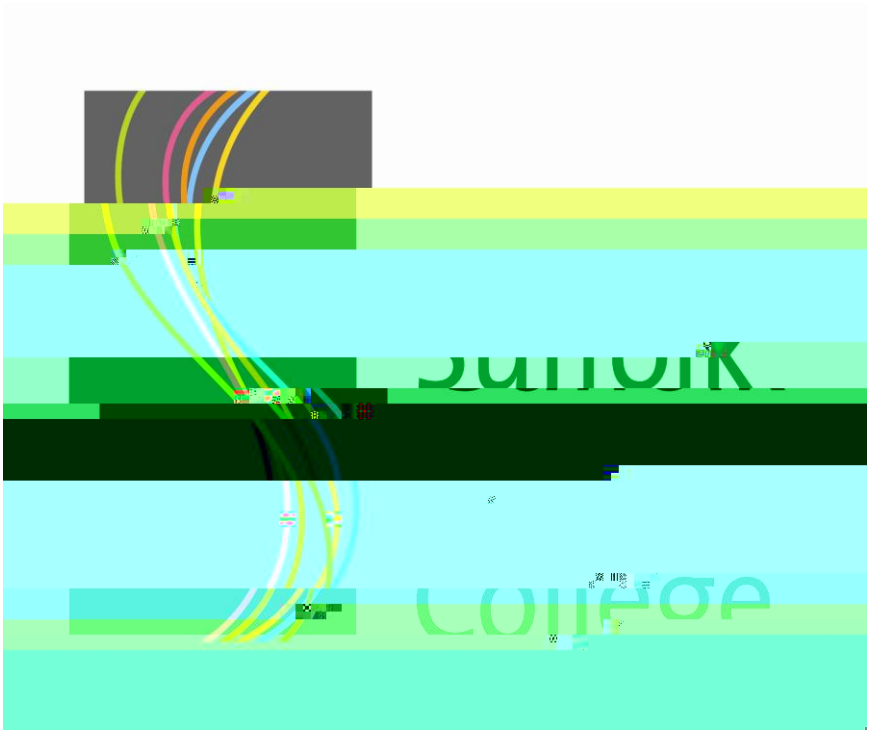

E-Safety Policy

Equality Impact Assessment Tool

Name of Policy: E-Safety Policy

1	**Does the policy/guidance affect one group less or more favourably than another on the basis of:**		
		No	
		No	
		No	
		No	
		No	

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 or social media.

Mobile devices, such as computers, tablets, mobile phones, smart watches and games consoles, and social media, are an 7ices, su

2 SCOPE OF THE POLICY

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 *I ou our rn rs or st r t r s wp s r port t to t Ant s n or n Group ttps pw .or .*
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 imy		

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 ille349(u)

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 Supporting Student Achievement Policy.

Strategic Safeguarding and Prevent Group

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

E-Safety Group

The E-Safety Group is made up of the Director of Quality, Teaching Development, Student Progress, Director of Student Services, Safeguarding and Support, Head of Student PD and Enrichment;; teaching staff representatives, Director of IT Services

ensure that communication to parents is accurate and up to date – via the College Website, the Parent Portal and Parent's evenings

Identifying and reviewing learner feedback opportunities

The group meet termly and reports to the Health and Safety Operational Sub-Committee; the Strategic Safeguarding and PREVENT Group and the Operational Safeguarding and PREVENT Group, contributes to the annual Safeguarding report.

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 internet and anti-spam filtering policy is 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).

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 guidance in 'Remote Working – Protocol and Guidance for on-line Learning' (Appendix A)

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 and the Student and Apprentice Code of Conduct for e-Learning (see Appendix B)

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;

- 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 Supporting Learner Achievement Policy.
- The Safeguarding team's follow up will take account advice provided by https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-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 peer-on-peer 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;

Responsible for adhering to the Student and Apprentice Code of Conduct for e-Learning

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 cyber-bullying;

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 Student Supporting Achievement policy and staff disciplinary codes.

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

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 and the 'Remote Working – Protocol and Guidance for on-line Learning' (Appendix A)

Students will:

Students 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);

Students will follow the college's guidelines for learning remotely and on-line

Students will not engage in an on-line communication that is of a bullying or harassment in nature

Students will 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 the campaign – 'Be E-aware –

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

Parents will be provided with current guidance through the Parents Induction website and the parent portal and parent evenings

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 you keep your young person safe online and signposts to further resources and reporting sites which may be of use.

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 will endeavour to meet the requirements for Cyber Essentials for a subset of key staff administrative PCs and servers linked to the internet, and has an ongoing programme of security reviews, server/software updates, capital procurement (new backup system, new server update patching system) and enhanced desktop patching solutions over the next 12-18 months to bolster protection and resiliency to cyber-attack.

The oversight and scrutiny of the effectiveness of the filtering systems will be undertaken by the Strategic Safeguarding Group as a standing agenda item.

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.

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, i-phone, i-pad or tablet) should be password protected and signed out by the 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

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

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 as this may cause the machine to power off.

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 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. For further details – refer to the Learner Anti-bullying and Harassment Policy, including signposting and referring externally where appropriate.