Online Safety Policy *(Students)*

2019-20

Author:	**Name**	J Kelly	
	Job Title	Assistant Principal Curriculum & Quality	
Date policy reviewed.	04/02/2019	**Date policy to be reviewed**	10/01/2020
Equality Impact assessed by:	J Kelly	**Date impact assessed:**	04/02/2019
GDPR Impact assessed by:	J Kelly	**Date impact assessed:**	04/02/2019
Policy approved by:	CET	**Date approved:**	07/02/2019

Contents

1. Introduction

1.1 The College has a positive policy of equality and diversity and strives to support students where ever possible. The College also has a duty of care to safeguard all of its stakeholders including staff, students and visitors and is committed to providing a safe environment for study and work.

1.2 As part of an ongoing commitment to safeguard all of its stakeholders the College operates a policy whereby all students must adhere to online safety restrictions.

> *"Sefton Local Safeguarding Children's Board [LSCB] recognise as the use of digital communications technology has grown, so too have the benefits and the risks that children now come into contact with on a daily basis. It has become the case that the online world has become firmly integrated into the lives of young people with most not making any distinction between their online and offline lives"*
>
> *-Sefton Local Safeguarding Children Board 'e-safety'*

1.3 The College will make every effort to ensure that students are given every opportunity to access online content in order to study, provided it can ensure its safeguarding commitment to the whole college community.

1.4 Computer skills are vital to access employment and life-long learning as ICT is now seen as an essential skill for life. However, technologies present risks to vulnerable groups as well as benefits. Internet use for work, home, social and leisure activities is expanding across all sectors of society. This brings staff and students into contact with a wide variety of influences some of which may be unsuitable.

1.5 The use of technology has become a significant component of many safeguarding issues such as child sexual exploitation; radicalisation and sexual predation. The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- Content: being exposed to illegal, inappropriate or harmful material
- Contact: being subjected to harmful online interaction with other users; and
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm

1.6 These new technologies are enhancing communication and the sharing of information, which inevitably challenge the definitions and boundaries of the College environment. Current and emerging technologies in College and more importantly, in many cases used outside the College by students, include (but are not limited to):

- Internet websites
- Virtual Learning Environments (Moodle)
- Instant messaging
- Social networking sites
- E-mails
- Blogs
- Podcasting
- Video broadcasting sites
- Chat rooms
- Gaming and gambling sites
- Music download sites
- Mobile phones with camera and video functionality
- Digital cameras
- Smart phones, iPads and Tablets with e-mail and web applications.

2. Aims of the Policy

2.1 To ensure that everyone who works and learns at the College achieves their full potential safely in an environment free from discrimination.

2.2 To have procedures that take account of an individual's right to education balanced by the risk to the College and its wider community.

2.3 To prepare students for the needs of today and their future working lives where the curriculum and their personal goals require them to learn how to locate, retrieve and exchange information using a variety of technologies.

2.4 To provide guidance on the safe and acceptable use of Online Technologies including social media communications, by students inside and outside of College.

3. Scope of Policy

3.1 This policy applies to all students irrespective of their method of application or enrolment or their type of study including those on further education, higher education (including programmes awarded by partner institutions), school links and apprenticeship programmes, studying either full-time or part-time, whilst attending a College centre, trip or at a College-approved placement.

3.2 This policy will apply to all College sites and all enrolment venues and programmes, regardless of location.

3.3 Any risks identified could relate to information / evidence arising prior to or at the time of enrolment, or arising post enrolment whilst studying at the College.

3.4 The policy also applies to use of social media and other communication platforms inside and outside the College.

4. Online Safety

4.1 The College has an Online Safety policy to protect students, staff and visitors. The policy recognises that Online Safety encompasses not only the Internet but any type of electronic communication, such as mobile phones and devices with wireless technology.

4.2 It is important for all students to understand the Internet is an unmanaged, open communications channel. Anyone can send messages, discuss ideas and publish material with no restriction. These features of the Internet make it an invaluable resource used by millions of people every day - however not all information is correct, accurate or valid. Students are advised to familiarise themselves with the Plagiarism, Copying and Cheating Policy which is available to download from our website, or in paper format from the Student guidance and Information Desk.

