Online Safety Policy 2025-2027

Author:	**Name**	Stephen Musa	
	Job Title	Deputy Principal (DSL)	
Date policy reviewed:	19.08.25	**Date policy to be reviewed:**	19.08.25
Equality Impact assessed by:	Stephen Musa	**Date impact assessed:**	September 2025
GDPR Impact assessed by:	Stephen Musa	**Date impact assessed:**	September 2025
Policy approved by:	SLT	**Date approved:**	September 2025

Contents

1. Introduction

The purpose of this policy is to establish the ground rules we have in Southport College and KGV Sixth Form College for the use of computing, mobile and new technologies including social media.

The College has a duty of care to safeguard all its stakeholders including staff, learners and visitors and is committed to providing a safe environment for study and work.

Computer skills are vital to access employment and life-long learning. However, technologies can present risks to vulnerable groups as well as benefits. Internet use for education, work, home, social and leisure activities is expanding across all sectors of society. This brings staff and learners into contact with a wide variety of influences, some of which may be unsuitable. The College will make every effort to ensure that learners are given every opportunity to access online content in order to study, providing it can ensure its safeguarding commitment to the whole College community.

All College staff should be aware that technology is a significant component in many safeguarding and wellbeing issues. Learners are at risk of abuse online as well as face to face. In many cases abuse will take place concurrently via online channels and in daily life. Learners can also abuse their peers online, this can take the form of abusive, harassing, and misogynistic messages, the sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography.

2. Scope

2.1 This policy applies to all members of the College community (including staff, learners, governors, volunteers, parents and carers, visitors, community users and those working in or on behalf of the college) who have access to and are users of College digital systems, both in and out of the College. It also applies to the use of personal digital technology on site.

2.2 This Online Safety Policy outlines our commitment to safeguard members of our College community online in accordance with statutory guidance and best practice. This policy has been produced using the legislative framework outlined in the attached 'Legislation' appendix.

2.3 College will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that takes place out of College.

3. Policy and Leadership

Online safety is a whole College responsibility; the following sections outline the online safety roles and responsibilities of individuals and groups within the College

Senior Leadership Team (SLT)

3.1 The CEO has a duty of care for ensuring the safety (including online safety) of members of the College community and fostering a culture of safeguarding though day-to-day responsibility for online safety is held by the Designated Safeguarding Lead as defined in Keeping Children Safe in Education.

3.2 The SLT and Designated Safeguarding Lead are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of the college community.

3.3 SLT are responsible for ensuring that the Online Safety Lead, technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.

3.4 SLT will ensure that there is a system in place to allow for monitoring and filtering of internal online activity.

3.5 SLT will support the safeguarding team in carrying out the internal online safety monitoring role.

3.6 SLT will receive regular monitoring reports from the Online Safety Lead though termly Governor's report.

Governors

3.7 Governors are responsible for the approval of the Online Safety Policy. Online safety updates will be provided to the Standard Committee as part of the semesterly Safeguarding update report which in turn, will review the effectiveness of the policy. The report will include information about online safety incidents and monitoring. The role of the Online Safety Governor includes:

- Attending the college's Safeguarding Committee meetings
- Provide support and challenge to the Online Safety Lead
- checking that Online Safety Policy is fit for purpose
- reporting to the Governing Body regarding online safety

3.8 The governing body will support the College in encouraging parents/carers and the wider community to become engaged in online safety activities.

3.9 Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/online safety/health and safety/safeguarding. This would include cyber-security training and training to allow the governor to understand the College's filtering and monitoring provision in order that they can participate in the required checks and reviews.

Online Safety Lead

3.10 The Online Safety Lead for Southport College and KGV Sixth Form College is –

Stephen Musa (Designated Safeguarding Lead).

3.11 The Deputy Online Safety Leads for the Southport College and KGV Sixth Form College are – Liz Jones and Karen Marsh (Deputy Safeguarding Leads).

