G57 - Online Safety Policy

St Cyres School

Online Safety Policy

September 2021

Policy updated: August 2021
Approved by SLT: 15th September 2021
Ratified by the GB: 27th September 2021
Review date: September 2022

Section 1: Introduction

This policy applies to **all** members of the school community (including staff, pupils, volunteers, parents/guardians, visitors, community users) who have access to and are users of St Cyres School and its ICT systems, both in and out of the school.

In St Cyres School, we see technology and one to one technology in particular, as a vital element of our teaching and learning strategy and endeavour to ensure that all staff and pupils have access to relevant, authentic and highly effective resources. In many areas of school life, the use of technology is crucial. It is essential therefore that the availability, integrity and confidentiality of the technology systems and data are maintained at a level that is appropriate for our needs and are in line with the General Data Protection Regulations (GDPR). Online safety is a fundamental part of all areas of ICT, whether generic, cross curricular or for administrative purposes and, at St Cyres school, it is a priority across all areas of the school.

The Education and Inspections Act 2006 empowers headteachers to such an extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.
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 school Behaviour Policy.
The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / guardians of incidents of inappropriate Online Safety behaviour that take place out of school.

Section 2: Development/Monitoring/Review of the policy

St Cyres Online Safety policy has been developed by a working party group made up of a link Governor, the Senior Leadership Team, IT Manager, staff from the Digital Leaders working party group and members of the school Council. (Appendix A)

The Online 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 September 2022.

The school will monitor the impact of the policy using:

- Logs of reported incidents.
- Monitoring logs of internet activity (Smoothwall Filter Alerts).
- Internal monitoring data for network activity.
- Pupil voice.

- Parental voice.

Should serious online safety incidents take place, the following professionals will be informed:

- Ms U Hirani Assistant Headteacher and DSP.
- Mr P Lewis, Headteacher.
- Mr J Redrup, VoG Safeguarding Lead.
- South Wales Police.

Section 3: Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within St Cyres School:

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors' sub-committee receiving regular information about online safety incidents and monitoring reports.

The St Cyres School Designated Online Safety Governor is Mrs T Viner.
The role of the Online Safety Governor includes:

- Regular meetings with the Online Safety Coordinator.
- Regular awareness of online safety incident logs.
- Regular monitoring of Smoothwall filtering logs.
- Reporting to Governors at sub-committee meetings.

Headteacher and the Leadership Team

The Headteacher has a duty of care for ensuring the safety (including online safety) of all members of the school community. However, the day-to-day responsibility for online safety will be delegated to the Online Safety Coordinator and Leadership Team.

The Headteacher and Designated Senior Person for Safeguarding (DSP) will be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. **(Appendix B)**

The Headteacher and Leadership Team are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as appropriate. The Headteacher and Leadership Team will ensure that there is a system in place to allow for monitoring and support of those in school 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.

Online Safety Coordinator

Ms U Hirani (Assistant Headteacher & DSP) in coordination with Mr I Stark (IT Manager) are the named members of staff with a day-to-day responsibility for Online Safety. The online safety coordinator is **Ms U Hirani.**

The role of the Online Safety coordinator will include:

- Leading on Online Safety in the school.
- Taking day to day responsibility for online safety issues and reviewing the school's online safety policy and associated documents.
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Providing training and advice for staff.
- Liaising with the Local Authority where necessary.
- Liaising with school IT technical staff.
- Receiving reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- Meeting regularly with Online Safety Governor to discuss current issues.
- Reviewing incident logs and filtering logs.
- Attending relevant meetings and reports regularly to Leadership Team.

IT Manager

The IT Manager is responsible for ensuring:

- The school's technical infrastructure is secure and is not open to misuse or malicious attack.
- The school meets required online safety technical requirements and any Local Authority guidance.
- 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.
- They keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- The use of the network, internet, iPads, remote access and the email system is regularly monitored in order that any misuse/attempted misuse can be reported to the Online Safety Coordinator/ Designated Senior Person for Safeguarding (DSP).
- That monitoring software/systems are implemented and updated.

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up-to-date awareness of online safety matters and of the current school Online Safety Policy and practices.
- They have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP). *(New staff to sign following online safety briefing)*
- They report any suspected misuse or problem to the Online Safety Coordinator and DSP.

- All digital communications with pupils, parents/guardians should be on a professional level and only carried out using official school systems.
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- Pupils understand and follow the Online Safety Policy.
- Pupils 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 school activities (where allowed) and implement current policies with regard to these devices.
- All online resources have been checked for suitability and are appropriate for the age of the pupils accessing the resources e.g., hyperlinks, videos etc.

