Digital Safety Policy

2021-22

Responsibility of:	Director of Teaching & Learning/e-Learning Manager
Inclusivity Assessed Date:	09/20
Quality Impact Assessed Date:	09/20
Supported by:	**Executive**
Approved by Corporation:	Click here to enter a date. November 2020 September 2021
Review Interval (unless statutory changes apply)	**1 year**
Current Revision Date:	26/08/21
Next Revision Date:	
Published as: **Website PdF Edition**	☒ Click here to enter a date.
Electronic Edition	☒
Hard Copy Edition *	☒

Amendments Since the Last Revision			
Section Number	**Title**	**Amendment Summary / Reference**	**Date**
			Click here to enter a date.

1. Development/Monitoring/Review of this Policy

This digital safety policy has been developed by a working group/committee made up of:

- Principal and Senior Leaders
- ICT Network Manager
- E-Learning Manager
- Staff – including teachers, support staff, technical staff
- Governors/Board

Consultation with the whole College community has taken place through a range of formal and informal meetings.

2. Schedule for Development/Monitoring/Review

This digital safety policy was first approved by the Governing Body/Governors Sub Committee on:	November 2020 and again in September 2021.
The implementation of this digital safety policy will be monitored by the:	Online Safety Leads
Monitoring will take place at regular intervals:	Annually

The digital safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	Sept 2021
Should serious online safety incidents take place, the following external persons/agencies should be informed:	LA Safeguarding Officer, LADO, Police

The College will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)/filtering
- Internal monitoring data for network activity
- Surveys/questionnaires of
  - students/pupils
  - parents/carers
  - staff

3. Scope of the Policy

This policy applies to all members of the College community (including staff, students, volunteers, parents/carers and visitors) 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. In the case of both acts, action can only be taken over issues covered in related policies, Student and Staff ICT agreements, Anti-Bullying Policy, Student code-of-conduct and Student Disciplinary procedures.

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.

4. Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the College:

Governors

Governors are responsible for the approval of the digital safety policy and for reviewing the effectiveness of the policy. Mike Wright, a member of the Governing Body, has taken on the role of Digital Safety Governor, this is in addition to his role of Child Protection/Safeguarding Governor. The role of the Digital Safety Governor will include:

- Regular meetings with the ICT/Network Manager and E-Learning Manager

- Attendance at Digital Safety Group meetings
- Regular monitoring of online safety incident logs
- Regular monitoring of filtering/change control logs
- Reporting to relevant Governors/Board/Committee/meeting

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 Digital Safety Leads; the Head of Safeguarding and Student Discipline, ICT/Network manager and E-Learning Manager.
- The Principal and (at least) another member of the Senior Leadership Team 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. (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant *Local Authority/MAT/other relevant body* disciplinary procedures).
- The Principal and Senior Leaders are responsible for ensuring that the Digital Safety Leads and other relevant staff receive suitable training to enable them to carry out their digital safety roles and to train other colleagues, as relevant.
- The Principal and Senior Leaders 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.
- The Senior Leadership Team will receive regular monitoring reports from the Digital Safety Leads.

Digital Safety Leads

The College has identified digital safety leads; Head of Safeguarding & Discipline, ICT/Network Manager and E-Learning Manager.

The role of the Digital Safety Leads will include:

- Leads the Digital Safety Group
- Takes day to day responsibility for digital safety issues and has a leading role in establishing and reviewing the College's digital safety policies/documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an digital safety incident taking place
- Provides training and advice for staff
- Liaises with the Local Authority/relevant body
- Liaises with College technical staff
- Receives reports of digital safety incidents and creates a log of incidents to inform future digital safety developments,
- Meets regularly with Digital Safety Governor to discuss current issues, review incident logs and filtering/change control logs
- Attends relevant meetings of Governors
- Reports regularly to Senior Leadership Team
- Investigates/actions/sanctions with incidents.

Network Manager/Technical staff

Those with technical responsibilities are responsible for ensuring:

- 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 and any Local Authority/other relevant body online safety policy/guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy
- The filtering policy is applied and updated on a regular basis and that its implementation 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 digital safety role and to inform and update others as relevant
- That the use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Digital Safety Leads for investigation/action/sanction
- That monitoring software/systems are implemented and updated as agreed in college policies

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 digital safety policy and practices
- They have read, understood and signed the staff acceptable use agreement (AUP)
- They report any suspected misuse or problem to the Digital *Safety Leads* for investigation/action/sanction
- All digital communications with students/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 Digital Safety Policy and acceptable use policies
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- 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

Designated Safeguarding Lead

The post holder is trained in online/digital safety issues and is 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

Online & digital Safety Group

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 part of the safeguarding group. The group will also be responsible for regular reporting to the Governing Body.

