POLICY / PROCEDURE

Document Title	**Online Safety and Remote Learning Policy**
Version	**1.0**
Equality Impact Assessment Status	**No issues identified against any of the protected characteristics. Low risk.**
Approved by	**Executive Team**
Date approved	**10th February 2021**
Effective date	**10th February 2021**
Date of next review	**September 2022**
Lead responsibility	**Designated Safety Lead assisted by the Technology and Innovation Manager**

1 Purpose

1.1 New technologies have become integral to the lives of most people in today's society. This is reflected in the use of technology by our staff and learners both within college and in their lives outside college. The requirement to ensure members of the college community are able to use the internet and related communications technologies appropriately and safely is addressed within this policy and forms a part of the wider safeguarding duty to which all who work in college are bound.

1.2 The use of these new technologies can put all learners, but particularly young people, at risk within and outside of the college. Some of the dangers they face include:

- access to illegal, harmful or inappropriate images or other content;
- unauthorised access to / loss of / sharing of personal information;
- the risk of being subject to grooming by those with whom they make contact on the internet;
- access to people and materials that promote extremism and radicalisation;
- the sharing / distribution of personal images without an individual's consent or knowledge;
- inappropriate communication / contact with others, including strangers;
- cyber-bullying;
- access to unsuitable video / internet games;
- an inability to evaluate the quality, accuracy and relevance of information on the internet;
- plagiarism and copyright infringement;
- illegal downloading of music or video files;
- the potential for excessive use which may impact on the social and emotional development and education of the learner.

1.3 Many of these risks reflect situations in the off-line world and therefore this policy will work in conjunction with other safeguarding policies and as part of the college's approach to the Prevent agenda. As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build learners' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

2 Scope

2.1 This policy applies to all members of the college community (including staff, governors, learners, 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.

2.2 The Education and Inspections Act 2006 empowers the Principal 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. 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. In the case of both acts, action can only be taken over issues covered by the Behaviour Policy.

2.3 The 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 take place out of college.

3 Aim

3.1 This policy will enable Derwentside College to demonstrate its commitment to keeping the college community safe while using online technologies. It should be read in conjunction with all of the associated College Safeguarding Policies and Procedures.

3.2 Whilst regulation and technical solutions are very important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety is therefore an essential part of the college's online safety provision. Learners will be provided with the help and support of the college to recognise and avoid online risks and build their resilience.

3.3 Staff will act as good role models in their use of ICT, the internet, and mobile devices. All staff and relevant Board members will take part in online safety training/awareness sessions which will take place at least every two years. Ongoing alerts and guidance in response to emerging threats or concerns will be issued by the IT and Innovation Team as they arise. All staff, members of the Board and learners must respond to and comply with the guidance/requests to maintain the integrity of the college infrastructure and ensure the safety of all members of the college community.

3.4 The college will be responsible for ensuring that the college infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the sections below will be effective in carrying out their online safety responsibilities.

4 Roles and Responsibilities

4.1 **Executive Team:**

4.1.1 The Executive Team has overall responsibility for ensuring the safety (including online safety) of members of the college community, though the day-to-day responsibility will be delegated to the Online Safety Lead within college. This role will sit with the Technology and Innovation Manager;

4.1.2 The Principal/Executive Team are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant;

4.1.3 The Principal/Executive Team will ensure that there is a system in place to allow for 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;

4.1.4 The Executive Team will receive regular monitoring reports from the Online Safety Lead;

4.1.5 The Executive Team will ensure learners are taught online safeguarding through teaching and learning opportunities as part of a broad and balanced curriculum.

4.2 **Board of Corporation**

4.2.1 The Board play a pivotal role in ensuring the safeguarding of learners and this includes online safeguarding and the impact of digital technology. Board members complete safeguarding update training every 2 years and review Keeping Children Safe in Education legislation on a yearly basis. In addition, they receive an annual safeguarding report and have representation on the College's Health and Safety and Safeguarding Committee.

4.2.2 Where relevant they will:

- understand their online safety responsibilities and accountabilities;
- attend training events provided by the Local Authority, the AoC or other relevant organisations;
- participate in College training events with staff;
- have an awareness of online threats, risks and trends in technology and internet use;
- support and critically challenge the college in implementing effective online safety policies, procedures and practices;
- receive and respond to regular online safety reports from senior leaders;
- have representation on the College's Health and Safety and Safeguarding Committee.