Designated Senior Person for Safeguarding

The DSP is trained in Online Safety issues and is aware of the potential for serious child protection and 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.
- Malicious and dangerous websites

In instances where these types of issues arise, staff that discover the concern must notify the safeguarding lead immediately. Escalation to the police may also be appropriate to remove such content from the web. CSC will be notified to remove any inappropriate apps and websites from their recommended lists where necessary.

Pupils

Pupils will have access to iPads in lessons and at home. As such, pupils:

- Are responsible for using the school digital technology systems in accordance with the iPad Acceptable Use Agreement.
- Need to 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/using images and on cyber-bullying.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school.

Parents/Guardians

Parents/Guardians play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, communications including letters, email and text. We have held information events for all year groups regarding online safety in previous years, currently Welsh Government guidance has not permitted this to take place over the last two years however, we will look to resume these sessions as soon as it is safe to do so. Parents are able to use of the school website to gain information about national/local online safety campaigns/literature.

Parents/Guardians will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events.
- Access to parents' sections of the website and online pupil records.

Section 4: Policy Statements

Education of pupils

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

Online safety is a focus in all areas of the curriculum and staff reinforce online safety messages across the curriculum. The online 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 safety curriculum as part of ICT and PHSE which is regularly revisited.
- Key online safety messages delivered as part of a planned programme of assemblies and TLC activities.
- Pupils are taught in lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils are 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 (*Counter Terrorism and Securities Act 2015).*
- Pupils are helped to understand the need for the pupil Acceptable Use Agreement and are encouraged to adopt safe and responsible use both within and outside school.
- Staff act as good role models in their use of digital technologies the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that pupils

are 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.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, pupils 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 IT support (and HoF as part of SoW liaison) temporarily remove those sites from the filtered list for the period of study. Any request to do so is audited by IT manager and kept in securely.

Education of parents/guardians

Many parents and carers have only a limited understanding of online safety risks and issues, yet they need to play an essential role in the education of their children and in the monitoring and regulation of their child's online behaviours. Parents may not be aware how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school therefore seeks to provide information and awareness to parents and carers through:

- Communication such as email, the school website, and twitter.
- Parents/Guardians evenings and information events.
- Reference to the relevant websites / publications e.g., swgfl.org.uk www.saferinternet.org.uk/
- Open evenings and inductions evenings.
- Transition events.

Education of the wider community

The school will provide opportunities for local community groups/members of the community to gain from the school's online safety knowledge and experience offered through the following:

- Providing induction to Year 7's in use of new digital technologies, digital literacy and online safety.
- The school website will provide online safety information for the wider community via a regularly updated thread with appropriate content and guidance.

Education and training for staff

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

- Online safety training will be made available to staff. This will be updated and reinforced annually.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety

Policy and Acceptable Use Agreements.

- It is possible that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Coordinator (or other nominated person) will receive regular updates through attendance at external training events (e.g., from SWGfL, the LA and other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updated versions will be presented to and discussed by all stakeholders in staff/team meetings and on INSET days.
- The Online Safety Coordinator (or other nominated person) will provide advice, guidance and training to individuals as and when required.

Education and training for governors

Governors will take part in online safety training/awareness sessions. The online safety coordinator will present the content of this policy in full governor meetings and sub-committees annually under the standing item; Safeguarding.

Section 5: Technical; infrastructure, filtering and monitoring

School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.

- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- All users (at KS3 and above) will be provided with a username by IT support who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password when necessary.
- The “master/administrator” passwords for the school IT system, used by the IT Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (RM STAFF).
- Mr I Stark 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 licenses purchased against the number of software installations (Inadequate licensing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs).
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the filtering provider, Smoothwall, by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored through Smoothwall. There is a clear process in place to deal with requests for filtering changes.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school has provided enhanced/differentiated user-level filtering (allowing

different filtering levels for different ages/key stages and different groups of users i.e., staff / pupils.)

- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for staff to report any actual/potential technical incident/security breach and pupils will be able to liaise with staff and ICT support team to solve any issues.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly.
- The school infrastructure and individual workstations are protected by up to date antivirus software.
- An agreed policy is in place through Head of School Administration/IT support for the provision of temporary access of "guests" (e.g., trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed acceptable use policy is in place regarding the extent of personal use that users (staff/pupils) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place that allows staff to download Apps from the App Store. However, IT support can stop the App working, and can monitor what is downloaded.
- An agreed policy is in place regarding the use of removable media (e.g., memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Section 6: Use of iPads as Mobile Technology

Mobile technology devices (iPads) are school owned/provided tablets which have the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning resources and other cloud-based services such as email and data storage. All users should understand that the primary purpose of the iPads in a school context is educational. Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's Online Safety education programme.

