Policy/Procedure/Guideline Review

Policy/Procedure/ Guideline:	E-Safety Policy
Senior Manager Responsible:	Vice Principal, Chief Information Officer
Author:	Vice Principal, Chief Information Officer/ Safeguarding and Prevent Manager
Approved By:	Board
Date Approved:	Board - 26th February 2024 (Reviewed and approved by SLT 30th January 2024
Next Review Date:	22nd January 2025
Publication:	Staff Hub NCCG Website
Changes Made:	Changes in KCSIE 2023 implemented, including filtering and monitoring requirements Organisational changes Legislative/Quality Framework updated

E-Safety Policy

1. Introduction

1.1 We recognise the benefits and opportunities that new technologies have to offer to teaching, learning and personal development. The College has an approach whereby we implement safeguards in the college and support staff and students to both identify and manage risks. We achieve this by implementing guidance, training and security measures. We will ensure that all learners are safe in accordance to Keeping Children Safe in Education. The e-safety policy should be read in conjunction with other relevant policies.

2. Purpose

2.1 An effective e-safety policy is one that provides clear direction to staff and others about expected codes of behaviour, security procedures and risk assessment in dealing with e-safety issues. An effective policy also makes explicit the college commitment to the development of good practice and sound procedures.

3. Legislative/Quality Framework

3.1 College should be aware of the legislative framework under which this Online Safety Policy and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online. It is recommended that legal advice is sought in the advent of an e safety issue or situation.

- Computer Misuse Act 1990
- Data Protection Act 1998
- Freedom of Information Act 2000
- Communications Act 2003
- Malicious Communications Act 1988
- Regulation of Investigatory Powers Act 2000
- Trade Marks Act 1994
- Copyright, Designs and Patents Act 1988
- Telecommunications Act 1984
- Criminal Justice & Public Order Act 1994
- Racial and Religious Hatred Act 2006
- Protection from Harassment Act 1997
- Protection of Children Act 1978

- Sexual Offences Act 2003
- Public Order Act 1986
- Obscene Publications Act 1959 and 1964

- Human Rights Act 1998
- The Education and Inspections Act 2006
- The Education and Inspections Act 2011
- Keeping Children Safe in Education 2023
- The Protection of Freedoms Act 2012
- The School Information Regulations 2012
- SeriousCrimeAct2015

4. Scope

4.1 This policy applies to all members of the College community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of College digital technology systems, both in and out of the College.

The Education and Inspections Act 2006 empowers Principals to such extent as is reasonable, to regulate the behaviour of students when they are off the College site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other Online Safety incidents covered by this policy, which may take place outside of the College but is linked to membership of the College. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data.

The College deal with such incidents within this policy and associated behaviour and antibullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out College.

5. Roles and Responsibilities

5.1 Governors / Board of Directors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents in the Safeguarding Reports. A member of the Governing Body / Board will take on the role of Online Safety Governor this will be a combined role with that of the Child Protection / Safeguarding Governor. The role of the Online Safety Governor will include:

- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors / Board / Committee

5.2 Principal and Senior Leaders

- The Principal has a duty of care for ensuring the safety (including online safety) of members of the College community, though the day to day responsibility for online safety will be delegated to the Safeguarding and Prevent Manager
- The Principal, Deputy Principal Curriculum and Quality and Human Resources Manager should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Principal / Senior Leadership Team are responsible for ensuring that the Safeguarding and Prevent Manager and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Principal / Senior Leadership Team will ensure that there is a system in place to allow for filtering and monitoring and support of those in College who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Safeguarding and Prevent Manager in the safeguarding and Prevent report

5.3 Operational lead for Online Safety by – Safeguarding and Prevent Manager

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the college online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with College technical staff
- receives reports of online safety incidents via College filtering and monitoring systems, creates a log of incidents to inform future online safety developments,
- meets regularly with SLT who discuss current issues, review incident logs and filtering / change control logs with the Online Safety Governor
- reports regularly to Senior Leadership Team

5.4 Chief Information Officer

- that the College's technical infrastructure is secure and is not open to misuse or malicious attack
- that the College meets required online safety technical requirements

- that users may only access the networks and devices through a properly enforced password protection policy
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of college devices and services in scope of responsibility are reported upon and any misuse / attempted misuse be reported to the Principal / Senior Leader; Online Safety Lead investigation / action / sanction
- that relevant software and systems are implemented and updated to comply with relevant safeguarding legislation and best practice, and assistance is given in the choice of systems procured.
- that appropriate filtering and monitoring systems are in place

5.5 Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current College Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Online Safety Lead for investigation / action / sanction
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official college systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the Online Safety Policy and acceptable use policies
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- with appropriate filtering and software systems, they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other College activities (where allowed) and implement current policies with regard to these devices.
- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

5.6 Designated Safeguarding Lead / Deputy Safeguarding Lead and Safeguarding Team

Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- online-bullying

5.7 Online Safety Group (Safeguarding and Prevent Committee)

The Online Safety Group provides a consultative group that has wide representation from the College community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. This group is opted into the Safeguarding and Prevent Committee group and attends on a termly basis to provide regular reports.

