St. Wulstan's Catholic Primary School

Online Safety Policy

Mission Statement

As a Catholic school, St Wulstan's seeks to enable each child to walk in faith with Christ, loving Him and each other. With the help of our families, our parish and our local community, we will do our best to use the gifts that God has given us to make our world a richer place.

Background

St Wulstan's Catholic Primary School believes that the Internet is an essential element in 21st century life for education, business and social interaction.

The purpose of Internet use in school is:

- To raise educational standards and promote pupil achievement.
- To support the professional work of staff.
- To enhance the school's management, information and administration systems.

At St Wulstan's Catholic Primary School we believe that we have a duty to provide students with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. We also acknowledge our responsibility to ensure that pupils use the Internet appropriately and safely.

The aim of this policy is to show how pupils, teachers, parents, Academy Representatives and the wider community can use this valuable resource and means of communication to enhance the learning experiences and life skills.

Educational benefits of the Internet

Benefits of using the Internet in education include:

- Access to world-wide educational resources including museums and art galleries.
- Inclusion in government and local initiatives.
- Educational and cultural exchanges between pupils world-wide.
- Cultural, social, vocational and leisure use in libraries, clubs and at home.
- Access to experts in many fields for pupils and staff.
- Staff professional development through access to national developments, educational materials and good curriculum practice.
- Communication with support services, professional associations and colleagues.
- Improved access to technical support including remote management of networks.
- Exchange of curriculum and administration data with the local authority and Department.

While developing technology brings many opportunities, it also brings risks and potential dangers of which these are just a few:

- Access to illegal, harmful or inappropriate images or other content
- Allowing or seeking unauthorised access to personal information
- Allowing or seeking unauthorised access to private data, including financial data
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive or addictive use which may impact on social and emotional development and learning

This policy sets out how we strive to keep children safe with technology while they are in school.

We recognise that children can often be more at risk when using technology at home (where we have no control over the technical structures put in place to keep them safe) and so this policy also sets out how we educate children about the potential risks. We also explain how we attempt to inform those people who work with our children beyond the school environment (parents, friends and the wider community) to be aware and to assist in this process.

St Wulstan's Catholic Primary School's online safety policy has been written from a template provided by the South West Grid for Learning.

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Academy Committee on:	July 2019
The implementation of this Online Safety policy will be monitored by the:	Online Safety Coordinator
Monitoring will take place at regular intervals:	Yearly
The Academy Committee will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Yearly
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:	July 2020
Should serious online safety incidents take place, the following external persons / agencies should be informed:	SLT, DSL, LADO, Police

The school 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 pupils/parents/carers/staff

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Principals to such 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 online-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 published 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/carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Roles and Responsibilities

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

Academy Committee Representatives

Academy Committee Representatives 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 Academy Committee Representatives receiving regular information about online safety incidents and monitoring reports. A member of the Academy Committee has taken on the role of Online Safety Academy Committee Representative. The role of the Online Safety Academy Committee Representative will include:

- regular meetings with the Online Safety Officer
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Academy Committee meetings

Principal and Senior Leaders

- The Principal has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Officer.
- The Principal and other members 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 at the end of this policy.)
- The Principal is responsible for ensuring that the Online Safety Officer and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Principal 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.
- The Principal will receive regular monitoring reports from the Online Safety Officer.

Online Safety Officer

The Online Safety Officer:

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents.
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff.
- liaises with the Local Authority/Saint Nicholas Owen MAC.
- liaises with school technical staff.
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- meets regularly with Online Safety Academy Committee Representative to discuss current issues, review incident logs and filtering / change control logs.
- attends relevant Academy Committee meetings.
- reports regularly to Senior Leadership Team.

Technical Staff

The Technical Staff are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- that the school meets required online safety technical requirements and any Local Authority/Saint Nicholas Owen MAC Online Safety Policy/Guidance that may apply.
- that users may only access the networks and devices through properly enforced password protection.
- 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 online safety role and to inform and update others as relevant.
- that the use of the network/internet/email is regularly monitored in order that any misuse/ attempted misuse can be reported to the Principal and Online Safety Officer for investigation.
- that monitoring software is implemented and updated when required.

Teaching and Support Staff

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 (see Appendix 1)
- they report any suspected misuse or problem to the Principal and Online Safety Officer for investigation.
- all digital communications with pupils/parents/carers 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 and acceptable use policies.
- 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, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- in lessons where internet use is pre-planned pupils 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 Designated Safeguarding Lead should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

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

Pupils

Pupils must:

- use the school digital technology systems in accordance with the Pupil 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.
- 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, if related to their membership of the school.