4.3 **Online Safety Lead**

4.3.1 The Online Safety Lead:

- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
- provides training and advice for staff;
- liaises with external agencies that will interface with college systems;
- liaises with college ICT technical staff;
- regularly reviews and audits the safety and security of college ICT systems;
- oversees requests from staff for sites to be removed from the filtered list for educational purposes;
- meets regularly with the Health and Safety and Safeguarding Committee to discuss current issues.

4.4 **Systems Administrator/ICT Support staff**

4.4.1 The Systems Administrator is responsible for ensuring:

- that the college's ICT infrastructure is secure and is not open to misuse or malicious attack;
- that the college meets the online safety technical requirements to monitor/filter internet usage;
- that users may only access the college's networks through a properly enforced password protection policy;
- the college's filtering policy, is applied and updated on a regular basis and that its implementation and monitoring is not the sole responsibility of any single person;
- 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 monitoring software/systems are implemented and updated as agreed in college policies;
- that the use of the network is regularly monitored in order that any misuse or attempted misuse can be reported.

4.5 **Teaching and Support Staff**

4.5.1 Staff should act as good role models in their use of ICT, the internet and mobile devices.

4.5.2 Staff are responsible for:

- ensuring that they have completed online safety training;
- ensuring that they fully understand the college Online Safety and Remote Learning Policy and Acceptable Use Policies;
- ensure personal data is not sent over the internet or taken off the college site unless safely encrypted or otherwise secured;
- immediately reporting, to the Online Safety Lead any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email;
- ensuring any digital communication with learners or parents/carers (email, chat, VLE etc) must be professional in tone and content. These communications should only take place on official (monitored) college systems or college run social media pages. Personal email, text messaging or public chat/social networking must not be used for these communications;
- personal information should not be posted on the college website or social media pages and only official email addresses should be used to identify members of staff;
- embedding where relevant online safety issues in the curriculum and other college activities;

- ensuring learners understand and follow the college online safety and acceptable use policy;
- learners having a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- monitoring ICT activity in lessons;
- ensuring all safeguarding issues are reported to the DSL or deputies;
- in lessons where internet use is pre-planned, learners are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches;

4.5.3 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 can request that the Technology and Innovation Manager temporarily remove 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.

4.6 **The Designated Safeguarding Lead**

4.6.1 The Designated Safeguarding Lead 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 online contact with adults/strangers;
- potential or actual incidents of grooming;
- cyber bullying;
- the Prevent strategy;
- the DSL has a leading role in establishing and reviewing the college online safety policies / documents.

4.7 **Learners**

4.7.1 Whilst regulation and technical solutions are very important, their use must be balanced by educating learners to take a responsible approach and understand they:

- are responsible for using the college ICT systems in accordance with the Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- need to report abuse, misuse or access to inappropriate materials and know how to do so;
- are expected to know and understand college policies on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand college policies on the taking/use of images and on cyber-bullying;
- should adopt good online safety practice when using digital technologies out of college and realise that the college's Online Safety Policy covers their actions out of college, if related to their membership of the college;
- should be critically aware of the materials/content they access on-line and validate the accuracy of information.

4.8 **Parents/Carers**

4.8.1 Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The college will take every opportunity to help parents understand these issues. Parents and carers will be encouraged to support the college in promoting good online safety practice and to follow guidelines on the appropriate use of their children's personal devices at home and in the college (where this is allowed).

5 Use of digital and video images – Photographic, Video

5.1 The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff and learners need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The college will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- when using digital images, staff should inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites;
- staff are allowed to take digital / video images to support educational aims, but must follow college policies concerning the sharing, distribution and publication of those images. These images should only be taken on college equipment; the personal equipment of staff should not be used for such purposes;
- care should be taken when taking digital / video images that learners are appropriately dressed and are not participating in activities that might bring the individuals or the college into disrepute;
- learners must not take, use, share, publish or distribute images of others without their permission;
- learners must not share/ distribute illegal, pornographic, sexualised or other inappropriate material of themselves or others while at college or linked by membership of the college or use, share, publish or distribute images of others without their permission;
- photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with good practice guidance on the use of such images. Permission must be sought for the use of these images including the permission of the parent/guardian for those learners under 18.