3.12 The Online Safety Lead and the Deputy Safety Leads will:

- Lead the Safeguarding Committee Group, where Online safety is a key agenda item.
- take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns.
- have a leading role in establishing and reviewing the College online safety policies.
- promote an awareness of and commitment to online safety education / awareness raising.
- provide (or identify sources of) training and advice for staff/ governors/ parents/ carers/ learners

3.13 Liaise with curriculum leaders to ensure that online safety curriculum is planned, mapped, embedded and evaluated.

- Ensure that staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents.
- Receive regularly updated training to allow them to understand how digital technologies are used and evolving (particularly by learners) with regard to the areas defined in Keeping Children Safe in Education; content, contact, conduct, commerce.

Designated Safeguarding Lead (DSL)

3.14 The Designated Safeguarding Lead should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate online contact with adults/strangers
- Potential or actual incidents of grooming
- Cyber crime
- Online bullying

4. Online Safety Group

The Online Safety Group (as part of the Safeguarding Committee) provides a consultative group that has wide representation from the College community, with responsibility for issues regarding online safety and monitoring the Online Safety Policy including the impact of initiatives.

The Online Safety Group has the following members:

- Designated Safeguarding Lead
- Online Safety Lead
- Senior Leaders
- Safeguarding Governor
- Technical staff
- Assistant Principal Learner Development and Careers (also presenting learner voice feedback)

Participants of the Safeguarding Committee will assist the Safeguarding Team with:

- The production/review/monitoring of the College Online Safety Policy
- The production/review/monitoring of the school filtering policy and requests for filtering changes
- Mapping and reviewing the online safety education provision
- Reviewing network/filtering/monitoring/incident logs, where possible
- Encouraging the contribution of learners to staff awareness, emerging trends and the College online safety provision
- Consulting stakeholders – including staff/parents/carers about the online safety provision

5. Curriculum and Staff

5.1 Progress coordinator and Head of Divisions will work with the Online Safety Lead to develop a planned and coordinated online safety education programme that are matched to need; are age related and build on prior learning. The online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.
This will be provided through:

- Themed progress sessions
- A mapped cross-curricular programme
- Bespoke sessions for targeted groups
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

5.2 Staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current College Online Safety Policy and practices.
- they understand that online safety is a core part of safeguarding.
- There is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc.
- users should immediately report to their line manager/safeguarding team the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- they have read, understood, and signed the staff acceptable use agreement (AUA)
- they immediately report any suspected misuse or problem to the safeguarding team for investigation/action, in line with the College safeguarding procedures.
- all digital communications with learners and parents/carers should be on a professional level and only carried out using official College systems, such as college email or Microsoft Teams.
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements. Where staff used AI, they should only use College-approved AI services (Copilot) for work purposes which have been evaluated to comply with organizational security and oversight requirements.

- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons, including the use of AI systems.
- in lessons where internet use is pre-planned learners 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.
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- Ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They model safe responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.
- They ahere to the College's technical security policy, with regard to the use of devices, systems and passwords and have an understanding of how the learners in their care use digital technologies out of College, in order to be aware of online safety issues that may develop from the use of those technologies.
- They are aware of the benefits and risks of the use of the use of Artificial Intelligence (AI) services in school, being transparent in how they use these services, prioritizing human oversight. AI should assist, not replace, human decision-making Staff must ensure that final judgements, particularly those affecting people, are made by humans, fact-checked and critically evaluated.
- it is accepted that from time to time, for good educational reasons, learners may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need
    - they model safe, responsible, and professional online behaviours in their own use of technology, including out of College and in their use of social media. Please refer to the college's Social Media policy.

When using communication technologies, the College considers the following as good practice:

- any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. Personal e-mail addresses, text messaging or social media must not be used for these communications.
- staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the College and its community.

5.3 Staff, learners and community users MUST report if they view any extremist or radical views expressed online to the safeguarding team immediately. All student incidents should be recorded on ProMonitor. Further information on The Prevent Duty can be found within the Safeguarding Policy.

