Online Safety Policy			
Current Status	Operational	**Last Review:**	June 2020
Responsibility for Review:	Deputy Principal	**Next Review:**	June 2021
Approved by:	SLT	**Originated:**	June 2010

1.0 Introduction

1.1 One has a duty to safeguard and promote the welfare of its students and this includes ensuring that students develop and apply their ICT capability effectively and responsibly in their everyday lives.

1.2 There are a number of documents that sets out how individuals and organisations should work in partnership to safeguard and promote the welfare of children. These include:

- *Working Together to Safeguard Children 2018*
- *Keeping Children Safe in Education* 2019
- *Serious Crime Act* 2015
- *Counter Terrorism and Security* Act 2015 amended 2019
- *Ofsted* 2019

1.3 In addition, there have been a number of reports which provide exemplar Online Safety practice. These include:

- *Teaching Online Safety in Schools* 2019 DfE
- *Education for a Connected World Framework* 2018 UK Council for Internet Safety
- *Vulnerable Children in a Digital World* 2019 Internet Matters.org and Youthworks
- *Commentary on "Screen Based activities and children and young people's mental health and psychosocial wellbeing: a systematic map of reviews"* 2019 United Kingdom Chief Medical Officer

1.4 Staying safe ensures that children and young people are:

- safe from maltreatment, neglect, violence and sexual exploitation
- safe from accidental injury and death
- safe from bullying and discrimination
- safe from crime and anti-social behaviour in and out of school
- secure, stable and cared for
- safe from radicalisation
- supported to ensure that they develop resilience in their online life

1.5 It is the duty of the college to ensure that every child and young person in their care is safe and the same principles should apply to the 'virtual' or digital world learners will encounter whenever they use ICT in all its various forms.

1.6 Recent government research activities such as Keeping Children Safe in Education consultation have focused on keeping young people safe online. In addition, both the UK Council for Child Internet Safety (UKCCIS) and National Crime Agency CEOP Command promote, support and investigate Online Safety issues.

1.7 Digital Wellbeing of Learners[1] understanding the positive benefits and any potential negative aspects of engaging with digital activities is key to ensuring the wellbeing and safety of students.

1.8 One's Online Safety Policy has been written by the College's Online Safety Lead in collaboration with the Designated Safeguarding Lead. It has been agreed by the senior management and approved by Governors. It will be reviewed annually.

1.9 This Policy document is drawn up to protect all parties and aims to provide clear advice and guidance on how to minimise risks and deal with any infringements.

2.0 The Technologies

2.1 ICT in the 21st Century has an all-encompassing role within the lives of children, young people and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in colleges and, more importantly in many cases, outside of college by children, young people and adults include:

- The internet
- e-mail
- Remote and blending learning
- Instant messaging (Skype, Snapchat, Whatsapp, Messenger) often using simple web cams or mobile devices.
- Blogs (online publishing e.g. Blogger, Tumblr, Wix, Wordpress)
- Podcasting (audio/video broadcasts either live or downloaded to computer or MP3/4 player e.g. Soundcloud)
- Social networking sites (e.g. Instagram, Facebook, Twitter, LinkedIn, Discord, TikTok)
- Video sharing/streaming sites (e.g. Youtube, Twitch, Snapchat, TikTok)
- Chat Rooms (e.g.www.omegele.com)
- Dating sites (e.g. Tinder, Grindr, Plenty of Fish, Match, Ok Cupid)
- Forums (e.g. Reddit, 9gag, 4chan)
- Gaming Platforms (e.g. Xbox online, Playstation, Nintendo Online, Steam)

[1] Jisc Digital Well Being of Learners 2020 https://www.jisc.ac.uk/guides/digital-wellbeing-of-learners

- Music download sites (e.g. iTunes, Spotify, Tidal, Deezer)
- Mobile phones with camera and video functionality
- Mobile technology (e.g. games consoles) that are 'internet ready'
- Smart phones with e-mail, web functionality and cut down 'Office' applications

- Location based services (services that allow you to check in your current location, so it is publicly viewable e.g. Google Maps and social media sites e.g. Facebook, Instagram, Twitter etc.