4.3 Students should be aware that publishing personal information could compromise your security and that of others. The 2018 revisions to the DfE statutory guidance 'Keeping Children Safe In Education' requires those working in education to act as follows:

> "Section *35. All school and college staff should be aware that* ***abuse, neglect and safeguarding issues are rarely standalone events*** *that can be covered by one definition or label. In most cases, multiple issues will overlap with one another.*
>
> *Section 36.* ***Abuse:*** *a form of maltreatment of a child. Somebody may abuse or neglect a child by inflicting harm or by failing to act to prevent harm. Children may be abused in a family or in an institutional or community setting by those known to them or, more rarely, by others (e.g. via the internet). They may be abused by an adult or adults or by another child or children (peer on peer abuse).*
>
> *Section 38.* ***Emotional abuse:*** *the persistent emotional maltreatment of a child such as to cause severe and adverse effects on the child's emotional development […] It may involve seeing or hearing the ill-treatment of another. It may involve serious bullying (including cyberbullying)"*
>
> *(Keeping Children Safe In Education, September 2018, section 35, 36 & 38)*

4.4 The College will continually make it clear to all students, staff and visitors that the use of College equipment for inappropriate reasons is unacceptable. The College will take reasonable actions and measures to protect all its users, including (although not limited to) disciplinary action. Please see MSR (Conduct) Policy for further information. **Students must** report to a tutor or a safeguarding officer if a member of staff attempts to communicate with them via social media.

5. Safeguarding

5.1 Radicalisation

5.1.1 Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism. Students must report to any member of staff if they view any extremist or radical views expressed online. Staff should report any concerns immediately to a member of the safeguarding team.

5.1.2 There is no single way of identifying an individual who is likely to be susceptible to an extremist ideology. It can happen in many different ways and settings. Specific background factors may contribute to vulnerability which are often combined with specific influences such as family, friends or online, and with specific needs for which an extremist or terrorist group may appear to provide an answer.

5.1.3 The Internet and the use of social media in particular has become a major factor in the radicalisation of young people.

5.1.4 *"Radicalised students can also act as a focal point for further radicalisation through personal contact with fellow students and through their social media activity. Where radicalisation happens off campus, the student concerned may well share his or her issues with other students. Changes in behaviour and outlook may be visible to staff. This guidance therefore addresses the need for institutions in receipt of public funding to self-assess and identify the level of risk, ensure all staff have access to training, and that there is welfare support for students and effective IT policies in place which ensure that these signs can be recognised and responded to appropriately".*

"Institutions must have clear policies in place for students and staff using IT equipment to research terrorism and counter terrorism in the course of their learning".
(Prevent Duty Guidance: for further education institutions in England and Wales 2015)

5.2 Child Sexual Exploitation

5.2.1 Child Sexual Exploitation (CSE) may involve utilising the Internet and Social Media to identify potential victims or as a tool to coerce and blackmail children into performing sexual acts, both on and offline.

5.2.2 Means of accessing the Internet may also be provided to children as a "gift" by perpetrators such as in the form of new mobile phones and devices. In some cases, CSE can take place entirely online such as children and young people being coerced into performing sexual acts via webcam/Social Media and therefore may not always result in a physical meeting between children and the offender.

5.2.3 "Section 39. **Sexual abuse**: involves forcing or enticing a child or young person to take part in sexual activities, not necessarily involving a high level of violence, whether or not the child is aware of what is happening. The activities may involve physical contact, including assault by penetration (for example rape or oral sex) or non-penetrative acts such as masturbation, kissing, rubbing and touching outside of clothing. They may also include non-contact activities, such as involving children in looking at, or in the production of, sexual images, watching sexual activities, encouraging children to behave in sexually inappropriate ways, or grooming a child in preparation for abuse (including via the internet). Sexual abuse is not solely perpetrated by adult males. Women can also commit acts of sexual abuse, as can other children."

(Keeping Children Safe In Education, September 2018, section 39)

5.3 Youth Produced Sexual Imagery and Sharing of Inappropriate Imagery

5.3.1 Youth Produced Sexual Imagery (YPSI – formerly known as 'Sexting') can be defined as 'an increasingly common activity among children and young people, where they share inappropriate or explicit images online'. This can include sharing indecent images of themselves or others via mobile phones, webcams, social media and instant messaging.

5.3.2 "Section *41. **All** staff should have an awareness of safeguarding issues. Staff should be aware that behaviours linked to the likes of drug taking, alcohol abuse, truanting and YPSI put children in danger."*

(Keeping Children Safe In Education, September 2018, section 41)

5.3.3 Although viewed by many young people as a 'normal' or 'mundane' activity and part of 'flirting', YPSI can be seen as harmless; but creating or sharing explicit images of a child is illegal, even if the person doing it is a child. A young person is breaking the law if they:

- take an explicit photo or video of themselves or a friend;
- share an explicit image or video of a child, even if it's shared between children of the same age;
- possess, download or store an explicit image or video of a child, even if the child gave their permission for it to be created.

