employment.

This Policy has been developed in line with Government publications, notably:

- Keeping Children Safe in Education, KCSiE (2025)
- The Prevent Duty (2024)

In addition to the UK Council for Internet Safety's 'Sharing nudes and semi-nudes: how to respond to an incident' (2024).

In the event of the College needing to flip to full-time remote learning, we will adhere to statutory guidance as appropriate at that time, recognising that the experience of the COVID-19 pandemic has enabled us to be fully prepared for such eventuality.

2 SCOPE OF THE POLICY

The policy applies to all users; learners, staff and all members of the College community who have access to the College IT systems, both on the premises and remotely, and to those using their personal devices on the premises. The E-Safety Policy applies to all use of the internet and electronic communication devices such as e-mail, mobile phones, games consoles and social networking sites and Apps, including generative-AI platforms.

The policy refers primarily to use of technology for College related teaching and learning activity either on College premises – utilising the College's WIFI network -

or remotely and for College related educational work or through communication channels that specifically link to the College. However, this policy may also apply to conduct by learners or staff, such as incidents of cyber-bullying or other e-safety incidents, including sexual harassment on-line, consensual and non-consensual sharing of nude and semi-nude images** and videos, including revenge porn and sextortion; technology assisted harmful sexual behaviour that may cause harm to self or others including generative-AI, which take place out of College, but is linked to membership of the College and which impacts on the College community, individuals or reputation.

**The types of incidents which this covers are:

- a person under the age of 18 creates and shares nudes and semi-nudes of themselves with a peer under the age of 18
- a person under the age of 18 shares nudes and semi-nudes created by another person under the age of 18 with a peer under the age of 18
- a person under the age of 18 is in possession of nudes and semi-nudes created by another person under the age of 18

This advice does not cover:

- the sharing of nudes and semi-nudes of under 18s by adults (18 and over) as this constitutes child sexual abuse and education settings should always inform their local police force as a matter of urgency[footnote 3]
- children and young people under the age of 18 sharing adult pornography or exchanging sexual texts which do not contain images.

The College has a separate Use of AI Policy which is reviewed every 3 months on account of the exponential growth and pace with which AI technology is developing. The policy should be read in conjunction with this one.

3 RISKS

There are a wide range of risks and dangers that face young people which could impact on the safety or security of learners. To help categorise the risks, this Policy adopts the categories identified in Keeping Children Safe in Education (2025). Whilst the breadth of issues classified within online safety is considerable and ever-evolving, these can be categorised into four areas of risk:

Content *	Contact	Conduct	Commerce
Access to illegal, harmful or inappropriate images or other content eg harmful challenges and on-line hoaxes	The risk of being subject to grooming by those with whom they make contact on the internet;	Unauthorised access to / loss of / sharing of personal information	On-line gambling
Access to unsuitable video / internet games/ gambling sites	Inappropriate communication / contact with others, including strangers, for example through social networking sites	Making, sending and receiving explicit images (eg consensual and non-consensual sharing of nudes and semi-nudes and or pornography)	Inappropriate advertising
An inability to evaluate the quality, accuracy and relevance of information on the internet		Cyber-bullying	Phishing and/or financial scams *If you feel your learners or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).*
Plagiarism and copyright infringement		Race hatred	
		Terrorism extremism	
		Financial abuse	
		Illegal downloading of music or video files	
The potential for use which may impact	The potential for use which may impact on the	The potential for use which may impact on the	

on the social and emotional development and learning of the young person, increasing their vulnerability through the sharing of personal data which may allow: - Access or exposure to illegal / inappropriate materials	social and emotional development and learning of the young person, increasing their vulnerability through the sharing of personal data which may allow: - inappropriate on-line contact with adults / strangers - potential or actual incidents of grooming - cyber-bullying	social and emotional development and learning of the young person, increasing their vulnerability through the sharing of personal data which may allow: - cyber-bullying - Inappropriate portrayal of self to others

* ‘Content’ risks of harm now also include misinformation and disinformation (including fake news), following the update to Keeping Children Safe in Education (2025). In the absence of nationally agreed definitions, those adopted by the College are: ‘Misinformation’ can be defined as ‘*fake news that is created and spread by mistake’* and ‘Disinformation’ as ‘*the deliberate creation and spread of false or misleading content’*.