Head of IT/technical staff

5.4 The Head of IT and technical staff are responsible for ensuring that:

- they are aware of and follow the College Online Safety Policy to carry out their work effectively in line with College policy.
- the College technical infrastructure is secure and is not open to misuse or malicious attack.
- there is clear, safe, and managed control of user access to networks and devices.
- The College meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & College and guidance from the local authority.
- There is clear, safe, and managed control of user access to networks and devices.
- 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.
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the safeguarding team for investigation and action.
- the filtering systems are applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- monitoring software/systems are implemented and regularly updated.

6. Learners, Parents and Carers

- are responsible for using the College digital technology systems in accordance with the acceptable use agreement and Online Safety Policy, including personal devices where allowed.
- any reports of abuse, misuse or access to inappropriate materials should be urgently reported to members of College staff and/or the safeguarding team
- if a student or someone they know feels vulnerable when using online technology they should reports concerns to College staff.
- Should avoid plagiarism and uphold copyright regulations, taking care when using Artificial Intelligence (AI) services to protect the intellectual property of themselves and others and checking the accuracy of content accessed through AI services.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the College's Online Safety Policy covers their actions out of College, if related to their membership of the College.

Contribution of Learners:

6.1 The College acknowledges, learns from, and uses the skills and knowledge of learners in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the College community and how this contributes positively to the personal development of young people. Their contribution is recognised through:

- mechanisms to canvass student feedback and opinion, including learner voice which can allow learners to contribute to the online safety education programme.
- learners designing/updating acceptable use agreements
- contributing to online safety events with the wider College community.

Parents and carers

6.2 Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way. The College will take every opportunity to help parents and carers understand these issues through:

- publishing the College Online Safety Policy on the College website
- publishing information about appropriate use of social media.

Parents and carers will be encouraged to support the College in:

- reinforcing the online safety messages provided to learners in College
- the safe and responsible use of their children's personal devices in the College (where this is allowed).

7. Those working in or on behalf of the college

7.1 Those working in or on behalf of the college who access College systems/website/learning platform as part of the wider College provision will be expected to sign a community user AUA before being provided with access to College systems.

The College encourages the engagement of agencies/members of the community who can provide valuable contributions to the online safety provision and actively seeks to share its knowledge and good practice with other Colleges and the community.

8. Filtering

8.1 The Internet is available on all College systems to assist learners with their studies. Whilst it is essential that appropriate filters and monitoring processes are in place, The College recognises that 'over blocking' does not replace what learners are taught regarding online safety and safeguarding.

8.2 Filtering is preventative. It refers to solutions that protect users from accessing illegal, inappropriate and potentially harmful content online.

8.3 The College filtering policies are agreed by senior leaders and technical staff and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours.

8.4 The College manages access to content across its systems for all users. The filtering provided meets the standards defined in the DfE Filtering Standards for schools and colleges and the guidance provided in the UK Safer Internet Centre.

8.5 Access to online content and services is managed for all users.

8.6 Abuse of the network will be seen as improper use of College equipment and will lead to disciplinary procedures.

9. Monitoring

9.1 The College has monitoring systems in place to protect the College, systems and users:

- The College monitors all network use across all its devices and services.
- Users are aware that the network is monitored. The Online Safety Lead is responsible for managing the monitoring processes and the IT service provider will have technical responsibility.
- Monitoring reports are urgently picked up within College hours, acted on and outcomes are recorded by the safeguarding team.
- Devices that are provided by the College have College-based monitoring applied irrespective of their location.
- Abuse/misuse should be reported using College Safeguarding and MSR Conduct procedures.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.
- Technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon.

10. Mobile technologies and Personal devices

10.1 Mobile technology devices may be College owned/provided or personally owned and might include smartphone, tablet, wearable devices, notebook/laptop or other technology that usually has the capability of utilising the College's wireless network.