Members of the Online & digital Safety Group will assist the digital Safety Leads with:

- The production/review/monitoring of the College's digital safety policy/documents.
- Mapping and reviewing the digital safety/digital literacy curricular provision – ensuring relevance, breadth and progression
- Monitoring network/internet/filtering/incident logs
- Consulting stakeholders – including parents/carers and the students about the online safety provision

Students

- Are responsible for using the *college* digital technology systems in accordance with the student ICT 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's digital safety policy covers their actions out of college, if related to their membership of the college.

Parents/carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their son/daughter and in the monitoring/regulation of their online behaviours. Parents may underestimate how often young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The college will therefore seek to provide information and awareness to parents and carers through:

- *Letters, web site, and e-learning platform*
- *High profile events/campaigns e.g. Safer Internet Day*
- *Reference to the relevant web sites/publications e.g.*

swgfl.org.uk, www.saferinternet.org.uk/, http://www.childnet.com/parents-and-carers

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:

- Digital and video images taken at college events
- Online Learning Platforms
- Their children's personal devices in the college

Community Users

Community Users who access college systems or programmes as part of the wider college provision will be expected to sign an ICT Acceptable Use agreement before being provided with access to college systems.

5. Policy Statements

Education – Students/Pupils

The education of students in online safety/digital literacy is an essential part of the College's online safety provision. Young people need the help and support of the College to recognise and avoid online safety risks and build their resilience.

Digital safety should be a focus in all areas of the curriculum and staff should reinforce online and digital safety messages across the curriculum. The online and digital safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online and digital safety curriculum should be provided as part of a Tutorial programme and should be regularly revisited
- Key online and digital safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- Students should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Students should be helped to understand the need for the student acceptable ICT user agreement and encouraged to adopt safe and responsible use both within and outside College.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- It is accepted that from time to time, for good educational reasons, students 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 Technical Staff (or other relevant designated person) can 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.

Education & Training – Staff/Volunteers

It is essential that all staff receive online and digital safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online and digital safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online and digital safety training needs of all staff will be carried out regularly.
- All new staff should receive online and digital safety training as part of their induction programme, ensuring that they fully understand the college digital safety policy and acceptable use agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Digital Safety Leads will receive regular updates through attendance at external training events (e.g. from SWGfL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This digital safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.
- The Digital Safety Leads (or other nominated person) will provide advice/guidance/training to individuals as required.
- Staff read and abide by the Laptop Loan Agreement (regarding the extent of personal use that users (staff/students) and their family members are allowed on college devices that may be used out of school)
- Staff/Student will not download executable files and install programmes on college devices without prior approval.

Training – Governors

Governors should take part in online and digital safety training/awareness sessions, with particular importance for those who are members of any group involved in technology/ digital safety/health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Governors Association/or other relevant organisation (e.g. SWGfL).
- Participation in college training/information sessions for staff or parents

Technical – infrastructure/equipment, filtering and monitoring

The College is 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. The technical staff will ensure that systems are kept secure and up to date, and will monitor and test the filtering and firewall system, as well as college Email, Teams, Onedrive and other cloud services.

- College technical systems will be managed in ways that ensure that the college meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of college technical systems

- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to college technical systems and devices.
- All users will be provided with a username and secure password by the ICT team, who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The "master/administrator" passwords for the college systems, used by the Network Manager (or other person) must also be available to the Principal or other nominated senior leader and kept in a secure place (e.g. college safe)
- The colleges' ICT/Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband provider and the college firewall / filtering system. Content lists are regularly updated automatically and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- Internet filtering/monitoring should ensure that young people are safe from terrorist and extremist material when accessing the internet.
- College technical staff regularly monitor, and record the activity of users on the college technical systems and users are made aware of this in the acceptable use agreement.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the College systems and data. These are tested regularly. The College infrastructure and individual devices are protected by up to date virus software.

Mobile Technologies (including BYOD/BYOT)

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

All users should understand that the use of mobile technologies should be consistent with and inter-related to other relevant college polices including but not limited to the safeguarding policy, behaviour policy, bullying policy, acceptable use policy, and policies around theft or malicious damage.