Parents/Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, websites and information about national local online safety campaigns. Parents and carers 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 / Learning Platform and on-line pupil records
- their children's personal devices in the school (where this is allowed)

Community Users

Community Users who access school systems/website as part of the wider school provision will be expected to sign a Community User Acceptable Use Agreement (AUA) before being provided with access to school systems. (See Appendix 5)

Policy Statements

Education - 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/digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should 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 should be provided as part of Computing/PHSE/other lessons and should be regularly revisited.
- Key online safety messages should be reinforced as part of a planned programme of assemblies.
- Pupils should be taught to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils 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.
- Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should 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 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.
- 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, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff 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 and approved in advance by the Principal and Online Safety Officer.

Education – Parents/Carers

Parents and carers may have a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate 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 will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, school website
- Parents/carers evenings / sessions
- 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 (see Appendix 9 for further links / resources)

Education – 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. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety.
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community
- Supporting community groups e.g. Early Years Settings, Childminders, youth/sports/voluntary groups to enhance their Online Safety provision.

Education & Training – Staff / Volunteers

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:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- 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 expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Officer will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings INSET days.
- The Online Safety Officer will provide advice/guidance/training to individuals as required.

Training – Academy Committee Representatives

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

- Attendance at training provided by the Local Authority/MAC/National Governors Association or other relevant organisation (e.g. SWGfL).
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

Technical – infrastructure / equipment, filtering and monitoring

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

- 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 KS2 and above) will be provided with a username and secure password by the Online Safety Officer 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 "administrator" passwords for the school ICT systems, used by the Technical Staff must also be available to the Principal and Senior Leaders and kept in a secure place.
- Technical Staff are 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 or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
- Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- 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 school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed procedure is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- Staff are prohibited from downloading executable files and installing programmes on school devices.

Mobile Technologies

The table below indicates which devices are allowed in school and the level of access they will be given to school systems:

	School Devices		Personal Devices		
	School owned for single user	**School owned for multiple users**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	Yes	Yes	Yes	Yes	Yes
Full network access	Yes	Yes	No	No	No
Internet only	No	No	No	Yes	Yes*
No network access	No	No	Yes	No	No

*****Only if authorised by the Principal/Vice Principal/Online Safety Officer

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet (images subject to Copyright must not be used without the permission of the copyright owner). However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school 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 pupils 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.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/social media/local press including physical sites outside of school.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act 2018). 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 pupils in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff (for example a 'phone) must not be used for such purposes.

- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with prior parental permission and good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation and in accordance with the St Nicholas Owen Catholic Multi Academy Company's Data Protection Policy and relevant Privacy Notice (as amended from time to time). A copy of these can be obtained on the web site www.stnicholasowen-mac.org.uk

The school must ensure that:

- It has a Data Protection Policy that is in line with General Data Protection Regulations.
- It has paid the appropriate fee to the Information Commissioner's Office (ICO).
- It has appointed a Data Protection Officer and a local School Data Champion.
- It will hold 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.
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice.
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIA) are carried out.
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller (see www.stnicholasowen-mac.org.uk for details of how to make such a request).
- There are clear and understood data retention policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
- All schools must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- All staff receive data handling awareness/GDPR training and are made aware of their responsibilities.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data 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.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media (which must only be school/MAC owned equipment):

- The data must be encrypted and password protected.
- The device must be password protected.
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Communications

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

	Staff & 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**
Mobile phones may be brought to the school	✓						✓	
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time		✓						✓
Taking photos on mobile phones / cameras				✓				✓
Use of other mobile devices e.g. tablets, gaming devices		✓						✓
Use of personal email addresses in school , or on school network		✓						✓
Use of school email for personal emails				✓				✓
Use of messaging apps				✓				✓
Use of social media				✓				✓
Use of blogs				✓				✓

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 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 /academy 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:

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

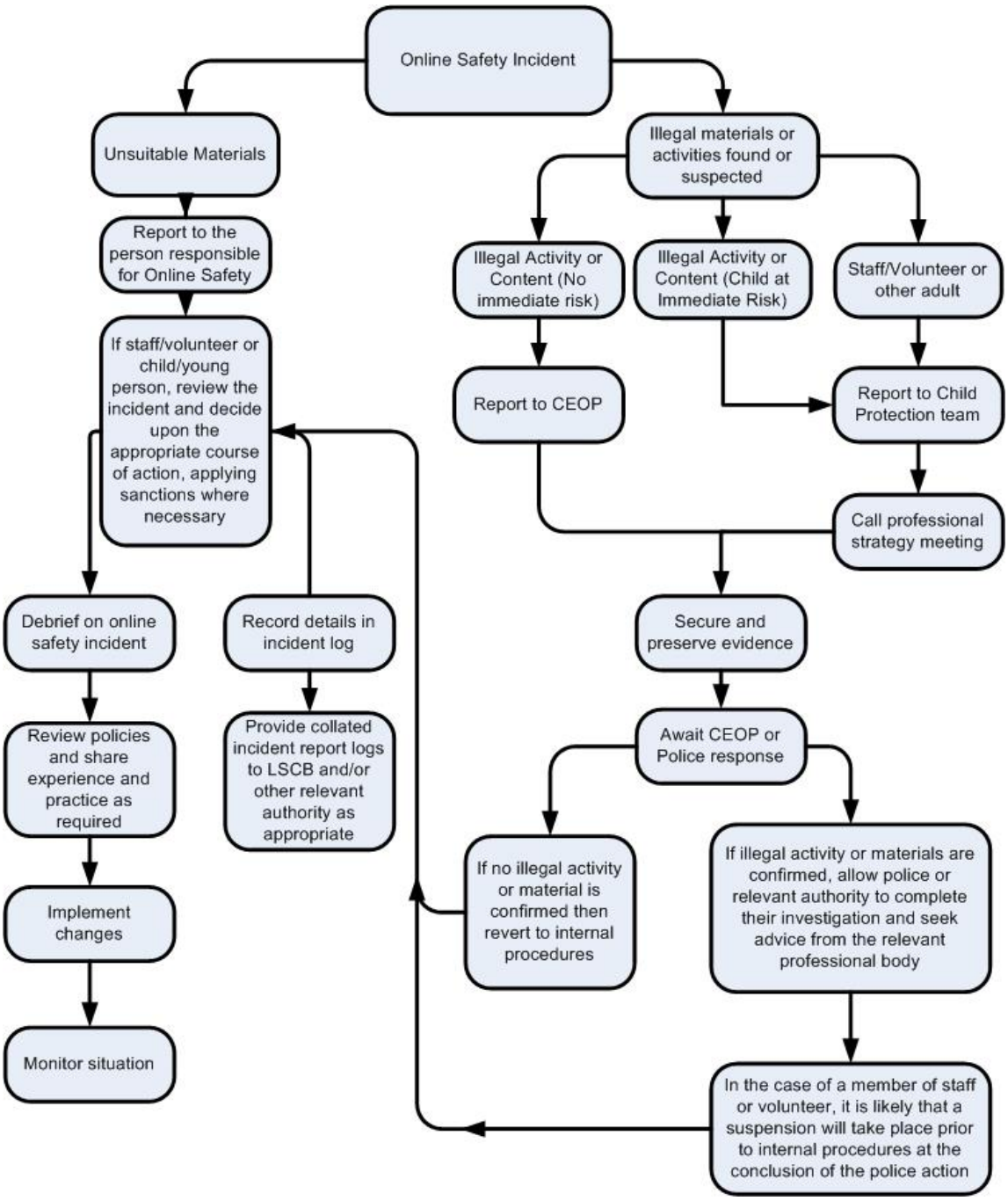
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)		X			
On-line gaming (non-educational)		X			
On-line gambling				X	
On-line shopping / commerce		X			
File sharing			X		
Use of social media			X		
Use of messaging apps				X	
Use of video broadcasting e.g. Youtube		X			

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

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 for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Debrief on online safety incident
Record details in incident log
Secure and preserve evidence
Review policies and share experience and practice as required
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Await CEOP or Police response
Implement changes
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
Monitor situation
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

Other Incidents

It is hoped that all members of the school community will be responsible users 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, 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 Senior Leadership Team 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/MAC or national/local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school 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 Senior Leadership Team for evidence and reference purposes.

