Online Safety			
Current Status	**Operational**	Last Review:	**February 2019**
Responsibility for Review:	**Assistant Principal, (Students)**	Next Review:	**February 2020**
Internal Approval:	**SLT**	Originated:	**June 2010**

1. Introduction

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.

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 2016*[1]
- Keeping Children Safe in Education 2015[2]
- Serious Crime Act 2015[3]
- Counter Terrorism and Security Act 2015[4]
- Ofsted 2015[5]

[1] Gov.uk. 2016. **Working Together to Safeguard Children**. [ONLINE]

[2] Gov.uk. 2016. **Keeping Children Safe in Education**. [ONLINE] Available at:

[3] Gov.UK. 2015. **Serious Crime Act 2015**. [ONLINE] Available at: https://www.gov.uk/government/collections/serious-crime-bill. [Accessed 07 March 16].

[4] Gov.UK. 2015. **Serious Crime Act 2015**. [ONLINE] Available at: https://www.gov.uk/government/collections/serious-crime-bill. [Accessed 07 March 16].

[5] Gov.UK. 2015. **Common inspection framework: education, skills and early years from September 2015**. [ONLINE] Available at: https://www.gov.uk/government/publications/common-inspection-framework-education-skills-and-early-years-from-september-2015. [Accessed 07 March 16].

The ‘staying safe’ outcome seeks to ensure 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

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.

All users in the organisation also need to be aware of e-Responsibility Digital Literacy, which supports Online Safety.

Digital Literacy can be defined as:

“The capabilities which fit someone for living, learning and working in a digital society.”[6]

Recent government research activities such as Keeping Children Safe in Education consultation[7] have focused on keeping young people safe online. In addition, both the UK Council for Child Internet Safety (UKCCIS)[8] and National Crime Agency CEOP Command[9] promote, support and investigate Online Safety issues.

---

[6] Jisc. 2015. **Developing digital literacies in practice**. [ONLINE] Available at: https://www.jisc.ac.uk/guides/developing-digital-literacies/in-practice. [Accessed 08 March 16].

[7] Gov.uk. 2016. **Keeping Children Safe in Education consultation**. [ONLINE] Available at: https://www.gov.uk/government/consultations/keeping-children-safe-in-education-proposed-changes. [Accessed 08 March 16].

[8] Gov.uk. 2016. **UK Council for child internet safety**. [ONLINE] Available at: https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis. [Accessed 08 March 16].

[9] National Crime Agency Command. 2016. **Child Exploitation & Online Protection Centre**. [ONLINE] Available at: https://www.ceop.police.uk/. [Accessed 08 March 16].

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

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. The Technologies

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
- Instant messaging (e.g. www.skype.com, www.snapchat.com) often using simple web cams or mobile devices.
- Blogs (online publishing e.g. www.blogger.com , www.tumblr.com)
- Podcasting (audio/video broadcasts either live or downloaded to computer or MP3/4 player e.g. www.soundcloud.com)
- Social networking sites (e.g. www.instagram.com , www.facebook.com, www.twitter.com, www.pinterest.com, www.askfm.com, www.linkedIn.com)
- Video sharing/streaming sites (e.g. www.youtube.com, www.liveleak.com www.snapchat.com, www.twitch.com)
- Chat Rooms (e.g.www.omegele.com)
- Dating sites (e.g. www.tinder.com,)
- Forums (e.g. www.reddit.com and www.9gag.com)
- Gaming Sites (e.g. www.miniclip.com/games/en/, www.runescape.com/)
- Music download sites (e.g. www.apple.com/itunes/ www.tidal.com www.spotify.com)
- 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. One's approach to the safe use of ICT