3.0. One's approach to the safe use of ICT

Figure 1: creating a safe learning environment

Online Safety and e-Responsibility are components, part of the College's commitment to the safeguarding of learners. Creating a safe ICT learning environment consists of three main elements:

- Policies and procedures, with clear roles and responsibilities
- An effective range of infrastructure and technology
- An Online Safety education and training programme for students, staff and parents

4.0 Roles and Responsibilities

4.1 At One Online Safety is recognised as an essential aspect of strategic leadership and the Principal, with the support of Governors, aims to embed safe practices into the culture of the College. The Principal ensures that the Online Safety policy is implemented, and compliance monitored.

4.2 The responsibility for Online Safety has been delegated to a member of the senior leadership and management team, the Designated Safeguarding Lead.

4.3 Governors need to have an overview and understanding of Online Safety issues and strategies at the College. One ensures governors are aware of local and national guidance on Online Safety and are updated annually on policy developments.

4.4 All teaching staff are responsible for promoting and supporting safe and responsible behaviour in their classrooms and following the College's Online Safety policy.

4.5 All staff and students will follow the written protocol/guidance for staff for safe online/remote learning and when needing to conduct 1:1s (See Appendix 2)

4.6 Our IT service partners are responsible for the security of the College network and for monitoring internet activity alerting the DSL of any potential breaches or inappropriate use by students, staff or visitors to the network including Bring Your Own Device.

4.7 One will include guidance on Online Safety in the tutorial programme and ensure that every student has been educated about safe and responsible use of ICT (e-Responsibility).

4.8 One will make efforts to engage with parents over Online Safety matters and make available resources to help guide them in safe internet and social networking usage.

5.0 Communications

5.1 How will the Online Safety policy be introduced to students?

5.1.1 A section on Moodle is available on Moodle through the Student Services section. Personal Progress Tutors (PPTs) will also cover this with their tutor groups to help raise awareness and to stress the responsible and safe use of new technologies. Exemplar materials will be used from the **Child Exploitation and Online Protection** Centre (CEOP) to support this. Information relating to reporting inappropriate material will be available on the One website and Moodle.

5.1.2 All students will be required to sign the acceptable use of ICT policy each September as part of the induction programme. Parental consent will also be sought during enrolment and induction.

5.1.3 Regular reminders about Online Safety will be promoted to students to keep the policy 'active'.

5.1.4 Students will also be reminded at the beginning of any lessons which involve the use of ICT of the rules and the potential risks of using the internet will be addressed.

5.1.5 Students who have Additional Learning Needs will be supported by One so they are able to access a broad and balanced curriculum and recognise the importance of tailoring activities to suit the educational needs of each student. Where a student has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of Online Safety awareness sessions and internet access.

5.2 How will the Online Safety policy be discussed with staff?

5.2.1 All staff will have access to the Online Safety policy and the framework for Acceptable us of ICT on Platform One and will have access to useful resources to support this and to help understanding. They will abide by the Staff Code of Conduct.

5.2.2 Online Safety refreshers will be available to staff across the year including mandatory online resources to complete. Staff will receive online safety updates throughout the year. Due to current situation with Covid19, this will include direct training with regard to conducting online meetings with students, with particular reference to one to ones.

5.2.3 If staff have any concerns or questions about the use of ICT within One, they must discuss this with the line manager immediately.

5.3 How will parents' support be enlisted?

5.3.1 Internet use in students' homes is increasing rapidly. Unless parents are aware of the dangers, students may have unrestricted access to the internet. A partnership approach with parents is encouraged and the LRC team have developed information to show both how we ensure a safe environment and also offer advice on responsible use of internet and social networking at home. This information is available at Consultation evenings and Open Events.