School Actions & 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 behaviour / disciplinary procedures as follows:

	Actions / Sanctions								
Pupils Incidents	**Refer to class teacher / tutor**	**Refer to Online Safety Officer**	**Refer to Principal**	**Refer to Police**	**Refer to technical support staff for action re filtering / security etc.**	**Inform parents/carers**	**Removal of network / internet access rights**	**Warning**	**Further sanction eg detention / 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	X	X
Unauthorised use of non-educational sites during lessons	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	X	X	X		X	X		X	
Unauthorised downloading or uploading of files	X	X	X		X	X		X	
Allowing others to access school network by sharing username and passwords	X	X	X		X	X		X	
Attempting to access or accessing the school network, using another student's / pupil's account	X	X	X		X	X		X	
Attempting to access or accessing the school network, using the account of a member of staff	X	X	X		X	X	X	X	X
Corrupting or destroying the data of other users	X	X	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	X	X	X
Continued infringements of the above, following previous warnings or sanctions	X	X	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	X	X
Using proxy sites or other means to subvert the school's filtering system	X	X	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	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act 2018	X	X	X		X	X	X	X	X

	Actions / Sanctions							
Staff Incidents	**Refer to line managerr**	**Refer to Principal Principal**	**Refer to Local Authority / HR**	**Refer to Police**	**Refer to Technical Support 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).		X	X	X				
Inappropriate personal use of the internet / social media / personal email	X	X				X		
Unauthorised downloading or uploading of files	X	X				X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	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			X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X					X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X		X				X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils		X		X				X
Actions which could compromise the staff member's professional standing		X	X			X		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X						
Using proxy sites or other means to subvert the school's filtering system		X			X			X
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X		X	X		X
Deliberately accessing or trying to access offensive or pornographic material		X	X	X	X			X
Breaching copyright or licensing regulations		X			X	X		
Continued infringements of the above, following previous warnings or sanctions		X	X		X			X

Appendix 1

Staff (and Volunteer) Acceptable Use Agreement

This Acceptable Use Agreement is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school in the Online Safety Policy.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will be professional in my communications and actions when using school ICT systems.
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use social networking sites in school in accordance with the Saint Nicholas Owen MAC Social Media Policy.
- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- When I use my mobile devices (laptops/tablets/mobile phones/USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

In my use of school systems and equipment:

- All equipment allocated to staff remains the property of St Wulstan's Catholic Primary School and as such should be returned to the school either on demand or at the termination of any employment contract with the school.
- Users of allocated machines (laptops or iPads) are responsible for the physical security of the equipment. All machines are insured under the school's insurance policies. However, this cover does not extend to cases where the user could be deemed negligent, such as the laptop/iPad being left unattended in a car or public place. In these cases, staff would be personally liable.
- iPads must be kept in the Griffin Survivor protective cases that have been provided and ensure that the cases fully enclose the iPads at all times.
- Requests for software or apps must be given to the ICT Coordinator with at least two days' notice before it can be used for teaching and learning. The purchase of apps is not guaranteed, consideration will have to be given to the cost of the app and time needed to sync apps to all the iPads.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.

- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Saint Nicholas Owen MAC GDPR Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based protected and restricted data must be held in lockable storage.
- I understand that the Saint Nicholas Owen MAC GDPR Policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Agreement applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, a referral to Academy Committee Representatives and/or the Local Authority and, in the event of illegal activities, the involvement of the police.
- I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name	
Signature	
Date	

Allocated Machine Information

Laptop Make	
Serial Number	
iPad Serial Number	
Signed	
Date	

Appendix 2

Parent/Carer Acceptable Use Agreement

Name of child/children	
Year Group/s	

This Acceptable Use Agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Agreements are attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents are requested to countersign each child's Acceptable Use Agreement as well agreeing to certain conditions below as to show their support of the school in this important aspect of the school's work. Please respond to each statement with a tick and sign in the space provided.

	As the parent/carer, I give permission for my son/daughter to have access to the internet and to ICT systems at school.
	I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
	I understand that my son's / daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.
	I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Parent Name	
Parent Signature	
Date	

Please see the Saint Nicholas Owen MAC GDPR policy for information on how we collect, use, store, share and destroy any personal data collected.

Appendix 3

Pupil Acceptable Use Agreement (EYFS/Key Stage 1)

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/tablets.
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will not use the computers/tablets to be unkind to anyone.
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer/tablet.

I acknowledge that I have read through the above conditions with my child and that they understand the rules regarding computer and online safety.

Name of Child	
Year	
Parent Name	
Parent Signature	
Date	

Appendix 4

Pupil Acceptable Use Agreement (Key Stage 2)

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details etc.)
- I will not arrange to meet people off-line that I have communicated with on-line.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

When Using School Systems and Equipment

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.
- I will only use my own personal devices (mobile phones / USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will not attempt to use social media sites within school.

Research

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

Respecting Others

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others; I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

Consequences/Sanctions

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities, involvement of the police.

Please complete the sections below to show that you have read, understood and agree to the rules included in this Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I use my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, VLE, website etc.

Name	
Year	
Signature	
Date	

I confirm that my child has read and understands the above conditions.