- The College acceptable use agreements for staff, students and parents/carers will give consideration to the use of mobile technologies:

The college allows:	College Devices			Personal Devices		
	College owned for single user	College owned for multiple users	Authorised device[1]	Student owned	Staff owned	Visitor owned
Allowed in school	*Yes*	*Yes*	*Yes*	Yes	Yes	Yes
Full network access	*Yes*	*Yes*	*Yes*			
Internet only				Yes		Yes
Limited network Access					Yes	
No network access						

Aspects that the College may wish to consider and be included in their digital safety policy, mobile technologies policy or acceptable use agreements. When personal data is stored on any mobile device or removable media, staff must ensure that:

- The data must be encrypted and password protected.
- The device must be password protected.
- The device must be protected by up to date virus and malware checking software
- The data must be securely deleted from the device, in line with College policy once it has been transferred or its use is complete.
- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Staff can recognise a possible breach, understand the need for urgency and know who to report it to within the College.
- Staff and data subjects understand their rights and know how to handle a request whether verbal or written. Know who to pass it to in the College
- Staff will not transfer any college personal data to personal devices except as in line with College policy
- Staff access personal data sources and records only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.

Use of digital and video images

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 students 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.

[1] Authorised device – purchased by the student/family through a college-organised scheme. This device may be given full access to the network as if it were owned by the college.

- Written permission will be obtained before photographs of students are published on the college website/social media/local press.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their son/daughter at college events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students in the digital/video images.
- Staff and volunteers 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.
- Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the college into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Student's work can only be published with the permission of the student and/or parents or carers.

6. Data Protection

The UK's data protection regime is set out in the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. Colleges are likely to be subject to greater scrutiny in their care and use of personal data. Colleges should ensure that they take account of policies and guidance provided by local authorities or other relevant bodies.

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The College must ensure that:

- It has a Data Protection Policy.
- It implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.
- It has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest.
- It has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it
- The information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded
- It will hold only the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for. The college

should develop and implement a 'retention policy" to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. Personal data held must be accurate and up to date where this is necessary for the purpose it is processed for. Have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals

- It provides staff, parents, volunteers, teenagers and older children with information about how the college looks after their data and what their rights are in a clear Privacy Notice.
- Procedures must be in place to deal with the individual rights of the data subject, e.g. one of the 8 data subject rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them (subject to certain exceptions which may apply).
- Data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier (this may also require ensuring that data processing clauses are included in the supply contract or as an addendum)
- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners
- It has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
- It understands how to share data lawfully and safely with other relevant data controllers.
- It reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.
- It must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- All staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

7. Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the college currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

	Staff & other adults			Students				
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the college		X				X	X	
Use of mobile phones in lessons		X				X	X	
Use of mobile phones in social time	X				X			
Taking photos on mobile phones/cameras		X				X	X	
Use of other mobile devices e.g. tablets, gaming devices						X	X	
Use of personal email addresses in college, or on college network				X				X
Use of college email for personal emails				X				X
Use of messaging apps i.e. Microsoft Teams	X				X			
Use of social media			X				X	
Use of blogs			X				X	

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

- The official college email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. *Staff and students should therefore use only the college email service to communicate with others when in college, or on college systems (e.g. by remote access).*
- Users must immediately report, to the nominated person – in accordance with the college policy, 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.
- Any digital communication between staff and students or parents/carers (email, social media, chat, blogs, VLE etc.) must be professional in tone and content. *These communications may* only take place on official (monitored) college systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Students will be provided with individual college email addresses for educational use.
- Students should be taught about online and digital safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with

inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

- Personal information should not be posted on the college website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'. Ofsted's online safety inspection framework reviews how an education establishment protects and educates staff and pupils in their use of technology, including the measures that would be expected to be in place to intervene and support should a particular issue arise.

All colleges and local authorities have a duty of care to provide a safe learning environment for students and staff. Colleges and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the *college* or local authority liable to the injured party.

The college provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the college through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

College staff should ensure that:

- No reference should be made in social media to students, parents/carers or college staff
- 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 or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

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

- A process for approval by senior leaders
- 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

Personal Use:

- Personal communications are those made via a 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

- Personal communications which do not refer to or impact upon the college are outside the scope of this policy
- Where excessive personal use of social media in college is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.

Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the college
- The college should effectively respond to social media comments made by others according to a defined policy or process.
- The college will ensure student and staff give consent for their pictures to be used on social media.
- The *college's* use of social media for professional purposes will be checked regularly by the senior risk officer and Digital Safety Group to ensure compliance with the college policies.

8. 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:

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,	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 N.B. Schools/academies should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					X

data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	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 school or brings the school 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 systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the college					X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)					X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X		
Using college systems to run a private business					X	
Infringing copyright					X	
On-line gaming (educational)				X		
On-line gaming (non-educational)						X
On-line gambling						X

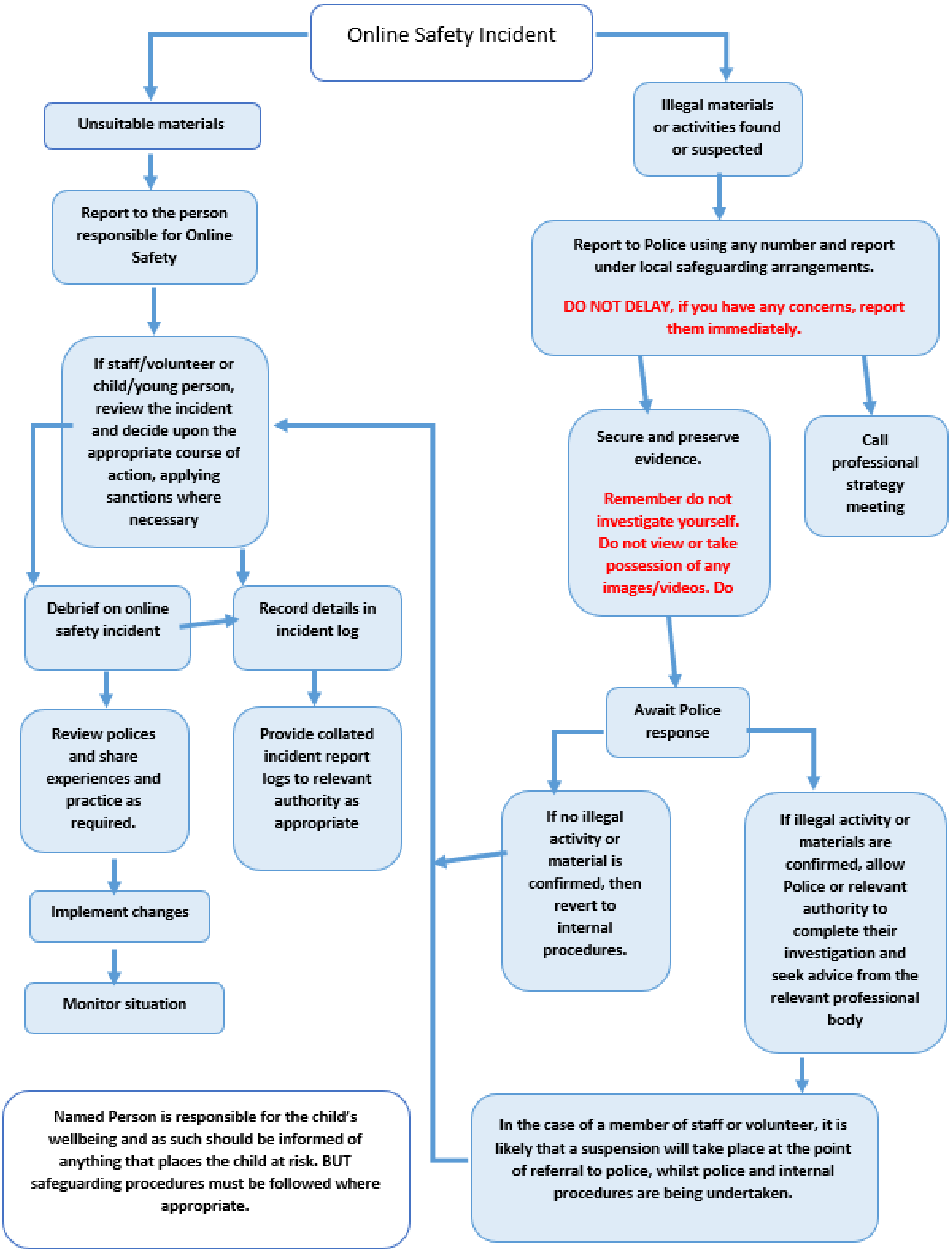
On-line shopping/commerce		X			
Internal File sharing	X				
Use of appropriate/approved social media	X				
Use of approved messaging apps		X			
Use of video broadcasting e.g. Youtube	X				

9. Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of digital services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).)