The school allows the following access:

Access	**School devices**	**Personal devices**

	School owned for single user	School owned for multiple users	Authorised device	Pupil owned	Staff owned	Visitor owned
Allowed in school	Yes	No	Yes	No	Yes	Yes
Full network access	Yes	No	Yes	No	No	No
Internet only	No	No	No	No	Yes	Yes
No network access	No	No	No	No	No	No

Please see User Agreements for pupils and staff.

Please also refer to the following policies: -

- School Internet Social Networking Policy
- Photographs, Videos and Digital Policy
- Mobile phone Policy
- Data Protection Policy - (GDPR Policy)

Section 7: Communications

A wide range of rapidly developing communications technologies have the potential to enhance learning. Please see Appendix C which shows how the school currently assesses the use of technologies for education purposes.

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

- The official school email service is regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g., by remote access).
- Users must immediately report, to the nominated person – in accordance with the school 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 pupils or parents/guardians (email, social media, chat, blogs, SIMS) must be professional in tone and content.
- These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils should be taught about online 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 school website and only official email addresses should be used to identify members of staff.

Personal Use

Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school 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 school are outside the scope of this policy.
Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.

Section 8: Careless, irresponsible or deliberate misuse

It is hoped that all members of the school community will be responsible in their use of digital technologies, who understand and follow school 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, the following steps 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 Headteacher/Chair of Governors 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.
    - Police involvement and possible action.

If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would Include:

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

It is important that all of the above steps are taken as they will provide an evidence trail for the school and where necessary, the police and will demonstrate that visits to these sites were carried out for safeguarding purposes.

Appendix A

Development/ Monitoring/ Review of this policy

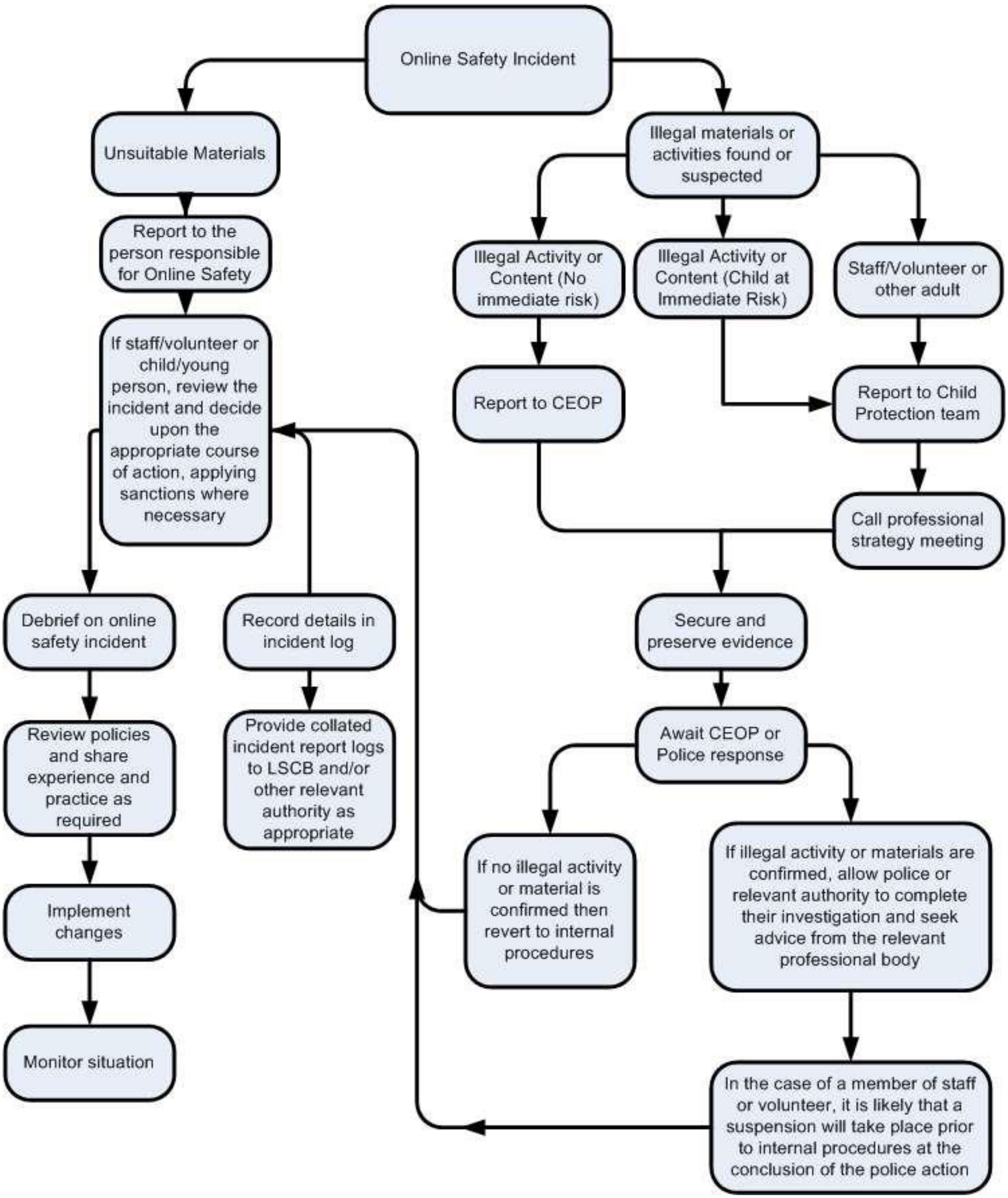
St Cyres Online Safety policy has been developed by a working party subgroup made up of:

Headteacher	Mr P Lewis
Assistant Headteacher & Online Safety Coordinator	Ms U Hirani
IT Manager	Mr I. Stark
Link Governor	Mrs T. Viner
Head of Faculty	Mr D Morgan
Digital Leaders staff	Mr Huw Thomas and Mr S McDonald.
Members of the School Council	Lucas Follon and Radhiya Islam

Appendix B

Responding to incidents of misuses

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 for responding to online 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
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or 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
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Appendix C

The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

	Staff and other adults				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobiles may be used in school	Y				Y* KS5			N
Use of mobiles in lessons	N	N	N	N	N			
Use of mobiles in social time	Y				N			
Ipads may be used in school	Y				Y			
Use of Ipads in lessons	Y				Y			
Use of Ipads in social time	Y				Y			
Taking photos on mobiles/cameras	N				N			
Taking photos on iPads		Y				Y		
Use of gaming devices	N				N			
Personal email in school or on network	Y						Y	
Use of messaging apps	Y				N			
Use of social media	Y				N			
Use of blogs	Y						Y	

** Years 12 and 13 have permission to use mobile phones ONLY in the 6th form area of the school.*

Appendix D

School Actions and Sanctions

It is more likely that the school 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 school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal disciplinary procedures as follows:

Refer to class teacher/LC	A
Refer to Head of Department/Year	B
Refer to Headteacher/SLT	C
Refer to Police	D
Refer to technical support staff for action	E
Inform parents / guardians	F
Removal of network/internet access rights	G
Warning	H
Further sanction e.g., detention/exclusion	I

Pupil Incident	A	B	C	D	E	F	G	H	I
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	
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	X
Unauthorised/inappropriate use of social media/ messaging apps/personal email/internet	X	X			X	X		X	X
Unauthorised downloading or uploading of files- N/A									
Allowing others to access school network by sharing username and passwords	X					X		X	
Attempting to access or accessing the school network, using another pupil's account	X					X		X	
Attempting to access or accessing the school network, using the account of a member of staff		X	X			X			X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	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

Actions which could bring the school/academy into disrepute or breach the integrity of the ethos of the school		X	X			X			X
Using proxy sites or other means to subvert the school’s filtering system	X	X			X	X			
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			X	X			
Deliberately accessing or trying to access offensive or pornographic material	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
Careless use of personal data e.g., holding or transferring data in an insecure manner	X	X							
Deliberate actions to breach data protection or network security rules		X			X	X			
Actions which could compromise the staff member’s professional standing	X	X	X		X	X			X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X		X	X			X
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X	X	X	X	X

Appendix E

Unsuitable and Inappropriate Activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school 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 school context, either because of the age of the users or the nature of those activities.

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

Acceptable	A
Acceptable at certain times	B
Acceptable for nominated users	C
Unacceptable	D
Unacceptable and illegal	E

	A	B	C	D	E
Child sexual abuse images – The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
Possession of an extreme pornographic image (grossly offensive, 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	X
Threatening behaviour, including promotion of physical violence or mental harm				X	X
Promotion of extremism or terrorism				X	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	X
Using school systems to run a private business				X	X

Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				X	
Infringing copyright				X	X
Revealing or publicising confidential or proprietary information (e.g., financial/personal information, databases, computer/network access codes and passwords)				X	X
Creating or propagating computer viruses or other harmful files				X	X
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)		X			
On-line gaming (non- educational)				X	
On-line gambling				X	
On line shopping, e-commerce				X	
File sharing				X	
Video broadcasting e.g., You tube				X	

Summary of changes to the policy since last update in 2018:

- Update of staff leading online safety
- Compliance with all relevant Legislation
- Update of staff, pupil and parental responsibilities
- Update of policy statements
- Alignment to behaviour for Learning policy for school actions and sanctions
- Update of unacceptable activities
- Update of school website information