Parent Name	
Parent Signature	

Appendix 5

Acceptable Use Agreement for Community Users

This Acceptable Use Agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices.
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential risk in their use of these systems and devices.

Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school:

- I understand that my use of school systems and devices and digital communications will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and/or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

Please respond to each statement with a tick and sign in the relevant space below.

	I understand that if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school systems/devices.
	I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name	
Signature	
Date	

Appendix 6

Record of reviewing devices/internet sites (responding to incidents of misuse)

Date	
Reason for investigation	
Details of first reviewing person	
Name	
Position	
Signature	
Details of first reviewing person	
Name	
Position	
Signature	
Name and location of computer used for review (for web sites)	

Website address/device	**Reason for concern**

Conclusion
Actions proposed/taken

Appendix 7

Reporting Log						
Date	**Time**	**Incident**	**Action Taken**		**Incident Reported By**	**Signature**
			What?	**By Whom?**		

Appendix 8

Training Needs Audit Log				
Relevant training the last 12 months	**Identified Training Need**	**To be met by**	**Cost**	**Review Date**

Appendix 9

Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy:

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

Others
LGfL – Online Safety Resources
Kent – Online Safety Resources page
INSAFE / Better Internet for Kids - https://www.betterinternetforkids.eu/
UK Council for Child Internet Safety (UKCCIS) - www.education.gov.uk/ukccis
Netsmartz - http://www.netsmartz.org/

Tools for Schools
Online Safety BOOST – https://boost.swgfl.org.uk/
360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/
360Data – online data protection self review tool: www.360data.org.uk
Bullying / Online-bullying / Sexting / Sexual Harrassment
Enable – European Anti Bullying programme and resources (UK coordination / participation through SWGfL & Diana Awards) - http://enable.eun.org/
Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
Scottish Government - Better relationships, better learning, better behaviour - http://www.scotland.gov.uk/Publications/2013/03/7388
DfE - Cyberbullying guidance - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Principals_and_School_Staff_121114.pdf
Childnet – Cyberbullying guidance and practical PSHE toolkit: http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit
Childnet – Project deSHAME – Online Sexual Harrassment
UKSIC – Sexting Resources
Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm
Ditch the Label – Online Bullying Charity
Diana Award – Anti-Bullying Campaign

Social Networking
Digizen – Social Networking
UKSIC - Safety Features on Social Networks
Children's Commissioner, TES and Schillings – Young peoples' rights on social media

Curriculum
SWGfL Digital Literacy & Citizenship curriculum
UKCCIS – Education for a connected world framework
Teach Today – www.teachtoday.eu/
Insafe - Education Resources
Mobile Devices / BYOD
Cloudlearn Report Effective practice for schools moving to end locking and blocking
NEN - Guidance Note - BYOD

Data Protection
360data - free questionnaire and data protection self review tool
ICO Guide for Organisations (general information about Data Protection)
ICO Guides for Education (wide range of sector specific guides)
DfE advice on Cloud software services and the Data Protection Act
ICO Guidance on Bring Your Own Device
ICO Guidance on Cloud Computing
ICO - Guidance we gave to schools - September 2012
IRMS - Records Management Toolkit for Schools
NHS - Caldicott Principles (information that must be released)
ICO Guidance on taking photos in schools
Dotkumo - Best practice guide to using photos

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

Infrastructure / Technical Support
UKSIC – Appropriate Filtering and Monitoring
Somerset - Questions for Technical Support
NEN – Advice and Guidance Notes

Working with parents and carers
SWGfL Digital Literacy & Citizenship curriculum
Online Safety BOOST Presentations - parent's presentation
Vodafone Digital Parents Magazine
Childnet Webpages for Parents & Carers
Get Safe Online - resources for parents
Teach Today - resources for parents workshops / education
The Digital Universe of Your Children - animated videos for parents (Insafe)
Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide
Insafe - A guide for parents - education and the new media

Research
EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011
Futurelab - "Digital participation - its not chalk and talk any more!"
Ofcom –Media Literacy Research

Glossary of Terms

AUP / AUA	Acceptable Use Policy / Agreement – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
FOSI	Family Online Safety Institute
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by NAACE
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MAC	Multi Academy Company
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational online safety programmes for schools, young people and parents.
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol
UKSIC	UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.

Copyright of the SWGfL School Online Safety Policy Templates is held by SWGfL. Schools and other educational institutions are permitted free use of the templates. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL and acknowledge its use.
Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in April 2016. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal / professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with school conduct or discipline.

Signed: _____ Principal

Signed: _____ Academy Representative

Date: _____