- all learners, staff and visitors are permitted to use personal mobile devices in College
- all users should understand that the primary purpose of the use of mobile/personal devices in a College context is educational
- No technical support is available for personal devices
- filtering of the internet connection to these devices is monitored
- taking/storage/use of images of learners is not permitted
- the College will take not responsibility liability for loss/damage or malfunction following access to the network
- misuse of personal devises will be dealt with under MSR Conduct procedures/Safeguarding procedures.

11. Social Media

11.1 With widespread use of social media for professional and personal purposes this policy sets out clear guidance for staff to manage risk and behaviour online.

11.2 All staff work within a position of trust and their conduct should reflect this.

11.3 The College provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:

- Social Media policy
- ensuring that personal information is not published
- Acceptable use agreements for staff, learners and community workers.
- Education will be provided on acceptable use, social media risks, checking of settings and

reporting issues.

College staff should ensure that:

- they do not engage in online discussion on personal matters relating to members of the College community
- personal opinions should not be attributed to the College
- security settings on personal social media profiles are regularly checked to minimize risk of loss of personal information
- they act as positive role models in their use of social media

Monitoring of public social media

- As part of active social media engagement, the College will pro-actively monitor the Internet for public postings about the College
- when parents/carers express concerns about the College on social media we will urge them to make direct contact with the College, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the College's complaints procedure.

12. Safeguarding

12.1 The internet and other digital and information technologies can put learners at risk within and outside the College. An effective whole College approach to online safety empowers us to protect and educate learners and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

12.2 The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk as outlined within KCSIE 2023:

content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and

commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

13. Cyber Crimes

13.1 Cyber criminals seek to exploit human or security vulnerabilities in order to steal passwords, data or money directly. The most common cyber threats include:

- Hacking - including of social media and email passwords

- Phishing - bogus emails asking for security information and personal details
- Malicious software – including ransomware through which criminals hijack files and hold them to ransom
- Distributed denial of service (DDOS) attacks against websites – often accompanied by extortion

13.2 Children and vulnerable adults can be exploited by Organised Crime Groups to carryout cyber-crimes. The main identified common pathway by Merseyside Police into cybercrime is through online gaming. Offenders often begin to participate in gaming cheating and 'modding' forums and progress to criminal hacking forums. Targeted interventions at a young age can lead to positive outcomes, any at risk learners can be referred for specialist support through our safeguarding team.

14. The use of Artificial Intelligence (AI) systems in College

As Generative Artificial Intelligence (gen AI) continues to advance and influence the world we live in, it's role in education is also evolving. There are currently 3 key dimensions of AI use in schools : learner support, tutor support and College operations; ensuring all use is safe, ethical and responsible is essential.

There are risks involved in the use of Gen AI services, but these can be mitigated through our existing policies and procedures, amending these as necessary to address the risks.

Staff and learners will be educated about safe and ethical use of AI, preparing them for a future in which these technologies are likely to play an increasing role.

- The College acknowledges the potential benefits of the use of AI in an educational context - including enhancing learning and teaching, improving outcomes, improving administrative processes, reducing workload and preparing staff and learners for a future in which AI technology will be an integral part. Staff are encouraged to use AI based tools to support their work where appropriate, within the frameworks provided below and are required to be professionally responsible and accountable for this area of their work.
- College will comply with all relevant legislation and guidance, with reference to guidance contained in Keeping Children Safe in Education and UK GDPR.
- Relevant training will be provided for staff and governors in the advantages, use of and potential risks of AI. We will support staff in identifying training and development needs to enable relevant opportunities.
- College will seek to embed learning about AI as appropriate in our curriculum offer, including supporting learners to understand how gen AI works, its potential benefits, risks, and ethical and social impacts. The school recognises the importance of equipping learners with the knowledge, skills and strategies to engage responsibly with AI tools..
- As set out in the staff acceptable use agreement, staff will be supported to use AI tools responsibly, ensuring the protection of both personal and sensitive data. Staff should only input anonymised data to avoid the exposure of personally identifiable or sensitive information.
- Staff will always ensure AI tools used comply with UK GDPR and other data protection regulations. They must verify that tools meet data security standards before using them for work related to the school.
- Only those AI technologies approved by the College may be used. Staff should always use

College-provided AI accounts for work purposes. These accounts are configured to comply with organisational security and oversight requirements, reducing the risk of data breaches.