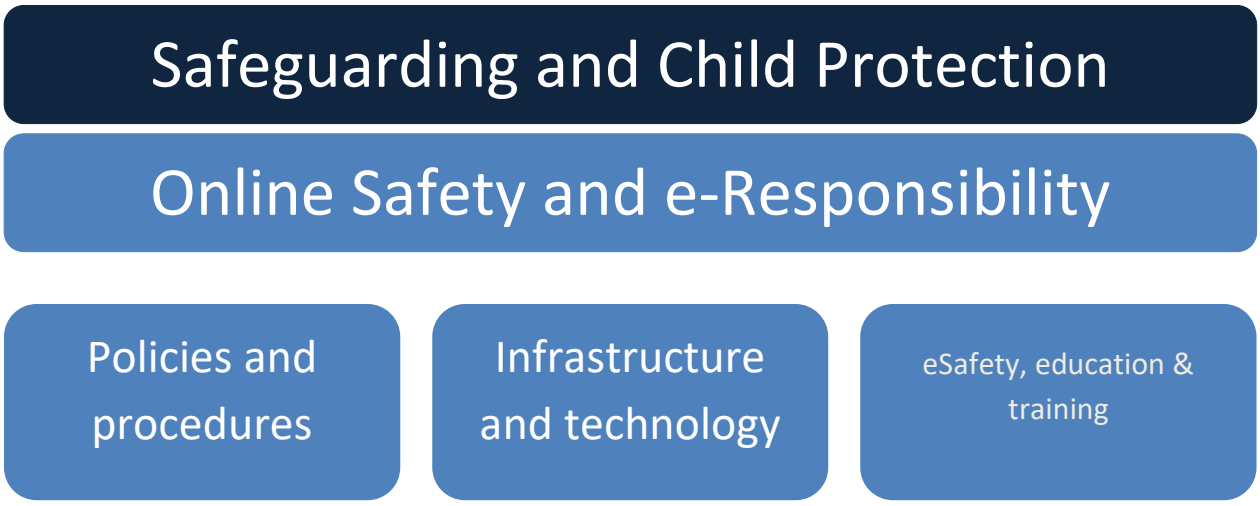


Figure 1: creating a safe learning environment

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[10]:

- 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

[10] 7 Cf. Becta's PIES model (Safeguarding children in a digital world)

4. Roles and Responsibilities

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.

The responsibility for Online Safety has been delegated to a member of the senior leadership and management team, the Assistant Principal,and eSafety Lead..

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.

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

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).

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. Communications

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

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.

All students will be required to sign the acceptable use of ICT policy each September as part of the induction programme.

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

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.

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 pupil. 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?

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.

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 as part of their 8.30 CPD sessions.

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?

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?

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

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.

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.

Sanctions available to students include:

☐ interview or referral to counselling by PPT, Student Services Leadership, Head or Directorof 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

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

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

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

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).

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 on the following pages.

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. When using 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

Please read the following statements:

- I agree to the College processing and using my personal data as detailed in the Privacy Notice for School Census form.

- I agree to 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.

- I agree to give permission for my previous student information to be passed from the Local Authority, to the College.

The College will contact Parents/Guardians to involve them in course progress reviews and open evenings.

- I have read and agree to the terms of the Code of Conduct.

- I have read and agree to the ICT User Policy.
- I agree to allow photographic images of myself to be used in promotional material.
- I agree to 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.