5.3.4 *"Section 42. **All** staff should be aware safeguarding issues can manifest themselves via peer on peer abuse. This is most likely to include, but not limited to: bullying (including cyber bullying), gender based violence/sexual assaults and YPSI. Staff should be clear as to the school or college's policy and procedures with regards to peer on peer abuse."*

(Keeping Children Safe In Education, September 2018, section 42)

5.3.5 The College utilises the CEOP (Child Exploitation & Online Reporting Centre) reporting button, which is available on all student machines and the College website. The implementation of this button allows students to be empowered to report suspicious individuals or activity directly to law enforcement professionals quickly and easily.

6. Social media

6.1 Social media is a useful tool; the College understand that students communicate and collaborate via sites and apps on a regular basis and it is to be noted that there are merits to this. Students should familiarise themselves with and adhere to guidelines and etiquette as found in Appendix 2 of this document.

6.2 Unfortunately, there are also risks attached to the use of social media; everyone at the College is expected to use it responsibly, inside and outside of College premises. **Students must** immediately tell their tutor or safeguarding staff if they receive offensive or inappropriate messages whilst they are a student at the college. This includes messages sent to personal mobile phones or devices.

7. Accessing the Internet on College premises: Monitoring & Filtering

7.1 The Internet is available on all College systems to help students with their studies. Whilst it is essential that appropriate filters and monitoring processes are in place, the College recognises that 'over blocking' does not lead to reasonable restrictions and does not replace what young people are taught with regards to online safety and safeguarding. **Students must** immediately tell a lecturer or safeguarding officer if they think their network account has been tampered with.

7.2 All the websites visited and unencrypted online content are automatically logged by Internet monitoring software including Sonicwall and Fastvue. These software filters use advanced techniques such as URL Reputation and Automatic Image Recognition technology. In addition, it can also monitor Cloud application activity such as WhatsApp/ Facebook / Instagram and more. Both on College computers and on Wi-Fi.

7.3 As members of the Internet Watch Foundation (IWF), Sonicwall and Fastvue adhere to strict guidance in order to block access to illegal Child Abuse Images and Content (CAIC) and integrate the CITRU block-list (a police assessed list of unlawful terrorist content, produced on behalf of the Home Office).

7.4 Sonicwall may block access to some sites; if such a site is related to a student's normal working requirements please contact the ICT Helpdesk to arrange for the site to be reviewed and unblocked (where permissible).

7.5 Uploading and/or circulation of derogatory or defamatory comments and/or images about the College and/or its staff and/or students to any internet service (websites, social media, etc) is not permitted. Abuse of the Internet facilities will be seen as improper use of College equipment and will lead to disciplinary procedures (see Appendix 1).

7.6 The College has implemented content filters to prohibit access to the categories listed below. Any student found attempting to access inappropriate or harmful material will be subject to the College's MSR (Conduct) procedures. This list is updated regularly:

- Discrimination: Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age or sex
- Drugs/Substance abuse: Displays or promotes the illegal use of drugs or substances
- Extremism: Promotes terrorism and terrorist ideologies, violence or intolerance

- Malware/Hacking: Promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content
- Pornography: displays sexual acts or explicit images
- Piracy and copyright theft: Includes illegal provision of copyrighted material
- Self-Harm: Promotes or displays deliberate self-harm (including suicide and eating disorders)
- Violence: Displays or promotes the use of physical force intended to hurt or kill

N.B. This list is not exhaustive

8. Data Protection

8.1 The college will comply with the Data Protection Act 2018 and GDPR by ensuring that personal data is:

- Collected and processed lawfully, fairly and transparently for only specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

- Adequate, updated and relevant and not excessive for the purposes it was collected.

- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. Including not being transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

9. Confidentiality

9.1 The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR). The General Data Protection Regulation (GDPR) replaced the Data Protection Act 1998 in the UK. It is part of the wider package of reform to the data protection landscape that includes the Data Protection Bill. The GDPR sets out requirements for how organisations will need to handle personal data from 25 May 2018.

9.2 These are not only restrictions on disclosure of information about the College, they are bound by a common law duty of confidentiality. This duty prevents the College

from releasing information about staff and students, without their consent. This duty applies to manual records as well as information held on computers.

9.3 Information which must be treated as confidential includes the names and addresses of employees and students and any other information about them which is not publicly known aka “personal data”. Accordingly, to ensure that we do not breach our duty, no information, even if it only exists in printed form, should be disclosed unless all the relevant procedures have been followed.

9.4 Since 1 January 2005 people have the right, under the Freedom of Information Act 2000, to request any information held by a public authority which it has not already made available through its publication scheme. Please see the Freedom of Information -A guide to the publication scheme (January 2009), which is available on the College website, for more information.

10. Raising Awareness

10.1 Online safety awareness is delivered throughout the year, to all students in a range of ways including through Pastoral/Progress sessions which focus on Online Reputation, Exploitation, Online Gaming and Sleep Awareness. Targeted events such as ‘Safer Internet Week’ and ‘Stay Safe Week’ are promoted at a cross-college level with a range of activities, information and external professionals providing advice and guidance to both students and staff.