- We will protect sensitive information. Staff must not input sensitive information, such as internal documents or strategic plans, into third-party AI tools unless explicitly vetted for that purpose. They must always recognise and safeguard sensitive data.
- The College will ensure that when AI is used, it will not infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.
- AI incidents must be reported promptly. Staff must report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately to the relevant internal teams. Quick reporting helps mitigate risks and facilitates a prompt response.

15. Reporting and Responding

15.1 The College will take all reasonable precautions to ensure online safety for all users but recognises that incidents may occur inside and outside of the College (with impact on the College) which will need intervention. The College will ensure:

- there are clear reporting routes which are understood and followed by all members of the College community which are consistent with the College safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- all members of the College community will be made aware of the need to report online safety issues/incidents, including logging all learner concerns on Promonitor.
- reports will be dealt with as soon as is practically possible once they are received
- staff have appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm, the incident must be escalated through College safeguarding procedures. This may include:
    - Non-consensual images
    - Self-generated images
    - Terrorism/extremism
    - Hate crime/abuse
    - Fraud and extortion
    - Harassment/stalking
    - Child Sexual Abuse Material (CSAM)
    - Child Sexual Exploitation Grooming
    - Extreme Pornography
    - Sale of illegal materials/substances
    - Cyber or hacking offences under the Computer Misuse Act
    - Copyright theft or piracy
- It is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- There are support strategies in place for those reporting or affected by an online safety incident
- Incidents will be logged on a students individual learning plan (Promonitor)
- Relevant staff are aware of external sources of support and guidance in dealing with

online safety issues eg. Local authority, police, CEOP etc.

- Those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions.
- The flowchart is attached for staff to support the decision-making process for dealing with online safety incidents.

College actions

15.2 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 our Positive Behaviour Policy and/or safeguarding procedures.

15.3 The impact of the Online Safety Policy and practice is regularly evaluated through the review of termly safeguarding reports; behaviour/bullying reports, surveys of staff, learners etc.

15.4 There is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work eg. Online safety education, awareness and training.

15.5 There is a well-established route to regularly report patterns of online safety incidents and outcomes to College leadership and Governors.

15.6 Parents/carers are informed of patterns of online safety incidents as part of the schools online safety awareness raising.