The Terms of reference for the online safety group are as follows:

- the production / review / monitoring of the College Online Safety Policy / documents.
- mapping and reviewing the online safety / digital literacy curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the students about the online safety provision
- monitoring improvement actions identified

5.8 Students:

- are responsible for using the College digital technology systems in accordance with the Student Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of College and realise that the College Online Safety Policy covers their actions out of College, if related to their membership of the College

5.9 Parents / Carers

Parents / Carers play a crucial role in ensuring that their children/vulnerable adult understand the need to use the internet / mobile devices in an appropriate way. The College will take opportunities to help parents / Carers understand these issues. Parents / Carers will be encouraged to support the College in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at college events
- access to parents' sections of the website / Learning Platform and on-line student records • their children's personal devices in College

5.10 Community Users

Community Users who access College systems / website / Learning Platform as part of the wider College provision will be expected to use the College digital technology systems and the Community technology systems in accordance with the Student Acceptable Use Agreement.

6. Reporting a Concern

6.1 Dealing with unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from College and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a College context, either because of the age of the users or the nature of those activities.

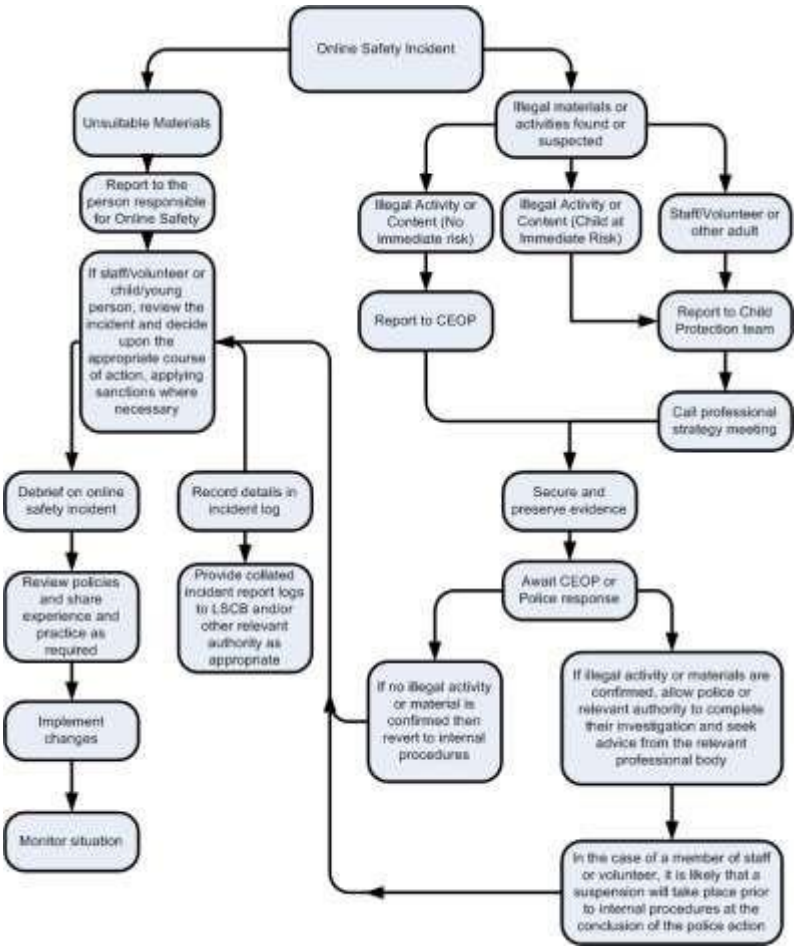
The College believes that the activities referred to in the following section would be inappropriate in a College context and that users, as defined below, should not engage in these activities in / or outside the College when using College equipment or systems. The College policy restricts usage as follows:

6.2 Illegal Incidents

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the college or brings the college into disrepute				X	
Using College systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the College					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)			X			
On-line gaming (non-educational)			X			
On-line gambling					X	
On-line shopping / commerce			X			
File sharing		X				
Use of social media			X			
Use of messaging apps			X			
Use of video broadcasting e.g. Youtube			X			

Safeguarding and Prevent Manager (Online Safety Lead) will:

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



6.3 Other Incidents

It is hoped that all members of the College community will be responsible users of digital technologies, who understand and follow College policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Report the incident to the E-Safety Lead following the Safeguarding Procedure.

The Safeguarding Team will ensure:

- Have more than one College manager been involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following: Internal response or discipline procedures /Involvement by Local Authority / Academy Group or national / local organisation (as relevant). Police involvement and/or action
- **If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**

  ○ incidents of 'grooming' behaviour ○ the sending of obscene materials to a child ○ adult material which potentially breaches the Obscene Publications Act ○ criminally racist material ○ promotion of terrorism or extremism ○ other criminal conduct, activity or materials

- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the College and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

6.4 College Actions & Sanctions

It is more likely that the College will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the College community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with

through normal behaviour / disciplinary procedures. All Illegal incidents must be reported to the Safeguarding Team.

7. Information Sharing

7.1 The College adopts the information sharing protocols recommended in local and national guidance. Any requests for information sharing will be considered by the Designated Safeguarding Lead or Deputies who will comply with relevant guidance and college policies and procedure.

