



# ST MARY'S CATHOLIC PRIMARY SCHOOL

## Online Safety Policy

# Contents

Online Safety Policy.....	1
Development / Monitoring / Review of this Policy.....	4
Schedule for Development / Monitoring / Review .....	4
Scope of the Policy.....	4
Roles and Responsibilities .....	5
Governors / Board of Directors .....	5
Headteacher and Senior Leaders.....	5
Network Manager / Technical staff.....	6
Teaching and Support Staff.....	6
Students / Pupils:.....	7
Parents / Carers .....	7
Policy Statements.....	7
Education – Students / Pupils .....	7
Education – Parents / Carers.....	8
Education – The Wider Community .....	9
Education & Training – Staff / Volunteers .....	9
Technical – infrastructure / equipment, filtering and monitoring .....	9
Mobile Technologies (including BYOD/BYOT).....	10
Use of digital and video images .....	11
Data Protection.....	12
Communications.....	13
Social Media - Protecting Professional Identity.....	14
Dealing with unsuitable / inappropriate activities .....	15
Responding to incidents of misuse .....	17
Illegal Incidents .....	18
Other Incidents .....	19
School / Academy Actions & Sanctions.....	20
Acknowledgements.....	23
Appendix 1 – Staff/ Volunteer Acceptable Use Policy.....	24
Appendix 2 – Pupil Acceptable Use Policy.....	27

Appendix 3 – Record of reviewing and responding to incidents of misuse .....	31
Record of reviewing devices / internet sites (responding to incidents of misuse) .....	31
Appendix 4 – Reporting Log .....	32
Reporting Log .....	32

## Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by:

- Headteacher / Senior Leaders
- Staff – including Teachers, Support Staff, Technical staff
- Governors / Board
- Parents/ carers
- Pupils

Consultation with the whole school / academy community has taken place in a variety of ways.

## Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Board of Directors / Governing Body / Governors Sub Committee on:	<i>Insert date</i>
The implementation of this Online Safety policy will be monitored by the:	<i>Headteacher, SLT and Assets committee</i>
Monitoring will take place at regular intervals:	<i>Once a year</i>
The Assets Committee will receive a report on the implementation of the Online Safety Policy generated by the Head teacher and Computing Co-ordinator (which will include anonymous details of online safety incidents) at regular intervals:	<i>Mid year</i>
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:	<i>November 2019</i>
Should serious online safety incidents take place, the following external persons / agencies may be informed:	<i>LA Safeguarding Officer, Plymouth CAST, LADO, Police</i>

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- Surveys / questionnaires

## Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers / Principals to such extent as is reasonable, to regulate the behaviour of students / 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 (see appendix for template policy). 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:

### Governors / Board of Directors

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 Assets Committee receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor, as part of their role as Safeguarding Governor. The role of the Online Safety Governor will include:

- regular meetings with the Head teacher
- regular monitoring of online safety incident logs
- reporting to Governors

### Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community. At St Mary's the Head teacher is also the Online Safety co-ordinator and Designated Safeguarding Lead.
- The Headteacher and another member of the Senior Leadership Team are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority disciplinary procedures.
- The Headteacher is responsible for ensuring staff receive suitable training to enable them to carry out their online safety roles.
- 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 / MAT / relevant body
- 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 Governor to discuss current issues, review incident logs and filtering / change control logs
- reports regularly to Senior Leadership Team
- is trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues that might arise from: sharing of personal data, access to illegal / inappropriate materials, inappropriate on-line contact with adults / strangers, potential or actual incidents of grooming and online-bullying.

## Network Manager / Technical staff

The IT Technician is 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 as recommended by Devon LA and SWGFL
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- 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 is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher/ Online Safety Officer for investigation / action / sanction

## 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)
- they report any suspected misuse or problem to the Headteacher / Online Safety for investigation / action / sanction
- all digital communications with students / 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

- students / pupils understand and follow the Online Safety Policy and acceptable use policies
- students / pupils have a good understanding of research skills and the need to avoid plagiarism
- 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
- in lessons where internet use is pre-planned students / 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

## Students / Pupils:

- are responsible for using the school's digital technology systems in accordance with the Student / Pupil Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should also know and understand policies on the taking / use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of 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, school website and information about national / local online safety campaigns / literature. 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.