15.7 Online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate.

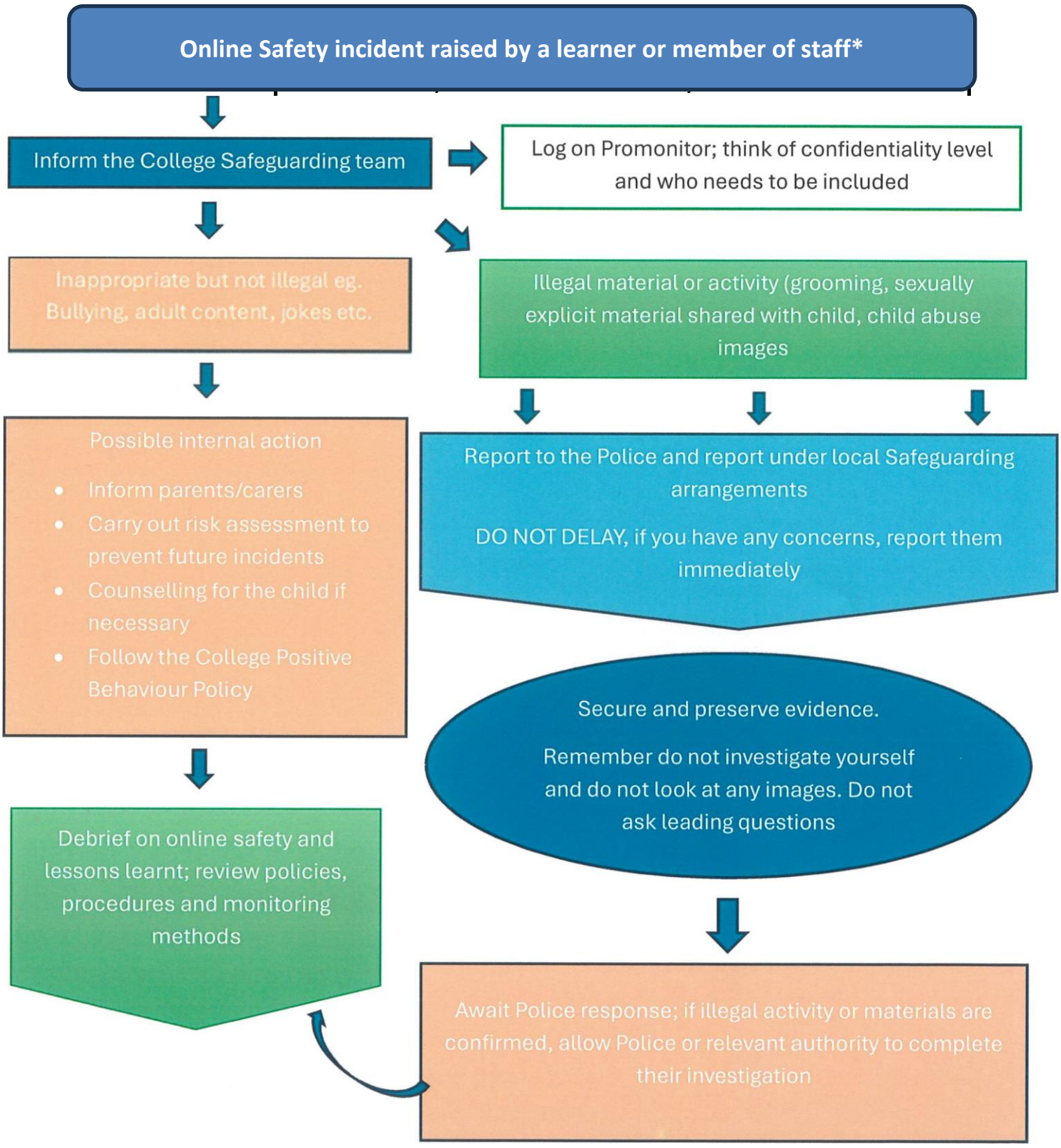
15.8 The evidence of impact is shared with other Colleges and agencies to help ensure the development of a consistent and effective local online safety strategy.

15.9 The impact of this Online Safety Policy and practice is regularly evaluated through reviewing online safety reports; behaviour/bullying reports and learner voice. Online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these revies, local themes/trends and best practice.

Data Protection

15.10 Personal data will be recorded, processed, transferred and made available according to the current data protection legislation, following our Data Protection Policy.

Online Safety Flowchart



*In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to the Police, whilst Police and internal procedures are being undertaken. The LADO also needs to be contacted and a referral made.

16 Appendix - Legislation

A useful summary of relevant legislation can be found at: Report Harmful Content: Laws about harmful behaviours

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.

Colleges may wish to view the National Crime Agency website which includes information about "Cyber crime – preventing young people from getting involved". Each region in England (& Wales) has a Regional Organised Crime Unit (ROCU) Cyber-Prevent team that works with Colleges to encourage young people to make positive use of their cyber skills. There is a useful summary of the Act on the NCA site.

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.

The Data Protection Act 2018:

Updates the 1998 Act, incorporates the General Data Protection Regulations (GDPR) and aims to:

- Facilitate the secure transfer of information within the European Union.
- Prevent people or organisations from holding and using inaccurate information on individuals. This applies to information regarding both private lives or business.
- Give the public confidence about how businesses can use their personal information.
- Provide data subjects with the legal right to check the information businesses hold about them. They can also request for the data controller to destroy it.
- Give data subjects greater control over how data controllers handle their data.
- Place emphasis on accountability. This requires businesses to have processes in place that demonstrate how they're securely handling data.
- Require firms to keep people's personal data safe and secure. Data controllers must ensure that it is not misused.
- Require the data user or holder to register with the Information Commissioner.