10.2 Students can access advice in regards to their online safety settings by speaking to their Library Learning Facilitator based in departmental LLC’s or by visiting the IT Helpdesk. Further guidance can be found from the websites listed below.

10.3 Students are expected to adopt an attitude of ‘collective responsibility’ towards online safety by encouraging others to stay safe and report any concerns to a member of College staff.

10.4 Regular training is provided for all staff in regards to online safety, safeguarding, sexual and criminal exploitation and radicalisation.

11. Other Relevant Procedures

11.1 Related College policies and procedures include:

- Maintaining Student Responsibility (Conduct) Policy and Procedures
- Maintaining Student Responsibility (Academic) Policy and Procedures
- Plagiarism, Copying and Cheating Policy
- Malpractice Policy
- Safeguarding Policy and Procedures
- Equality and Diversity Policy
- Data Protection Policy

12. Relevant Sources of Information

12.1 Relevant documents include:

- DfES 'Keeping Children Safe in Education' (September 2018)
- Working Together to Safeguard Children - A guide to inter-agency working to safeguard and promote the welfare of children (July 2018)
- UKCCIS 'YPSI in Schools and Colleges' (updated January 2017)
- HM Government 'Prevent Duty Guidance: for further education institutions in England and Wales '(2015)
- South West Grid for Learning 'So You Got Naked Online?'(2016)
- NICE 'Harmful Sexual Behaviour Amongst Children and Young People' (Sept 2016)

12.2 Useful websites include:

- Child Exploitation and Online Protection Centre http://www.ceop.police.uk/
- UK Safer Internet Centre http://www.saferinternet.org.uk/
- CEOP's Think You Know http://www.thinkuknow.co.uk/
- Safer Internet Centre Social Network Checklists www.saferinternet.org.uk/checklists
- Get It Right From a Genuine Site http://www.getitrightfromagenuinesite.org/
- Net Aware http://www.net-aware.org.uk/
- Internet Watch Foundation http://www.iwf.org.uk/

Appendix 1

Activity deemed inappropriate which may lead to disciplinary proceedings under the College MSR (Conduct) procedure

Gross Misconduct

- Bullying, including cyber-bullying i.e. any form of bullying which takes place online or through smartphones and tablets
- Wilful damage to College property including;
    - Malicious attacks on the network.
    - Distributing malware.
    - Physical Damage to computer equipment around college i.e re-arranging letters on keyboards, graffiti or Damage to computer screens, etc.
- Downloading, storing, transmitting or viewing pornographic or offensive material.
- Capturing, possessing and/or circulating inappropriate material.
- Bringing the College into disrepute.
- Inciting others to carry out acts of misconduct or gross misconduct.
- Spreading or publishing radicalised / intolerant views or materials.
- Violating any part of the Computer Misuse Act 1990.

Misconduct

- Misuse of the computer network i.e. chat lines/social networking sites, use of another students password, inappropriate use of the internet
- Failure to return equipment

N.B. This list is not exhaustive

Appendix 2

We must all adhere to the following guidelines when accessing social media sites and apps

- Use of sexually explicit language or viewing, creation or sharing of sexually explicit imagery is not permitted nor advised from a safeguarding perspective.
- Verbally abusive, intolerant or threatening language is strictly prohibited.
- Use of racist or extremist language which would directly contravene British or College values, is not permitted.
- Use of social media for radicalisation or the expression of extremist views is not permitted.
- Communication with staff unless on a College controlled platform is not permitted. Any such communication instigated by staff members to a student's personal social media must be reported to safeguarding team.

Please be mindful of the following when using social media:

- Avoid posting anything on social media that you wouldn't want others to see. Remember what you post could impact on your future career.
- Don't be pressured into doing anything inappropriate on social media like posting photos or videos. **You must** report any requests you receive through social media to post sexually explicit or offensive imagery online, to your tutor or safeguarding staff.
- Beware of accepting people as friends or engaging in conversations on social media if you don't know the people you are communicating with
- Exercise caution when accessing personal social media platforms in a public environment, e.g. a classroom or library.
- Set any personal social media profiles to "private" to ensure control over who is able to access / view your information.
- Ensure your behaviour online cannot be conceived as detrimental to the College or its reputation.
- Be security conscious and take steps to protect yourself from identity theft, this can be achieved by restricting the amount of personal information given out on Social Media platforms. These platforms allow people to post detailed personal information such as date of birth, place of birth and favourite football team. These are often the answers to security questions and parts of passwords.
- Change your social media password often. The ICT Helpdesk or LLC Facilitators can provide advice concerning password security if required.