Illegal Incidents

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 and digital safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as required.
Provide collated incident report logs to relevant authority as appropriate
Implement changes
Monitor situation
Illegal materials or activities found or suspected
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not view or take possession of any images/videos. Do
Call professional strategy meeting
Await Police response
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.
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 police, whilst police and internal procedures are being undertaken.

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:

- Have more than one senior member of staff 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 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 (see User Actions chart above)
    - 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.

10. 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 as follows:

	Actions/Sanctions								
Students/Pupils Incidents	Refer to class teacher/tutor	Refer to Senior Safeguarding and Disciplinary Officer	Refer to Director of Students	Refer to Police	Refer to ICT Network Manager for action re filtering/security etc.	Inform parents/carers	Removal of network/internet access rights	Warning	Further sanction e.g. suspension/exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X	X	X	X	X		X
Unauthorised use of non-educational sites during lessons	X	X	X					X	X
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device	X	X	X					X	X
Unauthorised/inappropriate use of social media/ messaging apps/personal email	X	X	X			X		X	X
Unauthorised downloading or uploading of files		X	X		X	X			X
Allowing others to access college network by sharing username and passwords		X	X			X		X	X
Attempting to access or accessing the college network, using another student's account		X	X		X	X	X		X
Attempting to access or accessing the college network, using the account of a member of staff		X	X		X	X	X		X
Corrupting or destroying the data of other users		X	X		X	X	X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X			X		X	X
Continued infringements of the above, following previous warnings or sanctions		X	X			X		X	X
Actions which could bring the college into disrepute or breach the integrity of the ethos of the college		X	X			X		X	X

Using proxy sites or other means to subvert the college's filtering system		X	X		X	X	X		X
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X	X	X	X	X		X
Deliberately accessing or trying to access offensive or pornographic material		X	X	X	X	X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X		X	X	X		X	X

Actions/Sanctions

Staff Incidents	Refer to line manager	Refer to Principal and HR	Refer to Local Authority/HR	Refer to Police	Refer to ICT Network Manager Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).	•	• •	• •	• •	•	• •	• •	• •
Inappropriate personal use of the internet/social media/personal email	•	• •	• •	•	•	• •	• •	• •
Unauthorised downloading or uploading of files	•	• •	• •	•	•	• •	• •	• •
Allowing others to access college network by sharing username and passwords or attempting to access or accessing the college network, using another person's account	•	• •	• •	•	•	• •	• •	• •
Careless use of personal data e.g. holding or transferring data in an insecure manner	•	• •	• •	•	•	• •	• •	• •
Deliberate actions to breach data protection or network security rules	•	• •	• •	•	•	• •	• •	• •

Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	•	• •	• •	•	•	• •	• •	• •
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	•	• •	• •	•	•	• •	• •	• •
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students	•	• •	• •	•	•	• •	• •	• •
Actions which could compromise the staff member's professional standing	•	• •	• •	•	•	• •	• •	• •
Actions which could bring the college into disrepute or breach the integrity of the ethos of the college	•	• •	• •	•	•	• •	• •	• •
Using proxy sites or other means to subvert the college's filtering system	•	• •	• •	•	•	• •	• •	• •
Accidentally accessing offensive or pornographic material and failing to report the incident	•	• •	• •	•	•	• •	• •	• •
Deliberately accessing or trying to access offensive or pornographic material	•	• •	• •	•	•	• •	• •	• •
Breaching copyright or licensing regulations	•	• •	• •	•	•	• •	• •	• •
Continued infringements of the above, following previous warnings or sanctions	•	• •	• •	•	•	• •	• •	• •

Appendix : ICT ACCEPTABLE USE – STUDENT AGREEMENT

Student ID Number:		Tutor Group:	
Student Name (BLOCK CAPITALS):			

St Mary's College must comply with Data Protection Regulations (GDPR 2018) recognises duties under section 21 of the Counter Terrorism and Security Act 2015 and Government PREVENT Strategy.

The I.T. resources provided by St Mary's College Blackburn are for academic use only and as a student, you agree to use the College systems and devices in a responsible way as per the following agreement.