All data subjects have the right to:

- Receive clear information about what you will use their data for.
- Access their own personal information.
- Request for their data to be revised if out of date or erased. These are known as the right to rectification and the right to erasure
- Request information about the reasoning behind any automated decisions, such as if computer software denies them access to a loan.
- Prevent or query about the automated processing of their personal data.

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 Harassment 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 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, connexions staff 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 Headteachers, to such extent as is reasonable, to regulate the behaviour of learners 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 Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

(see template policy in these appendices and for DfE guidance - http://www.education.gov.uk/Colleges/learnersupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation)

The Protection of Freedoms Act 2012

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

The College Information Regulations 2012

Requires Colleges to publish certain information on its website:

https://www.gov.uk/guidance/what-maintained-Colleges-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)

Criminal Justice and Courts Act 2015

Revenge porn – as it is now commonly known – involves the distribution of private and personal explicit images or video footage of an individual without their consent, with the intention of causing them embarrassment and distress. Often revenge porn is used maliciously to shame ex-partners. Revenge porn was made a specific offence in the Criminal Justice and Courts Act 2015. The Act specifies that if you are accused of revenge porn and found guilty of the criminal offence, you could be prosecuted and face a sentence of up to two years in prison.

For further guidance or support please contact the Revenge Porn Helpline

Links to other organisations or 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

Revenge Porn Helpline - https://revengepornhelpline.org.uk/

Internet Watch Foundation - https://www.iwf.org.uk/

Report Harmful Content - https://reportharmfulcontent.com/

Harmful Sexual Support Service

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 Internet Safety (UKCIS) - https://www.gov.uk/government/organisations/uk-council-for-internet-safety

Tools for Colleges / other organisations

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

SWGfL Test filtering - http://testfiltering.com/

UKCIS Digital Resilience Framework - https://www.gov.uk/government/publications/digital-resilience-framework

SWGfL 360 Groups – online safety self review tool for organisations working with children

SWGfL 360 Early Years - online safety self review tool for early years organisations

Bullying/Online-bullying/Sexting/Sexual Harassment

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

SELMA – Hacking Hate - https://selma.swgfl.co.uk

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

Curriculum

SWGfL Evolve - https://projectevolve.co.uk
UKCCIS – Education for a connected world framework
Department for Education: Teaching Online Safety in Colleges

Teach Today – www.teachtoday.eu/
Insafe - Education Resources

Data Protection

360data - free questionnaire and data protection self review tool
ICO Guides for Organisations
IRMS - Records Management Toolkit for Colleges
ICO Guidance on taking photos in Colleges

Professional Standards/Staff Training

DfE – Keeping Children Safe in Education
DfE - Safer Working Practice for Adults who Work with Children and Young People
Childnet – College Pack for Online Safety Awareness
UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure/Technical Support/Cyber-security

UKSIC – Appropriate Filtering and Monitoring
SWGfL Safety & Security Resources
Somerset - Questions for Technical Support
SWGfL - Cyber Security in Colleges.
NCA – Guide to the Computer Misuse Act
NEN – Advice and Guidance Notes

Working with parents and carers

SWGfL – Online Safety Guidance for Parents & Carers
Vodafone Digital Parents Magazine
Childnet Webpages for Parents & Carers
Get Safe Online - resources for parents
Teach Today - resources for parents workshops/education
Internet Matters

Prevent

Prevent Duty Guidance
Prevent for Colleges – teaching resources
Childnet – Trust Me

Research

Ofcom –Media Literacy Research
Ofsted: Review of sexual abuse in Colleges and Colleges

Further links can be found at the end of the UKCIS Education for a Connected World Framework