AI Safety
The College recognises that AI-generated harms and abuse are ever-evolving and at the time of writing staff understand that such harms can include (but not limited to):

• Chatbot ‘companion’ app services
• AI voice-cloning scams
• Deep-fakes – including fake nudes (where the majority are created to harm, abuse, de-fraud, bribe, sextort, humiliate and shame)
• De-clothing / nudifying apps – widely available and increasingly promoted to young people via social media (where a significant proportion of victims are female).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, to build learners’ resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks. This is built into the College’s Professional Development (PD) safeguarding curriculum.

4 ROLES AND RESPONSIBILITIES

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

The College recognises that many learners have unlimited / unrestricted access to the internet via mobile phone networks. It is further recognised that as a result, some learners will use their mobile and / or smart technology to:

- Sexually harass their peers whilst at college
- Share nudes, either consensually or non-consensually (often via large social media chat groups)
- View and share pornography and other harmful content including revenge porn
- Generate fake nudes via generative-AI, including through use of 'nudifying' apps.

Where such occurrences become known to staff, they must report this via MyConcern, such that appropriate actions and support can be identified, liaising with Heads of Department as appropriate in accordance with the College's Learner Disciplinary Policy.

Strategic Safeguarding, Prevent and E-Safety Group

This group has strategic oversight of matters related to e-Safety which are reported through the Safeguarding, Prevent and E-Safety Operational Group.

Senior Management Team

The Senior Management Team is responsible for ensuring the safety (including e-safety) of members of the College community and will take action as appropriate and as necessary in line with relevant college policies.

Safeguarding, Prevent and E-Safety Operational Group

The Group is made up of the Deputy CEO, Director of Student Services, Safeguarding and Support, Director of Quality, Teaching Development, Student Progress, Director of HR, Head of IT, Safeguarding and Welfare Manager and Head of Student PD and Enrichment. The group takes responsibility for e-safety issues and has a leading role in:

- establishing and reviewing the College e-safety policies, including procedures that need to be followed in the event of an e-safety incident taking place
- advises regarding e-safety guidelines for staff and learners
- advises regarding CPD for the group and the wider college community
- informs development and promotion of the staff and student e-safety section on MySNC and the staff intranet
- reviews and plans e-safety activity, including Student Induction, PD sessions and Safer Internet Day activities and awareness raising content and themes
- receives updates from the Head of IT regarding any potential issues with regards to Cyber Security, filtering and key word searching on college devices on the WIFI network
- reviews impacts of new technologies on student and staff practice, including advancements in AI

- receives relevant updates in regards online safety concerns submitted via My Concern to monitor trends and to inform future e-safety developments and any updates to PD sessions
- understanding the impact of online safety on mental health, including specific focus on companion apps and their use by young people
- implements guidance from Suffolk's Safeguarding Partnership and any other e-Safety related materials or guidance
- ensure that communication to parents / carers is accurate and up to date – via the College website, Parent Portal and Parents' Evenings, and the recently introduced new Parent App
- Identifying and reviewing learner voice feedback opportunities.

The group meet termly and report in to the Strategic Safeguarding, Prevent and E-Safety Group, communicating and reporting updates to Corporation through the Deputy CEO's reporting cycle, alongside annual training facilitated for Governors and delivered by the Director of Student Services, Safeguarding and Support.

IT Services

IT Services is responsible for ensuring:

- that the College's IT infrastructure is secure and is not open to misuse or malicious attack
- that the College meets the e-safety technical requirements according JANET agreements
- that users may only access the College's networks through a properly enforced password protection policy
- the College's web-filtering, anti-spam and anti-virus filtering processes are applied and updated on a regular basis
- that the use of the College network remote access and email is logged where appropriate in order that any misuse or attempted misuse can be investigated and reported
- that logging software / systems are implemented and updated as agreed in College policies (Refer to the GDPR Policy)
- that the College's IT infrastructure is protected by MFA and / or other additional security measures as appropriate in order to ensure business need is safely and securely met
- that staff have regular access to centrally recorded updates on cyber security new and developing threats and best practices.