1. Student Agreement –ICT:

- You will not attempt to hack College systems, knowingly introduce viruses, attempt to access / capture data or by-pass any security measures installed on the College network or equipment.
- You will only use your own College login provided to you and not use or attempt to use other student's logins or attempt to login as anyone else but you to any College system.
- You will only use the internet and College email for research purposes only and you will not search, view, download, store, publish, transmit or communicate content that is or relates to materials which are illegal or inappropriate :-

Threatening Behaviour / Offensive Content / Abusive / Libellous / Harassment / Pornographic / Sexist / Racist / Terrorism / Extremism / Cults / Illegal Drugs / Gambling / Criminal Skills / Social Chat / Encouragement of violence or unlawful conduct or any other content which could cause harm or distress to the College or others

- You will not damage, alter or tamper with College equipment, software or resources and will report any issues directly to a member of staff.
- You will not install any software on to the College network or attempt to run software from external sources such as a pen drive.
- You will not publish photographs or videos on social media of any individual within the College without the permission of the individual.
- You will not use the College's systems to access and re-publish material, as if it is your own work.
- You will not use College workstations unproductively in the Library or classrooms to watch videos, listen to music or to play games. When working in these areas you will respect other students and staff and keep the noise down to a minimum and not cause disruption to other users. You will also visibly wear your ID badge at all times.
- You will not store any person files/data on the College computers or network drives (e.g.photos / personal information)
- Ensure that any work is saved to your own network area (Q drive) and if you save work to a pen drive or external hard drive, please back up these documents on a regular basis.

- I will only use my hand held / external devices (Phones, Tablets, Laptops etc.) in class if I have permission. Usage of any personal device must be in line with the College policy.
- When I leave College I understand that my email account and online access will be disabled immediately and that documents associated with my learning will be retained for a maximum of 12 months on the St Mary's College ICT network.

Microsoft Teams / E-Learning

Microsoft Teams has been provided to all staff and students for use in relation to College teaching and learning activity e.g. to deliver online lessons, support discussions, collaboration and communication relating to: academic study, engagement in college clubs, events and activities; staff meetings and collaboration networks.

Microsoft Teams is an Office 365 cloud service and therefore information contained within St Mary's Teams sites is stored in Microsoft Data Centres. This meets UK and EU data protection and security standards.

I.T. Administrators can access any data attached to a St Mary's email.

2. Student Agreement –E-Learning:

Students are expected to uphold the same standards of conduct and behaviour during live online lessons as they would be expected to within College. This includes but is not limited to:

General:

- Ensuring full engagement with the tasks in hand, including submission of any required work by the deadline that has been set.
- Ensuring that clothing is appropriate, following the same guidance as a normal day in College.
- Students should think carefully about what acceptable language is with regards to what they type and post in a lesson.
- Be professional – be polite, no haters, trolling or hijacking posts. Treat team members with respect. It is important that this is maintained throughout, even in instances when opinions differ. Be clear and avoid using ambiguous language which may be open to misinterpretation.
- Keep discussions relevant – make sure you clearly understand the purpose of the discussion. Stay on topic and avoid sharing irrelevant content as this may frustrate other users.

Focused:

- Students must not attempt to chat or set up private groups between each other on Microsoft Teams (this feature has been disabled for students).
- Students must not attempt to start or record a meeting/lesson (this feature has been disabled for students).
- Where background noise is unavoidable, students should leave themselves muted during a lesson and use the *hand up* feature to indicate they have a question. Students should only unmute themselves when directed by the teacher.

- Students must leave the lesson once instructed to do at the end of the lesson. The teacher must be the last person in the meeting to hang up.
- Students must not attempt to re-join a meeting once it has ended. The teacher will be notified if this is attempted. Students must leave the meeting at the end of the lesson.
- Students are not permitted to share recorded videos/lessons made by teachers to any person outside of St Mary's College.
- Students should blur their background during all online activities involving a camera or webcam.
- Be transparent – use your own name and photograph within your Office 365 profile. It is important that users are clear about who they are interacting with.
- Be safe – do not over disclose personal information and protect yourself against identity theft.
- Sharing images and videos – you should ensure that the sharing of images and videos does not breach image rights and copyrights. You must seek permission from anyone included in personal photographs prior to sharing them.
- Information shared within your Microsoft Teams site is for use by your site members only and should not be shared outside of the Microsoft Teams site without appropriate permissions.
- If you post inappropriately and later remove this post this may still be accessed by the College and used within disciplinary procedures as appropriate; such posts may lead to disciplinary action. The teacher will monitor usage and ensure inappropriate posts are removed.
- Microsoft Teams sites are created for use by students and teacher groups. External participants can only be invited by staff/teachers.
- Online lessons and meetings may be recorded to enable those unable to attend due to absence or ill health. This practice is in accordance with the College's commitment to inclusive practice which enables a rich learning environment, flexible learning and meets accessibility requirements. Recordings are solely for students' personal study and must not be reproduced or distributed to any third party, and must not be made available on any external website or social media channel.