5.4 How will Governors' support be enlisted?

5.4.1 All governors will receive training on Online Safety in the form of an annual refresher. The Principal will inform Governors about the progress of or any updates to the Online Safety curriculum and ensure Governors know how this relates to safeguarding

6.0 How will complaints and incidents regarding Online Safety be monitored?

6.1 One will take all reasonable precautions to ensure Online Safety. However, owing to the international scale and linked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a College computer or

mobile device. Having taken all reasonable security precautions, the College cannot accept liability for material accessed, or any consequences of internet access.

6.2 The Acceptable Use Policy for students and the Staff Code of Conduct outlines the expectations and responsibilities of staff and students, gives information about what constitutes an infringement and documents the range of sanctions that could be applied.

6.3 Sanctions available to students include:

- interview or referral to counselling by PPT, Student Services Leadership, Head or Director of Curriculum or a member of the Senior Leadership Team
- removal of internet and College network access for a specified period of time
- communication with parents or carers
- suspension
- exclusion
- police referral

6.4 Complaints about student misuse will be dealt with through the college disciplinary procedures.

6.5 Any complaint about staff misuse is referred to the Director of Human Resources.

6.6 Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy and Code of Conduct.

6.7 Complaints related to child protection are dealt with in accordance with the College's safeguarding policy (this policy is also an appendix of the Safeguarding Policy).

6.8 Complaints relating to the policy or its application will be dealt with through the College's complaints procedures.

7.0 Compliance

7.1 **Staff**

If colleagues are found to be in breach of this policy and/ or the guidelines, they will be subject to the Disciplinary Procedure.

7.2 **Students**

Please see documents in Appendix 1

Revision History

Revision date	Reason for revision	Section number	Changes made
June 2020	Updated to include Virtual meeting and lessons	Appendix 2	Added following Covid 19

Appendix 1

ICT User Agreement - Students

Acceptable Use of ICT at One

Users requesting access to the Network, Internet, or **e-mail** resources must agree to the proper use of the college's ICT resource, sign a copy of this statement and return it to the college. Users who fail to follow this agreement may be denied access to some, or all, of the college's resources and disciplinary procedures may be invoked.

The computer system is owned by the college and is made available to students to further their education and to staff to enhance their professional activities during teaching, research, administration and management.

The college reserves the right to examine or delete any files that may be held on its ICT system, to monitor any internet sites visited, and to examine any **e-mails**.

I understand and accept that:

1. Access to the resource can be made only via the User's own user name and password.
2. Users must not make their User ID or Password available to any other person.
3. All activities utilising the college's system should be appropriate to the enhancement of the student's education.
4. Copyright of materials must be respected.
5. Use of the network to access inappropriate materials (e.g. pornographic, racist or offensive material) is forbidden.
6. Unauthorised use for personal financial gain, gambling, political purposes or advertising is forbidden.
7. Activity that threatens the integrity of the college's ICT systems, or activity that attacks or corrupts ICT systems is forbidden, including attaching unauthorised electronic media or devices.
8. Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received.
9. Posting anonymous messages and/or forwarding chain mail is forbidden.
10. Language and content used for any electronic communication should be as is acceptable for normal work.
11. This Agreement covers college's ICT system even when access is made to the system from a home computer via the Internet.
12. The inappropriate use of social network sites, which brings Suffolk One into

disrepute or causes offence to students or staff is not acceptable. Suffolk One expects students and staff to use social network sites such as Face Book, You Tube, and Twitter in a mature and responsible manner.

13. When submitting an assignment it is my responsibility to print my own work. To support this Suffolk One will provide me with a termly printing allowance which I will have the ability to top up.