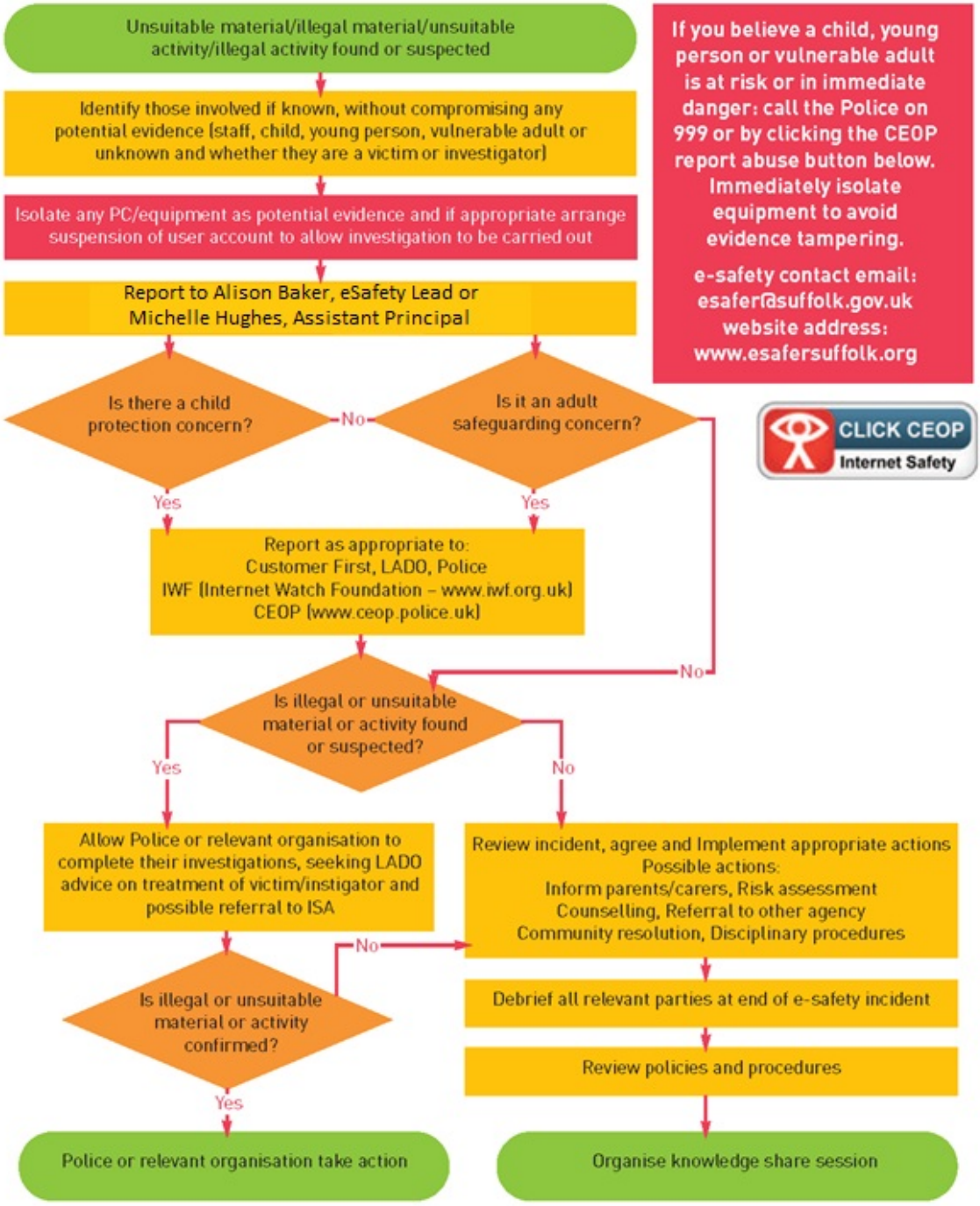
- I have read the finance information sheet. I understand that I will be required to pay a fine of £1 per day for forgotten badges and a charge of £5 for a new badge to be issued.

Student signature:…….. Date:……..

Printed Student Name:……..

Appendix 1

e-Safety Incident Flowchart



If you believe a child, young person or vulnerable adult is at risk or in immediate danger: call the Police on 999 or by clicking the CEOP report abuse button below. Immediately isolate equipment to avoid evidence tampering.

e-safety contact email: esafer@suffolk.gov.uk
website address: www.esafersuffolk.org

CLICK CEOP
Internet Safety

Recording Form for Safeguarding Concerns
(Must be hand-written)

Nature of Concern / Disclosure.

Only record what was actually said DO NOT add your own opinion.

Your signature: Date:

Was there an injury?	YES		NO		Did you see it?	YES		NO	
Describe the injury:									
Have you filled in a body plan to show where the injury is and its approximate size?						YES		NO	
Was anyone else with you? Who?						YES		NO	
Where were you?									
Has this happened before?	YES		NO						
Did you report the previous incident?	YES		NO		To Whom?		Date:		
Does the safeguarding concern involve a technological device?						YES		NO	

If yes, discuss this with your eSafety Lead and follow the eSafety reporting flow chart (on Platform One). This is to be recorded on the eSafety Lead's log by Alison Baker or Michelle Hughes.

Who are you passing this information to?	Name:	Time:
	Date:	

Your Signature:

PRINT NAME: Date:

Action taken by SDP

If the safeguarding concern involved a technological device, please state at what level:

To be completed by the ABK/MHU:	***SAP Level - please tick box the level applies to***	*Lev 1*	*Lev 2*	*Lev 3*	*Lev 4*	*Lev 5*

Referred to..?

Police ☐ School Nurse ☐ Social Services ☐ Connexions ☐ Parents ☐
Other ☐

Parents informed?

Feedback given to…?

☐ Pastoral team ☐ Tutor ☐ Student ☐ Person who recorded disclosure

SDP Signature: Date:

Additional information (if required)