When using the internet for research and recreation, students should recognise that:

- They should have permission to use the original work of others in their own work.
- Where work is protected by copyright, students will not try to download copies (including music and videos).
- When students are using the internet to find information, they should take care to check that the information accessed is accurate. Students should understand that the work of others may not be truthful and may be a deliberate attempt to mislead.

Mobile Phones/Mobile Technologies

Mobile Phones/technology devices may be a college owned/provided or privately-owned smartphone, smartwatch, tablet, notebook/laptop or other technology that usually has the capability of utilising the college's wireless network. These guidelines aim to promote safe, respectful and responsible use of mobile phones/technology by all members of the St Mary's community.

3. Student Agreement –Mobile Phones/Mobile Technologies:

Respectful use:

- Mobile phones and headphones must not be used when moving around the college site, in particular on corridors.
- Mobile phones can be used for learning with the teacher's permission, however the making or receiving of calls and text messages is not permitted, unless in an emergency.
- Mobile phones must not disrupt lessons with ringtones, beeping or music.
- No photographs, videos and images of students/staff should be captured via a personal mobile in any setting.
- It is forbidden for students to 'gang up' on another student and use their mobile phones to take pictures/videos of acts to denigrate and humiliate that student and then send the pictures to other students or upload to a website for public viewing. This also includes using mobile phones to photograph or film any student without consent. It is a criminal offence to use a mobile phone to menace, harass or offend another person and almost all calls, text messages and emails can be traced. As will all college incidents, the college may consider it appropriate to involve the police.
- Mobile phones are not to be used or taken into changing rooms or toilets or used in any situation that may cause embarrassment or discomfort to their fellow students, staff or visitors at the college.

Responsible use:

- It is the responsibility of students who bring mobile phones to college to abide by the guidelines outlined in this document.
- The college accepts no responsibility for replacing, lost, stolen or damaged mobile phones.

Safe use:

- It is strongly advised that student use passwords/pin numbers and keep these confidential.
- Students are reminded of the inappropriate behaviour, relating to materials which are illegal or inappropriate (as mentioned in bold on page 1)
- Students are strongly urged not to communicate with individuals unless they are known to them.

Exams:

Any student caught using a mobile phone in key assessments or exams will face disciplinary action as well as the consequences sanctioned by the applicable Awarding Body.

……………………………………………………………………………………………………

Student declaration:

I will:

- *Abide by the ICT Acceptable Use –Student Agreement set out in this document.*
- *Report any illegal, inappropriate or harmful material or incident to a member of staff immediately.*
- *Check emails regularly and read and respond to communication from the College*

Monitoring:

I understand that:

- *The internet is filtered and my activities on the network and via Microsoft Teams are logged and monitored, this also includes online lessons and emails.*
- *Online lessons may be recorded and herby give my permission to St. Mary's College to record lessons and meetings.*
- *Recorded lessons are for personal use only and I will not share them on social media, external websites or with a third party.*
- *Chat logs from both one-to-one and group chats can be provided in the event of misconduct or a complaint.*
- *The College has the right to take action against a student who is involved in an incident of inappropriate behaviour, relating to materials which are illegal or inappropriate (as mentioned in bold on page 1)*
- *If my behaviour is considered as inappropriate or violates the above standards*, I understand that this may result in my access being blocked and/or being dealt with under the College disciplinary procedures.*
- *The sharing of Confidential, Personal and Sensitive information increases the risk of data breaches and when breaches occur this may result in disciplinary action taken against the individual sharing the data.*

* Inappropriate posts: this may include posts that damage the reputation of individuals or the College, include defamatory comments that cause distress to members of our College community, that contain obscene content or breach civil or criminal law.

Student Signature:	
Date:	