6 Sexting: responding to an incident

6.1 In the latest advice for schools and colleges (UKCCIS, 2016), sexting is defined as the production and/or sharing of sexual photos and videos of and by young people who are under the age of 18. It includes nude or nearly nude images and/or sexual acts. It is also referred to as 'youth produced sexual imagery'. The production and distribution of sexting images involving anyone under the age of 18 is illegal and needs very careful management for all those involved.

6.2 'Sexting' does not include the sharing of sexual photos and videos of under-18-year-olds with or by adults. This is a form of child sexual abuse and must be referred to the police.

6.3 **If an incident involving 'sexting' comes to your attention report it to your Designated Safeguarding Lead (DSL) or deputy immediately:**

- Never view, download or share the imagery yourself, or ask a child to share or download – this is illegal;
- If you have already viewed the imagery by accident (e.g. if a young person has showed it to you before you could ask them not to), report this to the DSL;
- Do not delete the imagery or ask the young person to delete it;
- Do not ask the young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL;
- Do not share information about the incident to other members of staff, the young person(s) it involves or their, or other, parents and/or carers;

- Do not say or do anything to blame or shame any young people involved;
- Do explain to them that you need to report it and reassure them that they will receive support and help from the DSL.

7 Social Media – Protecting Professional Identity

7.1 The college provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners, staff and the college through limiting access to personal information by training on the college acceptable use policy, social media risks and data protection.

7.2 College staff should ensure that:

- no reference is made in social media to learners or parents/carers;
- they do not engage in online discussion on personal matters relating to other members of the college community;
- personal opinions are not attributed or associated with the college;
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information;
- social media sites are used in line with the Staff Code of Conduct.

7.3 When official college social media accounts are established there should be:

- approval by a Curriculum Leader, Head of Student Services, Head of Classroom Provision, Area Manager or Senior Leader;
- clear processes for the administration and monitoring of these accounts – involving at least two members of staff;
- a code of behaviour for users of the accounts, including:
- systems for reporting and dealing with abuse and misuse;
- understanding of how incidents may be dealt with under college disciplinary procedures.

8 Personal Use

8.1 Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with the college or impacts on the college, it must be made clear that the member of staff is not communicating on behalf of the college with an appropriate disclaimer. Such personal communications are within the scope of this policy.

8.2 Personal communications which do not refer to or impact upon the college are outside the scope of this policy.

8.3 Where excessive personal use of social media in college is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.

8.4 The college permits reasonable and appropriate access to private social media sites.

9 Monitoring of Public Social Media

9.1 As part of active social media engagement, the college considers it good practice to pro-actively monitor the internet for public postings about the college.

9.2 The college will effectively respond to social media comments made by others in line with the policy.

9.3 The college use of social media for professional purposes will be checked regularly by the Online Safety Lead and the Health and Safety and Safeguarding Committee to ensure compliance with the college policies.

10 Online Teaching and Learning from Home

10.1 Guidance for staff

10.1.1 Consider carefully the opportunities and limitations presented by remote learning. The nature of working online, particularly where it involves 1:1 lessons, does pose additional safeguarding and data protection challenges.

10.1.2 For all remote lessons please observe the following points for every lesson:

- never conduct lessons from a bedroom or a personal space, ensure your background is neutral or blurred;
- inform learners if the lesson is to be recorded;
- set appropriate boundaries and behavioural expectations, and maintain the same professional standards as at college (e.g. they should start the lesson muted and unmute to ask questions);
- ensure that all learners are aware that they must not record the session either as video or images;
- never make inappropriate jokes or comments online;
- for 1:1 lessons, your line manager, colleague or LSA should always be a member of the relevant Team, they do not have to attend each session, but can 'drop in' to lessons on occasion. Please contact a member of the Safeguarding team if you have any questions with regards to 1:1 lessons;
- in many cases it is sensible to record a lesson so that it can be made available to learners who are unable to attend at the time the lesson is running. However, consideration should be given to how long that recording is available for. If the lesson includes any content involving learners it should not be shared with other groups, or colleagues, unless this has been agreed with the learners;
- when sharing your desktop with learners as part of a lesson it is advisable to only have open applications that you will be using during the lesson. This avoids the risk of inadvertently sharing sensitive material, such as items in your inbox if Outlook is open;
- Teams now has the option for the host to end the meeting for everyone and this is something that you should always do at the end of a lesson to avoid any potential issues between learners left in the online classroom environment;
- any behavioural issues that occur during an online lesson should be dealt with as sensitively as would be the case in a physical lesson. However, asking to speak to a learner at the end of the lesson would not be appropriate in this context. While usual best practice is to speak to a learner face to face regarding their behaviour it would be more appropriate to send an email to the learner, copying in any other relevant teachers, CL and if appropriate parent/guardian;
- 'classroom standard' of behaviour is always expected from all participants and ground rules should be set out to ensure a safe space. This message will be reiterated at the start of each session;
- should you have any safeguarding concerns relating to any aspect of an online lesson please contact a member of the Safeguarding team.