## Policy Statements

### Education – Students / 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 in all lessons 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 / academy.
- 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 students / 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, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

## Education – Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their 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, web site*
- *Parents / Carers evenings / sessions*
- *High profile events / campaigns e.g. Safer Internet Day*
- *Reference to the relevant web sites / publications e.g. [www.swgfl.org.uk](http://www.swgfl.org.uk) [www.saferinternet.org.uk/](http://www.saferinternet.org.uk/)  
<http://www.childnet.com/parents-and-carers>*

## Education – The Wider Community

The school will provide opportunities for 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.

## 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.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school / academy Online Safety Policy and Acceptable Use Agreements.
- Some staff may identify online safety as a training need within the performance management process.
- 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 – Governors / Directors

Governors should take part in online safety training / awareness sessions. This may be offered in a number of ways:

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

## 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:

- 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 / academy technical systems and devices.
- All users will be provided with a username and secure password by the IT technician and School Bursar who will keep an up to date record of users and their usernames.
- The “administrator” passwords for the school ICT systems, used by the Network Manager (or other person) must also be available to the Headteacher / School Bursar and kept in a secure place.
- IT Technician will liaise with the Head teacher in 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**
- 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 policy is in place for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems. This is granted by the use of a “guest” username and password.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

## Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has 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 platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school policies including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school’s Online Safety education programme. **The** school Acceptable Use Agreements for staff, pupils/students and parents / carers will give consideration to the use of mobile technologies.

- The school allows:

	School Devices			Personal Devices		
	School owned for single user	School owned for multiple users	Authorised device <sup>1</sup>	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	Yes (if kept in school office)	Yes	Yes
Full network access	Yes	Yes	Yes	No	Yes	No
Internet only				No	Yes	Yes

## 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. 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 students / pupils are published on the school website / social media / local press
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.

- Staff 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 should 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 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 student / pupil and parents or carers.

## Data Protection

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

The school must ensure that:

- It has a Data Protection Policy
- It has paid the appropriate fee to the Information Commissioner's Office (ICO).
- It has appointed a Data Protection Officer (DPO).
- 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.
- 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.
- Consideration has been given to the protection of personal data when accessed using any remote access solutions.

- 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 / data protection 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:

- The data must be encrypted and password protected.
- The device must be password protected.
- The data must be securely deleted from the device, 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:

Communication Technologies	Staff & other adults			Students / Pupils				
	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 / academy	x					x		
Use of mobile phones in lessons				x				x

Use of mobile phones in social time		X						X
Taking photos on school cameras	X				X			
Use of other mobile devices e.g. tablets, gaming devices				X				X
Use of personal email addresses in school / academy , or on school / academy network		X						X
Use of school / academy email for personal emails				X				X
Use of messaging apps		X						X
Use of social media		X						X
Use of blogs		X					X	

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- 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 / carers must be professional in tone and content. These communications may only take place on official (monitored) school / academy systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class email addresses may be used at KS1, while pupils at KS2 and above will be provided with individual school / academy email addresses for educational use.
- Students / 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.

## Social Media - Protecting Professional Identity

All schools, academies, MATs and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies, MATs and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

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

- Ensuring that personal information is not published

- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the 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

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.
- The school should effectively respond to social media comments made by others according to a defined policy or process.

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety Group to ensure compliance with the school policies. Online Safety BOOST includes Reputation Alerts that highlight any reference to the school/academy in online media (newspaper or social media for example) <https://boost.swgfl.org.uk/>)

## 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 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 / academy context and that users, as defined below, should not engage in these activities in / or outside the school when using school / academy equipment or systems. The school policy restricts usage as follows:

		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	

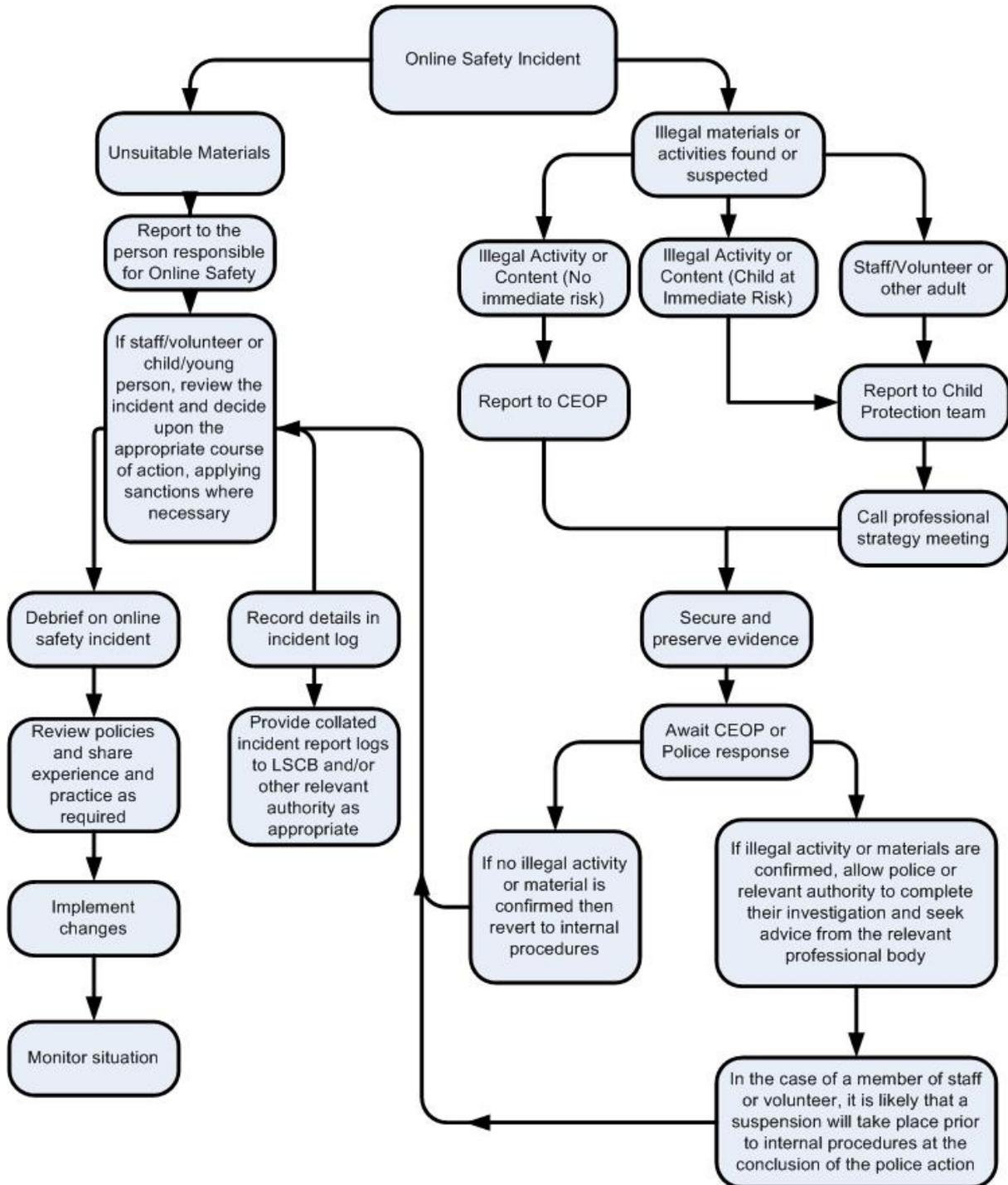
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy				X	
Infringing copyright				X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network 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 (when downloaded at home)		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 (see "User Actions" above).

## Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



## 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 group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by Local Authority / Academy Group 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 group for evidence and reference purposes.

## School / Academy Actions & Sanctions

It is more likely that the school / academy 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:

Students / Pupils Incidents	Refer to class teacher / tutor	Refer to Headteacher / 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					
Unauthorised use of non-educational sites during lessons		X			X			
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device		X			X			
Unauthorised / inappropriate use of social media / messaging apps / personal email		X			X			
Unauthorised downloading or uploading of files		X			X	X		
Allowing others to access school / academy 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	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	X			X	X		
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X			X	X		
Continued infringements of the above, following previous warnings or sanctions	X			X			
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X			X		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	
Deliberately accessing or trying to access offensive or pornographic material	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	