14. The use of any technology designed to avoid or bypass the college/education setting or other establishment filtering system is forbidden. I understand that intentional violation of this rule may result in disciplinary procedures being initiated

I will:

15. Notify a member of staff if I receive unpleasant messages or other material.

16. Respect the college's ICT equipment and use it suitably and with care.

Student Agreement

By signing this form you confirm that you have:

- Read and agreed to the terms of the Code of Conduct – found on the website
- Read, signed and agreed to the ICT User Policy – found on the website
- Read and agree to the Finance and Printing information – found on the website

You also agree to:

- The College processing and using my personal data as detailed in the Privacy Notice
- The College processing and using my personal data contained in the enrolment form and other information (such as photos and portfolios), which the College may obtain from other people or me, whilst I am a student and for any purposes connected with my studies, my health and safety or for any other legitimate reason
- Give permission for my previous student information to be passed from the Local Authority, to the College
- The College contacting Parents/Guardians to involve them in course progress reviews and open evenings
- Look after all resources allocated to me. I understand that the College will seek to reclaim any cost above my resource deposit for replacement resources

Signed: ……

Date of Birth: …….

Dated: ……

Please print your name: ……..

Appendix 2

PROCEDURE FOR DELIVERING LESSONS/ONE TO ONES - USING ONLINE PLATFORMS

The following information applies to both curriculum and student services:

We have taken advice from safeguarding professionals and our own colleagues to create the following protocols. There are some general rules and more specific information for how to conduct the sessions. We will be delivering further training in the induction week for both students and staff and a policy will exist that directly refers to online delivery.
As we are delivering live lessons via online platforms, we have assessed any risks and taken appropriate actions to minimise potential harm to both students and staff.

General procedures

Ratio Sessions can operate with one staff member to one student, as long as the procedures below are adhered to. There may be some instances where exceptional circumstances apply and this may require more staff to be present. If you are ever unsure, please liaise with your line manager or DSL

Risk assessment we will be producing a Security Risk Assessment in the first instance, in accordance with advice taken from the National Cyber Security Centre that addresses the following – amongst more general information, it will address how we implement basic security controls; where the data / recordings are stored; who has access and what can we do with it

Staff are responsible for ensuring that they are up to date with requisite safeguarding training

Consent Communication will go home to ensure that parents, carers and students understand the benefits and risks of online lessons and consent will be gathered at enrolment, within pre-existing paperwork and alongside other disclaimers that students are asked to sign

Platform Staff must make sure that the platform they are using is suitable (age specific). New accounts may need to set-up for any online platforms you use (no personal staff accounts). If staff members are accessing families' contact details at home, we must ensure that they comply with the Data Protection Act 2018. Staff should only use either school email accounts or parents' and carers' email addresses or phone numbers to communicate with students, unless this poses a safeguarding risk. Always check the privacy settings before conducting the session

Recording Everyone needs to be reminded that the session is being recorded.

It should also be made clear that it is not acceptable for students to record and onward share parts or all of the recording (SWGfl). It is therefore essential that the member of staff initiates the recording and **not** the student and that the staff member remains the 'owner'

Scheduling Staff should only contact students during normal school hours, or at times agreed by the school leadership team (DfE, 2020). **All online meetings MUST be scheduled into staff and student calendars and not be 'ad hoc' in nature.**

Any 1:1 for the Foundation Learning students and high safeguarding concern student must then take place only at the days / times agreed with parents / carers. **Parents and carers should be present in the home at the time**

QA To comply with safeguarding quality assurance measures, managers must always have the capacity to 'drop in' to any session and both staff and students should be made aware of this as part of any overall policy

Behaviour Staff should familiarise themselves with the privacy settings and know how to report any offensive or abusive content – this will be contained within the policy. End the call, if at any time you feel uncomfortable with something done or said during a 1:1 call and report any concerns to your line manager and / or DSL

The Teaching 'live' Session

Whilst using an online platform to teach 'live' sessions to students by means of screen sharing, audio and/or video, Staff must:

- Test your audio and video before a scheduled call
- Be punctual and courteous
- Meetings which include external parties, introduce yourself and take note of other attendees' names
- Put your phone on silent
- Remind students of the '*hand raising*' and '*chat*' function, at the start of the session – where appropriate, suggest guidelines for conducting the chat in accordance with the aims of the session
- For sessions involving students, please insert a suitable background before the session begins and avoid recording in a bedroom
- If you need visual access to a teaching aid, please use a neutral background
- Dress as you would for work
- Double check that any other tabs you may have open in the browser, that would be inappropriate for a student to see, are closed - if you happen to be sharing the screen
- Use professional language at all times
- Remind students at the start of each session that it is being recorded
- Recommend that students use a shared space in their house for video, rather their bedrooms
- Encourage students to dress appropriately for video, if they are not – request that they switch off video, if the situation persists – follow-up with PPTs
- Ensure that students are not left in the meeting after the teacher departs – the member of staff should close each session and be the last to leave
- Under NSPCC guidelines, give sensitivity to the needs of individual students, either SEND or the sensitivity around certain topics or issues that may arise during the livestream, for instance remind participants that they can always "turn off incoming video"

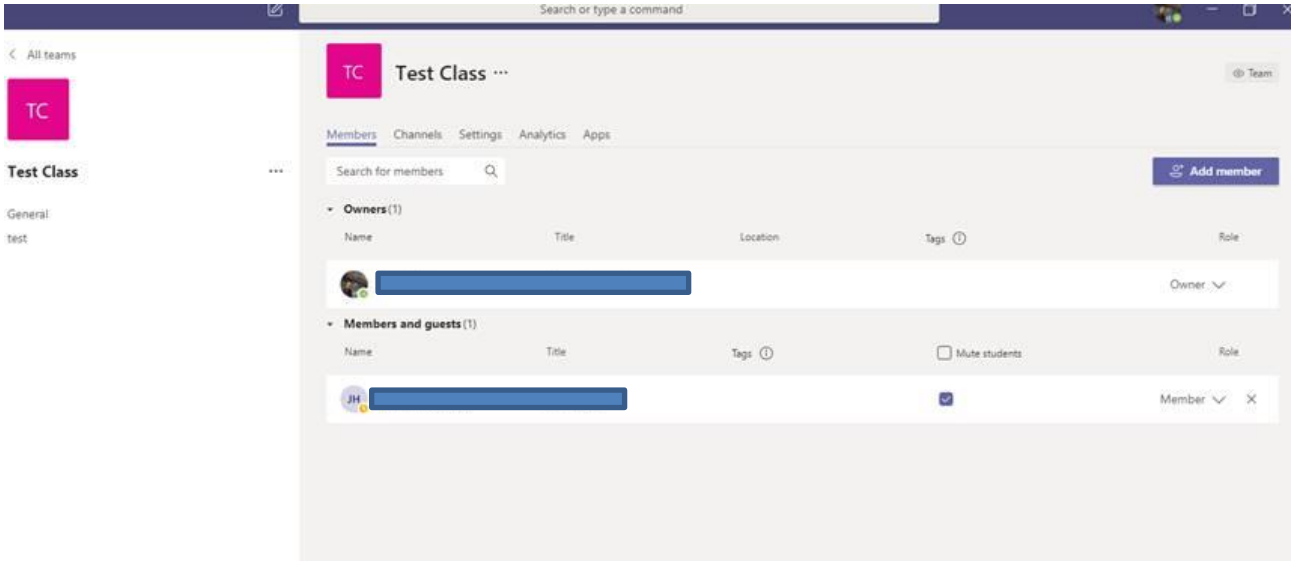
Don't:

- Multi-task; your audience will be aware.
- Wear stripes or heavy patterns creating pixilation of images
- Extend one to one discussions unnecessarily

Slide available if required:

How to use the mute function using class teams:

Create a new 'Team' which is the Class, then it is possible to choose 'Manage Team' and mute individuals (see screenshot).



Useful further guidance:

https://www.tes.com/news/coronavirus-10-safeguarding-rules-teachers-home

https://learning.nspcc.org.uk/news/2020/march/undertaking-remote-teaching-safely/

https://www.nspcc.org.uk/keeping-children-safe/online-safety/internet-connected-devices/