10.2 Guidance for learners

10.2.1 The usual standard of behaviour expected during lessons in college still apply to any remote online learning experience this includes disciplinary sanctions if required. Additional rules that learners should follow are:

- you should ideally be based in an area conducive to learning, try to avoid your bedroom if at all possible;
- you should be appropriately dressed for a lesson; this should be the sort of clothes you would normally wear to college;
- use a neutral background or if you are sharing a video feed you should have your background blurred;

- you should not make any recording of the lesson. Your tutor may choose to record the lesson in order to make it available to members of the class who are not able to join the lesson at the usual time;
- it is good practice to start any lesson or meeting with your mic muted and to only unmute when you are going to talk. Your tutor may ask you to make use of the chat function during the lesson to note questions, please do keep the chat bar open so that you can see what other questions are being asked;
- should anything happen in an online lesson that makes you uncomfortable please contact a member of the Safeguarding team below.

Patrick O'Doherty, Designated Safeguarding Lead and Head of Student Services (01207 585936) (patrick.odoherty@derwentside.ac.uk)

Karen Hankey, Deputy DSL and Curriculum Leader Student Services (01207 585900 Ext. 728) (karen.hankey@derwentside.ac.uk)

Julie Eddy, Deputy DSL and SEND Lead/Functional Skills Tutor (01207 585900 Ext. 605) (julie.eddy@derwentside.ac.uk)

11 Adding Content Online:

11.1 Staff should ensure that all content added/stored online, including messages, images, videos, are in line with GDPR, safer working practice and staff code of conduct;

11.2 No content should be added online if it places a learner at risk of harm;

11.3 Any content shared must not bring the college into disrepute and behaviour, appearance, environment of staff must be appropriate for sharing with learners;

11.4 If possible parents/carers will be made aware of what is shared with their child online including what they are expected to complete and any websites they need to visit in order to achieve this;

11.5 Online content must be regularly reviewed by staff and line managers.

12 Interactive online communication:

12.1 Staff should not use personal devices when communicating with learners;

12.2 Staff must only communicate with learners and parents/carers using official college systems or online platforms and avoid personal online accounts;

12.3 Restrictions should be in place so that learners cannot create unsupervised groups using official college systems;

12.4 Staff should ensure that all communication with learners online is in line with GDPR, safer working practice and staff code of conduct.

13 Accountability:

13.1 Staff will keep a log of remote learning sessions;

13.2 Staff will record in the log details of the sessions, including timings, who participated and any issues that arose – any issues will be reported in line with college procedures;

13.3 There will be regular review meetings between staff and their line manager, as well as line managers dropping-in to online teaching sessions to ensure that this guidance is being followed appropriately;

13.4 learner voice and parental voice will also be sought regularly to ensure the remote learning provision is appropriate and supporting the needs of the child (including additional considerations for SEND/those with a social worker) – this will include reinforcing how to raise a concern;

13.5 Any safeguarding concerns/allegations must be reported in line with the college safeguarding procedures as stated in the Safeguarding Young People and Adults at Risk Policy.

14 Ensuring online education practices are inclusive

14.1 Effective communication channels are important to support learners with special educational needs and disabilities (SEND) and learners engaged with social care. We are aware that these children are particularly vulnerable and need added support both in terms of staying safe online and accessing education successfully. Approaches and support will need to be tailored to individual needs to prevent children falling further behind. This is particularly important for vulnerable children who might have further barriers to learning in their home environment.