Teaching and Support Staff

All staff are responsible for using the College IT systems and mobile devices in accordance with the Staff IT Acceptable Use Policy, which they must actively promote through embedded good practice.

Teaching and support staff are responsible for ensuring that they:

- have read, understood the College's E-safety and Staff IT Acceptable Use policy and understand and apply the remote working guidance *when applicable*
- take responsibility for ensuring that learners are e-safety aware and that learners understand and follow the College's E-Safety Policy, IT Acceptable Use Policy
- take responsibility for the safe use by learners of specified technologies which are part of teaching and learning
- complete CPD/training as required by the College
- have an up to date awareness of e-safety matters
- report any suspected misuse or problem, including incidents of cyberbullying, or sexual harassment or abuse including sharing – consensual and non-consensual – of nudes and revenge porn, including when AI-generated

  Where such occurrences become known to staff, they must report this via MyConcern, such that appropriate actions and support can be identified, liaising with Heads of Department as appropriate in accordance with the College's Learner Disciplinary Policy. The Safeguarding team's follow up will take account of advice

  https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advicefor-education-settings-working-with-children-and-young-people
- monitor IT activity in lessons – in college or remotely - student use of college related e-learning facilities, extra-curricular and where appropriate extended College activities.
- engage with learners on social media within stated guidelines in the Staff IT Acceptable Use Policy, **using only college accounts**, so as to safeguard both parties and manage expectations

Learners

Learners are:

- reminded of the College's commitment regarding child-on-child abuse which includes sexual harassment on-line
- responsible for using the College IT and/or communication systems and mobile devices in accordance with the College Student IT Acceptable Use Policy which they are expected to read at induction and agree to adhere to each time they log on to the College IT system
- encouraged to seek help and talk about what their concerns are where they are worried or concerned, or where they believe an e-safety incident has taken place involving them or another member of the College community
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so; and know where to report incidents – either at College or directly to a social media platform
- expected to know and understand College policies on the use of mobile phones, digital cameras and mobile devices. They should also know and understand College policies on the taking / use of images and on cyberbullying

- expected to understand the importance of adopting good e-safety practice when using digital technologies out of College and realise that the College's Student IT Acceptable Use Agreement covers their actions out of College, if related to their membership of the College.

5 ACCEPTABLE USE

The College has an IT Acceptable Use Policy for learners and staff. These policies aim to inform learners and staff in relation to usage of the College IT systems, of their responsibilities, what is acceptable and unacceptable use and consequences of misuse. They also help to ensure the security of the College IT systems, to safeguard the College's business and reputation and to help provide a safe and appropriate teaching and learning environment for all College IT users.

The College will not tolerate any abuse of IT systems. Whether offline or online, communications by staff and learners should be courteous and respectful at all times. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the Learner Disciplinary Policy and staff disciplinary policies and procedures.

Where conduct is found to be unacceptable, the College will deal with the matter internally. Where conduct is considered illegal, the College will report the matter to the Police.

6 COMMUNICATIONS

Computers, tablets, mobile phones, smart watches, games consoles, apps, social media and other smart technology all provide opportunities for online communication, as well as challenges and risk. All digital communications with learners must be professional in tone and content at all times, in line with the staff code of conduct.

Staff will:

- ensure that personal e-mail accounts, mobile/home telephone numbers are not shared with learners
- not allow learners to add a member of staff as a friend to their personal social networking site nor will staff add them as friends to their personal social networking site(s)
- ensure that any private social networking sites / blogs etc. that they create or actively contribute to are not confused with their professional role
- not use personal digital cameras or camera phones for transferring images of children and young people or staff – college devices or the students own device should be used for the purpose of recording any such evidence
- not engage in any online activity that may compromise their professional responsibilities

- engage in social media communication using appropriate forums and at appropriate times, as guided by the Staff IT Acceptable Use Policy.

Learners will:

- not request a member of staff as a friend to their personal social networking site nor will staff add them as friends to their personal social networking site(s)
- follow the college's guidelines for learning remotely and on-line
- not engage in an on-line communication that is of a bullying or harassment in nature including where considered to be AI-generated
- report any incidents that they become aware of or a victim of, to a staff member so that the matter can be dealt with swiftly and robustly.