## Staff Incidents

	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
<b>Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).</b>	X	X	X	X	X	X
Inappropriate personal use of the internet / social media / personal email			X	X	X	X
Unauthorised downloading or uploading of files			X	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	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	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 students / pupils				X	X	X
Actions which could compromise the staff member's professional standing				X	X	X
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy				X	X	X
Using proxy sites or other means to subvert the school's / academy'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
Breaching copyright or licensing regulations				X	X	X
Continued infringements of the above, following previous warnings or sanctions				X	X	X

## Acknowledgements

SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School Online Safety Policy Template and of the 360 degree safe Online Safety Self Review Tool:

- Members of the SWGfL Online Safety Group
- Avon and Somerset Police
- Representatives of SW Local Authorities
- Plymouth University Online Safety
- NEN / Regional Broadband Grids

Copyright of these Template Policies is held by SWGfL. Schools / Academies and other educational institutions are permitted free use of the Template Policies for the purposes of policy writing, review and development. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL ([onlinesafety@swgfl.org.uk](mailto:onlinesafety@swgfl.org.uk)) and acknowledge its use.

Every effort has been made to ensure that the information included in this document is accurate, as at the date of publication in April 2018. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material.

© South West Grid for Learning Trust Ltd 2018

## Appendix 1 Staff/ Volunteer Acceptable Use Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

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 / academy 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 Policy 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 students / 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 St Mary's School will monitor my use of the school digital technology and communications systems.
- 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 St Mary's 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. 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 communicate with students / 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.

The school, Multi Academy Trust and local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the St Mary's School:

- When I use my mobile devices 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 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 ensure that my data is regularly backed up. This is carried out by St Mary's School.
- 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 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 has been agreed with the head teacher.
- I will not disable or cause any damage to school / academy equipment, or the equipment belonging to others.
- Where digital personal data is transferred outside the secure local network, it must be encrypted.
- I understand that data protection 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 St Mary's 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 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 be a warning, a suspension, referral to Governors / Directors 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.

Staff / Volunteer Name: .....

Signed: .....

Date: .....

## Appendix 2 – Pupil Acceptable Use Policy

### i) Parent / Carer Acceptable Use Agreement for younger pupils (Foundation Stage / KS1)

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

#### **This Acceptable Use Policy 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 / academy 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 Policy is 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 sign the permission form below to show their support of the school in this important aspect of the school's work.

#### **Permission**

I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I understand that the school has discussed the Acceptable Use Agreement with my son / daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of 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's / Carer's Name: ..... Signed.....

## i) Acceptable Use Policy Agreement (KS2 Pupils)

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, financial details, etc. )
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

### **I understand that everyone has equal rights to use technology as a resource and:**

- 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 (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 use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube).
- I will act as I expect others to act toward me:
- 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.

### **I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:**

- I will only use my own personal devices for example, USB pen key, in school if I have permission. I understand that, if I do use my own devices in 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.

**When using the internet for research or recreation, I recognise that:**

- 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.

**I understand that I am responsible for my actions, both in and out of school:**

- 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 Policy Agreement, there may be a consequence such as loss of access to the school network / internet, contact with parents and in the event of illegal activities involvement of the police.

## Student / Pupil Acceptable Use Agreement Form

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

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 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, website, etc.

Name of Pupil: .....

Class: .....

Signed: .....

Date: .....

## ii) Parent / Carer Acceptable Use Agreement (KS2)

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

**This Acceptable Use Policy 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 / academy 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 Policy is 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 sign the permission form below to show their support of the school in this important aspect of the school's work.

### **Permission**

I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I know that my son / daughter will be discussing the Acceptable Use Agreement in class which they will then be asked to sign and my son / daughter has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of 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's / Carer's Name: .....Signed.....

## Appendix 3 – Record of reviewing and responding to incidents of misuse

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

Group: .....

Date: .....

Reason for investigation: .....

.....

.....

.....

#### Details of first reviewing person

Name: .....

Position: .....

Signature: .....

#### Details of second reviewing person

Name: .....

Position: .....

Signature: .....

#### Name and location of computer used for review (for web sites)

.....

.....

Web site(s) address / device	Reason for concern

#### Conclusion and Action proposed or taken


## Appendix 4 – Reporting Log

### Reporting Log

Group: .....

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		