14.2 ALS staff will work with these vulnerable learners adapting resources to support them with online learning. Utilising video calls, instant messaging, accessibility features such as voice-to-text and text-to-speech conversion, or different viewing formats to support pupils with dyslexia and other special educational needs along with regular phone calls to support with their learning needs.

15 Mental Health

15.1 Teachers are aware that distance learning can affect the mental health of learners and their parents. Teachers should take this into account in setting expectations of learners' work when they are at home. Staff should raise a concern if they suspect, from a child's behaviour or emotional state during online lessons, that there may be underlying mental health issues. Teachers or support staff should contact a member of the wellbeing team in the first instance who can investigate and then escalate to the DSL if appropriate.

16 Contacting learners by phone:

- Call in college hours as much as possible;
- Make sure someone else at college is aware, and keep a record of the date and time of each call;
- With 16-18 learners if possible have a parent there at the child's end, and have the phone on speaker if possible;
- Staff should use the college phone, mobile or email and not use their personal devices and should not share their personal contact details.

17 Dealing with unsuitable/inappropriate activities

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

17.2 The college believes that the activities referred to in the following section are for the most part inappropriate in the 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:

User Actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Child sexual abuse images – The making, production and 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 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	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)					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
illegal downloading of music or video files					x
Revealing or publishing confidential or proprietary information (e.g. financial, passwords, personal information)					X
Creating or propagating computer viruses or other harmful files					X
Unfair usage (downloading/uploading large files that hinder others in their use of the internet)				X	
Online gaming (educational or for educational purposes)			X		
Online gaming (non-educational)				X	
Online gambling				X	
Online shopping		X			
File sharing				X	
Use of social media		X			
Use of messaging apps		X			
Use of video broadcasting e.g. YouTube			X		