7 USE OF IMAGES AND VIDEO

The use of images, or photographs and video, is popular in teaching and learning and should be encouraged where there is no breach of copyright or other rights of another person. This will include images downloaded from the internet and images belonging to staff or learners. Learners are asked to provide their consent to the use of personal images at the point of enrolment.

All learners and staff should understand the risks in downloading these images as well as posting them online and sharing them with others. There are particular risks where personal images are posted onto social networking sites for example.

Where learners wish to take and/or use photographs or videos of learners or staff, they must obtain the consent of the individual(s) in advance and be clear about what their intentions are in relation to using the material, ie how they plan to use it.

Photographs or videos of activities on the College premises should be considered carefully and should not include full names of individuals. Our aim is to reinforce good practice as well as offer further information for all users on how to keep their personal information safe.

8 EDUCATION AND TRAINING

Learners

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

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

- Promoting e-safety with learners
- e-safety will be an integral part of the Steps to Success and Apprentice inductions to include activities such as an introduction to the Digital Resilience

Framework, Safer Internet to help learners develop an understanding of the College Acceptable Use Policy, and the e-safety material on MySNC

- e-safety sessions will be run as part of the Safeguarding Unit of the PD curriculum in the first term as part of the safety unit.
- learners will be helped to understand the need for the Student Acceptable Use Policy and encouraged to adopt safe and responsible use of IT an all college areas – including the Digi Hubs, and on-line using the internet and mobile devices both within and outside College;
- key e-safety messages will be reinforced as part of curriculum delivery which will cover:
  - the need to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information, including recognising that access to selected information and exposure to one-sided narratives could be potentially harmful
  - AI-generated risks of harm and impact on mental health, in particular the use of 'companion' apps
  - Awareness of potential harmful material and activity, e.g. challenges and hoaxes, money laundering and unsafe enterprising activities through social media platforms
  - acknowledgement of the potentially serious impact of inappropriate use on the College and individuals
  - how to report misuse that they observe or are subject to and how to receive appropriate support
  - the need to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

- Learners will be encouraged and supported to develop positive and professional social media profiles to enhance their employability prospects, through Professional Development sessions and Safer Internet Day activities.

Staff

It is essential that all staff understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- An introduction to e-safety will be part of the safeguarding introduction for all new staff
- A schedule of planned CPD activity to update staff will be provided by the Teacher Development Coach with responsibility for e-Safety and PREVENT – this training will be tailored appropriate to staff's role
- Follow up on-line e-safety and guidance for remote learning protocol will be shared via the Teacher's Toolkit - available to staff
- the Designated Safeguarding Lead and the Safeguarding Team will receive updated and training and share these as relevant through e-safety updates in CPD sessions.

Parents / Carers

- Parents will be provided with current guidance through the Parent Portal and Parents Evenings, mailouts and via the College's new MySNC Parent App
- Online safety is a whole community issue and this portal is designed to improve parents' knowledge and understanding of the risks their young person may face online and signpost to external sources of help and support.
- It also provides practical strategies and advice to help keep their young person safe online and signposts to further resources and reporting sites which they may find helpful.

9 SECURITY

The College will undertake all reasonable measures to ensure that the network is safe and secure whilst remaining flexible enough to provide the curriculum and business administrations needs the College has within the resource constraints that the College operates under.

Cyber Security is a continually evolving requirement which will require a continuous programme of activity and development – both as threats change, and the resources required to address threats adapt over time.

Appropriate security measures currently include an enterprise-grade internet firewall, Smoothwall website filtering, anti-spam and anti-virus software which auto-updates, lockdown of computers to limit installation of software and where possible limit the ability to run scripts, privileged access permissions, password policy, segregation of student BYOD and the use of MFA for protecting Remote Desktop access for staff.

Furthermore, the College utilises services provided by JISC/JANET to increase its security awareness, DNS (Internet Domain Name Service) filtering and also makes use of the NCSC services to regularly scan the College's external websites for security issues.