8. Dissemination

8.1 Nelson and Colne College Extranet and Accrington and Rossendale Intranet

8.2 Nelson and Colne College, Lancashire Adult Learning and Accrington and Rossendale College Moodle

8.3 Nelson and Colne College, Lancashire Adult Learning and Accrington and Rossendale College Website

9. Monitoring and Review

9.1 The policy will be reviewed annually by Vice Principal : Chief Information Officer.

10. Management Responsibility

10.1 Deputy Principal Curriculum and Quality has overall management responsibility for this policy. Day to day management responsibility for this policy has been devolved to the Safeguarding and Prevent Manager with support from the Director of Learner Services and Chief Information Officer.

11. Related Policies/Procedures

- Bullying and Harassment policy
- Acceptable Use of IT Policy
- Behaviour Policy
- Whistleblowing procedure
- Social media policy
- Staff Code of Conduct
- Disciplinary Policy

- Safeguarding Children and Vulnerable Adults Policy and Procedures

12. Appendices

12.1 Legislation

Computer Misuse Act 1990 This
Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The college reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or

- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harrassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the college context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion

- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The college is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Principals, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the college site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Principals (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.
http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screeningsearching-and-confiscation)

Keeping Children Safe in Education 2019

This is statutory guidance from the department of education issued under section 175 of the education act. Schools and colleges in England must have regard to it when carrying out their duties to safeguard and promote the welfare of children.

The Protection of Freedoms Act 2012

Requires coleges to seek permission from a parent / carer to use Biometric systems

The School Information Regulations 2012

Requires schools/colleges to publish certain information on its website:

https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

12.2 **Links to supporting documents**

UK Safer Internet Centre

Safer Internet Centre – https://www.saferinternet.org.uk/
South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/
Childnet – http://www.childnet-int.org/
Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline Internet Watch Foundation - https://www.iwf.org.uk/

CEOP

CEOP - http://ceop.police.uk/
ThinkUKnow - https://www.thinkuknow.co.uk/

Others

LGfL – Online Safety Resources

Kent – Online Safety Resources page

INSAFE / Better Internet for Kids - https://www.betterinternetforkids.eu/

UK Council for Child Internet Safety (UKCCIS) - www.education.gov.uk/ukccis

Netsmartz - http://www.netsmartz.org/

Tools for Schools and Colleges

Online Safety BOOST – https://boost.swgfl.org.uk/

360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/

360Data – online data protection self review tool: www.360data.org.uk

Bullying / Online-bullying / Sexting / Sexual Harrassment

Enable – European Anti Bullying programme and resources (UK coordination / participation through SWGfL & Diana Awards) - http://enable.eun.org/

Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/

Scottish Government - Better relationships, better learning, better behaviour - http://www.scotland.gov.uk/Publications/2013/03/7388

DfE - Cyberbullying guidance - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Childnet – Cyberbullying guidance and practical PSHE toolkit: http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit

Childnet – Project deSHAME – Online Sexual Harrassment

UKSIC – Sexting Resources

Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm

Ditch the Label – Online Bullying Charity Diana Award – Anti-Bullying Campaign

Social Networking

Digizen – Social Networking

UKSIC - Safety Features on Social Networks

Curriculum

SWGfL Digital Literacy & Citizenship curriculum

UKCCIS – Education for a connected world framework

Teach Today – www.teachtoday.eu/

Insafe - Education Resources

Mobile Devices / BYOD

Cloudlearn Report Effective practice for schools moving to end locking and blocking

NEN - Guidance Note - BYOD

Data Protection

360data - free questionnaire and data protection self review tool

ICO Guide for Organisations (general information about Data Protection)

ICO Guides for Education (wide range of sector specific guides)

DfE advice on Cloud software services and the Data Protection Act

ICO Guidance on Bring Your Own Device

ICO Guidance on Cloud Computing

ICO - Guidance we gave to schools - September 2012

IRMS - Records Management Toolkit for Schools

NHS - Caldicott Principles (information that must be released)

ICO Guidance on taking photos in schools

Dotkumo - Best practice guide to using photos

Children's Commissioner, TES and Schillings – Young peoples' rights on social media

Professional Standards / Staff Training

DfE – Keeping Children Safe in Education

DfE - Safer Working Practice for Adults who Work with Children and Young People

Childnet – School Pack for Online Safety Awareness

UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure / Technical Support

UKSIC – Appropriate Filtering and Monitoring

Somerset - Questions for Technical Support

NEN – Advice and Guidance Notes

Working with parents and carers

SWGfL Digital Literacy & Citizenship curriculum

Online Safety BOOST Presentations - parent's presentation

Vodafone Digital Parents Magazine

Childnet Webpages for Parents & Carers

Get Safe Online - resources for parents

Teach Today - resources for parents workshops / education

The Digital Universe of Your Children - animated videos for parents (Insafe)

Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide

Insafe - A guide for parents - education and the new media

Research

EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011

Futurelab - "Digital participation - its not chalk and talk any more!"

Ofcom –Media Literacy Research