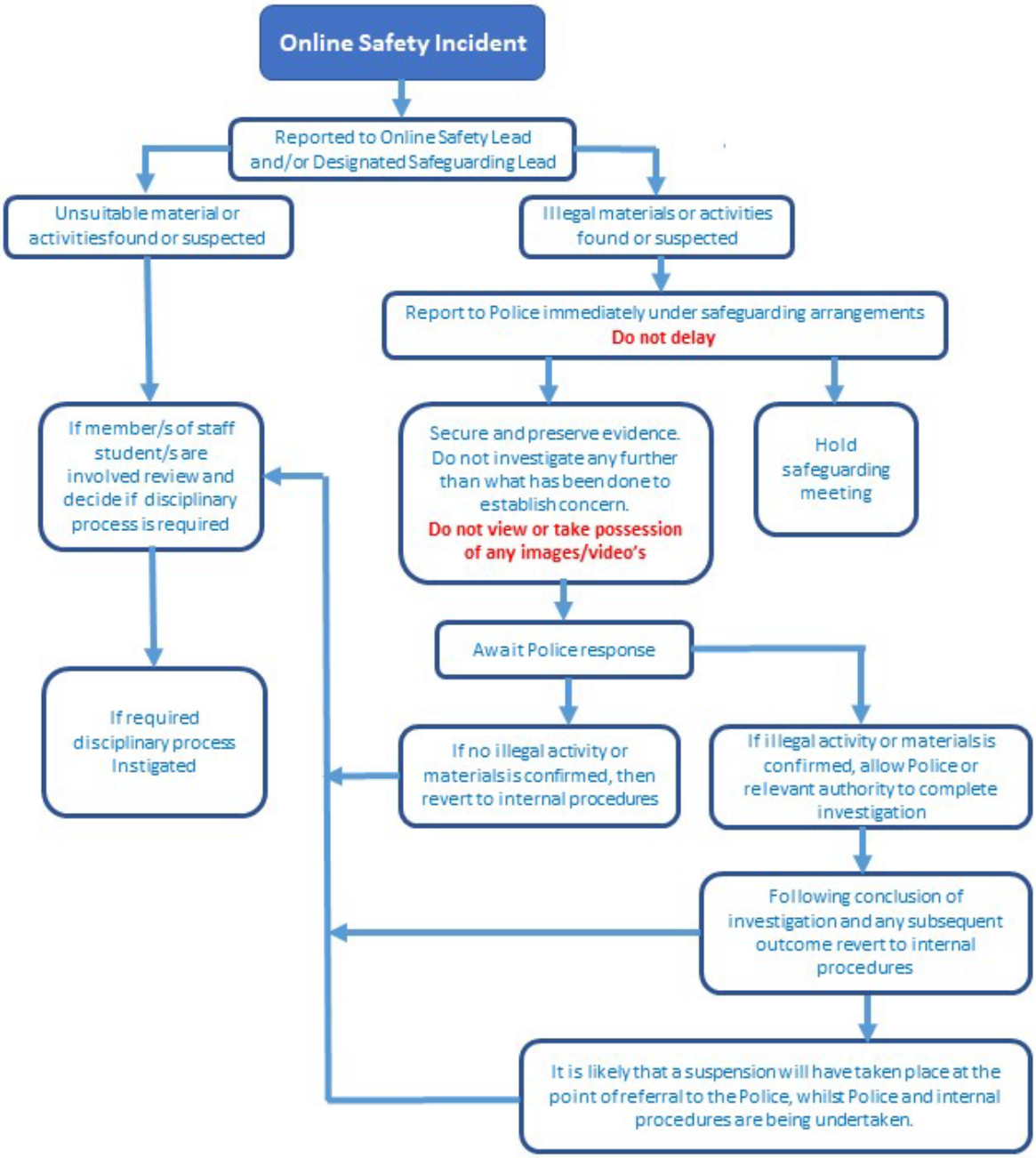
18 Breach of Online Safety Policy

18.1 Any breach of the online safety policy will be dealt with as follows:

- Any suspected illegal activities will be reported to the police;
- Any suspected breach of policy by a learner will be dealt with using the Student Behaviour and Disciplinary Policy;
- Any suspected breach of policy by a member of staff will be dealt with using the Staff Disciplinary Procedure;
- Any breach of policy by a guest user will dealt with by removing access to all college systems for the user.

19 Illegal Incidents

19.1 If there is any suspicion of a website(s) or material found such as child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart (below) for responding to online safety incidents and report immediately to the police.



20 Other Incidents

20.1 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.

20.2 In the event of suspicion of an incident, all steps outlined in the investigation procedure below should be followed.

21 Investigation Procedure

21.1 In the event of suspicion of an incident, isolate the computer or device in question as best you can. Any change to its state may hinder a later police investigation.

21.2 Have more than one senior member of staff involved in the investigation process. This is vital to protect individuals if accusations are subsequently reported.

21.3 Conduct the procedure using a designated computer that will not be used by learners 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.

21.4 It is important to ensure that the investigating staff 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).

21.5 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 and signed (except in the case of images of child sexual abuse – see below).

21.6 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.

21.7 Once this has been completed and fully investigated the college will judge whether the 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 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;
- offences under the Computer Misuse Act;
- other criminal conduct, activity or materials.

22 College actions and sanctions

22.1 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.

23 Equality & Diversity

23.1 The College has paid due regard to equality considerations during the preparation and implementation of this Policy and Procedure.

23.2 These considerations included the potential for any differential negative effect on the grounds of age, disability, gender reassignment, pregnancy and maternity, race (including ethnic or national origins, colour or nationality), religion or belief (including lack of belief), sex, sexual orientation, marriage or civil partnership.

23.3 The College's judgement is that there is no such negative effect on those grounds and, consequently, no potential breach of the Equality Act 2010.

23.4 The operation of this Policy and Procedure will be monitored by the Head of Human Resources in order to establish that no unlawful discrimination is taking place and to identify opportunities for the College to enhance equality of opportunity and fair treatment.

24 Review

24.1 This document will be reviewed by September 2022.

24.2 The Designated Safeguarding Lead will undertake this review, taking into account the outcomes of the monitoring process, legislative changes and developments in good practice.

24.3 As part of the review, the DSL will seek and consider the views of the College's employees and of the recognised trade unions.

24.4 The outcome of the review will be reported to the Executive Team.

25 Document Identification

Category [select ONE only]	☐Programmes/courses ☐Partnerships ☐Finance ☐Quality ☐Governance ☒Health and safety ☐Facilities ☒IT and Innovation ☐MIS ☐Admissions ☒Teaching and learning ☐Personnel
Audience [select ALL that apply]	☒Employees ☒Learners ☒Partners ☐Suppliers