The College implemented a backup system and a new server update patching system and is currently conducting a trial of a new desktop patching solution to identify if this can be deployed across the wider network. Regular desktop patching has already been deployed to InTune managed devices successfully. These improvements help further enhance the existing ongoing programme of security reviews, server / software updates and capital procurement to bolster protection and resiliency to cyber-attack. Penetration Tests are conducted annually to assess the network's security, to ensure continuous improvement.

The oversight and scrutiny of the effectiveness of the filtering systems is undertaken by the College's Safeguarding, Prevent & E-Safety committee groups.

Technical infrastructure

- College IT systems will be managed in ways that ensure that the College meets required e-safety technical requirements
- There will be regular reviews and audits of the safety and security of College IT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to College IT systems
- All users will be provided with a username and password at enrolment or commencement of employment
- 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
- Users will be encouraged to adopt a unique password for their college username which is not then used for their personal accounts
- The College maintains and supports the managed filtering service
- Concerns regarding any internet filtering categories or prohibited websites will be communicated by the Head of IT to the Director of Student Services, Safeguarding & Support (to determine any immediate response and onward safeguarding actions as required)
- Phishing
- The College maintains and supports the classroom management system provided by appropriate software
- College IT technical staff may monitor and record the activity of users on the College IT systems and users are made aware of this in the Acceptable Use Agreement.

Personal Information

Suffolk New College collects and stores the personal information of learners and staff regularly e.g. names, dates of birth, email addresses, assessment materials and so on. The College will keep that information safe and secure, and only share information within the parameters of information sharing agreements as required through GDPR legislation.

Staff must keep learners' personal information safe and secure at all times and minimise the risk of its loss or misuse. Personal data should only be used on password protected computers and other devices. Every user should ensure that they are properly 'logged off' at the end of any session in which they are using personal data or where they are physically absent, the device should be locked or logged off. When transferring data encryption and secure password protected devices should be used. Any college owned mobile device (laptop, USB, iphone, ipad or tablet) should be password protected and signed out by IT/HR staff.

Where the personal data is no longer required, it must be securely deleted in line with the College's Data Protection Policy.

10 RESPONDING TO INCIDENTS

It is hoped that all members of the College community will be responsible users of IT, 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.

When this occurs staff and learners may be subject to disciplinary process. It is the responsibility of staff and learners to report any apparent or actual incidents of misuse by learners or staff which may include:

- Any behaviour by staff or learners which affects the safety and security of the IT systems or other users and is against the IT Acceptable Use Agreement
- Any failings in technical safeguards which may become apparent when using the systems and services
- Any incidents, messages or access to sites that make staff or learners feel uncomfortable or unsafe – eg cyber bullying, trolling, sexual harassment or abuse (including the sharing of – consensual and non-consensual – of nudes and revenge porn), sextortion, including where generative AI has been used
- Any damage or faults involving equipment or software, however this may have happened.

Misuse by learners should also be reported to the relevant Head or Director and will be dealt with through the College Learner Disciplinary Policy. If this is considered a safeguarding issue, it must also be reported via MyConcern.

Misuse by staff should be reported to the relevant College Manager, who will inform HR and where necessary a referral to the Local Authority Designated Safeguarding Officer may be made.

Incidents involving illegal content

On discovery of illegal content, the equipment or materials found should not be touched.

- Computers or other devices should not be switched off unless it is authorised to do so by the Police
- Further access to the illegal content should be prevented by keeping other people out of the area
- If necessary the monitor itself can be turned off but the computer should remain as you have found it (DO NOT shut the machine down)
- If the device is a laptop, do not close the lid as this may cause the machine to power off, ensure remains connected to a power supply

- No attempt should be made to view, download, print or send any materials found. (By doing so you may commit further offences and yourself be liable to police investigation and prosecution)
- All illegal content must be reported to the Police and the Internet Watch Foundation (www.iwf.org.uk)

11 ADVICE AND ASSISTANCE

Teaching staff, Progress Tutors / Coaches and the Student Support and Safeguarding Team can provide advice, support, guidance and assistance to learners subjected to bullying or harassment. Any advice and assistance is not intended to vary the procedure above. Any concerns of a safeguarding nature must be reported via MyConcern, in accordance with the terms of the College's Safeguarding and Child Protection Policy.