

Blessed Sacrament Catholic Primary School



Online Safety Policy

“Aim high – live life to the full”

Written By	J. Griffin
Ratified by Governors	
Date for review	Summer 2019
Signed Chair of Governors	
Signed Headteacher	C Davey



Development / Monitoring / Review of this Policy

This online safety policy has been developed by the Computing Curriculum Team Leader.

- *Headteacher: Mr C. Davey*
 - *Designated Safeguarding Officer: Mrs. J. Griffin*
 - *Deputy Designated Safeguarding Officer: Mrs. E. Crist*
- *Online safety Officer / Coordinator: Mrs J. Griffin*
- *Computing Team: Miss E. Shaw, Miss G. Shaw*
- *Governors*

The online safety is a regular agenda in Computing Team meetings.

Schedule for Development / Monitoring / Review

This online safety policy was approved by the <i>Governing Body</i> :	Autumn 2018
The implementation of this online safety policy will be monitored by the:	<i>SMT</i> <i>Online safety Coordinator, Computing Team</i>
Monitoring will take place at regular intervals:	Annually
The <i>Governing Body</i> 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:	Annually
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:	Summer 2019
Should serious online safety incidents take place, the following external persons / agencies should be informed:	Mrs. J. Griffin

The school will monitor the impact of the policy using:

- *Logs of reported incidents*
- *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 Computing systems, both in and out of the *school*.

The Education and Inspections Act 2006 empowers Headteachers 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 cyber-bullying, or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the 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

Governors:

Governors are responsible for the approval of the Online safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors* 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*

The role of the *Online safety Governor* will include:

- *regular meetings with the Online safety Co-ordinator*
- *reporting relevant information or incidents to Governors*

Headteacher:

- **The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community**, through the day to day responsibility for online safety will be delegated to the *Online safety Co-ordinator*.
- **The Headteacher and the Designated Safeguarding Officer 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.**
- The Headteacher and Senior Leaders are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher and Senior Leaders 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 Senior Leadership Team will receive regular monitoring reports from the Online safety Co-ordinator.

Online Safety Coordinator:

The Online Safety Coordinator is the Assistant Head teacher and the Designated Safeguarding Officer.



- leads the online safety committee
- 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 Safeguarding Officer / 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
- attends relevant meeting
- reports regularly to Senior Leadership Team

Network Manager / Technical staff: Internet Provider BT / MGL

The Network Manager Technical Staff and Co-ordinator for Computing 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 and any Local Authority and BT (the Network Provider) Online safety Policy and Guidance that may apply.**
- **that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.**
- the filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (see appendix 'Technical Security Policy Template')
- 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 / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher C. Davey, Senior Leader J. Griffin; Online safety Coordinator / Officer E. Shaw for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies.

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current *school* online safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the Headteacher, Senior Leader ; Online safety Coordinator for investigation / action / sanction
- 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 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, 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 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.

Child Protection and Safeguarding Officer: J. Griffin

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
- cyber-bullying

Online safety Group: Computing Curriculum Team

The Online safety Group provides a consultative group called the Computing Curriculum Team, that has wide representation from the school, with responsibility for issues regarding online safety and the monitoring the online safety policy including the impact of initiatives. Depending on the size or structure of the school this committee may be part of the safeguarding group. The group will also be responsible for regular reporting to the Governing Body.

Members of the Online safety Group will assist the Online safety Coordinator with:

- the production / review / monitoring of the school online safety policy / documents.
- the production / review / monitoring of the school filtering policy (refer to the internet provider, BT's, Service Level Agreement and requests for filtering changes).
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the pupils about the online safety provision
- monitoring improvement actions identified through use of the 360 degree safe self review tool

Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online safety Policy covers their actions out of school, 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, 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
- access to parents' sections of the website.

Community Users: Extended Services

Community Users who access the school website and systems as part of the wider school provision will be expected to sign a Volunteer User AUA before being provided with access to school systems.

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 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 and pastoral activities
- 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 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, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (MGL) 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 on-line 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, safeguarding 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 www.saferinternet.org.uk/ <http://www.childnet.com/parents-and-carers>*

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:

- 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.
- The Online safety Coordinator will receive regular updates through attendance at external training events (e.g. from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online safety Coordinator will provide advice / guidance / training to individuals as required.

Training – Governors

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

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant online 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 infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the 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 academy 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 Ks 1 & KS2 will be provided with a username and secure password for My Maths, Purple Mash, Education City and Reading Plus. MGL technical support, class teachers and the Online Safety Coordinator will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password. KS1 & 2 children will be issued with a year group username and login for using the laptops that must be updated and changed every year.**
- **The “master / administrator” passwords for the school COMPUTING system, used by technical support (MGL) also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe).**
- **The Computing Team and MGL 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. There is a clear process in place to deal with requests for filtering changes.
- The school has provided enhanced / differentiated user-level filtering allowing different filtering levels for different groups of users –i.e. staff / pupils .
- Headteacher regularly monitors and records the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to inform the Headteacher, Senior leader or Online safety Officer/Coordinator.
- Appropriate security measures are in place by the Network Provider 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” (e.g. trainee teachers, supply teachers) onto the school systems.
- An agreed policy is in place (Computing policy, iPad AUP) that forbids staff from downloading executable files and installing programmes or apps on school devices.
- An agreed policy is in place restricting the use of removable media (e.g. memory sticks or CDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Bring Your Own Device (BYOD)

- The school has a set of clear expectations and responsibilities for all users in regard to mobile phones in school.
- Staff are not allowed to use mobile phones in classrooms or areas where pupils are present.
- Pupils are restricted from bringing in their own devices into school. Only Year 6 pupils are allowed to bring in personal mobile phones for security purposes. The mobile phone must be passed onto their class teacher every morning, to be locked away safely, and returned by the class teacher at the end of the school day.

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.**
- 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 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 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.*
- *Written permission from parents or carers will be obtained before photographs of pupils are published on the school website (this is part of the AUA signed by parents or carers at the start of the year).*
- *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 Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school must ensure that:

- **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.**
- **Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.**
- **All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".**
- **It has a Data Protection Policy.**
- **It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)**
- **It has clear and understood arrangements for the security, storage and transfer of personal data.**
- **Data subjects have rights of access and there are clear procedures for this to be obtained.**
- **There are clear and understood policies and routines for the deletion and disposal of data.**
- **There is a policy for reporting, logging, managing and recovering from information risk incidents.**



- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties.
- There are clear policies about the use of cloud storage / cloud Computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

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.

Removable media is not permitted on the school network. This includes any personal files/programs/apps on any portable computer system, memory stick or any other removable media.

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 and other adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed
Mobile phones may be brought to school	X				X			
Use of mobile phones in lessons				X				X
Use of mobile phones in social time		X						X
Taking photos on mobile phones / cameras				X				X
Use of other mobile devices e.g. tablets, gaming devices	X							X
Use of personal email addresses in		X						X



school, or on school network								
Use of school 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 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.** *Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).*
- **Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.**
- **Any digital communication between staff and pupils or parents / carers (email) must be professional in tone and content.** *These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.*
- *Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.*
- *Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.*

Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority 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 limiting access to personal information:

- Training to include: 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 or local authority



- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and online safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Unsuitable / inappropriate 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 school or outside 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	
	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		



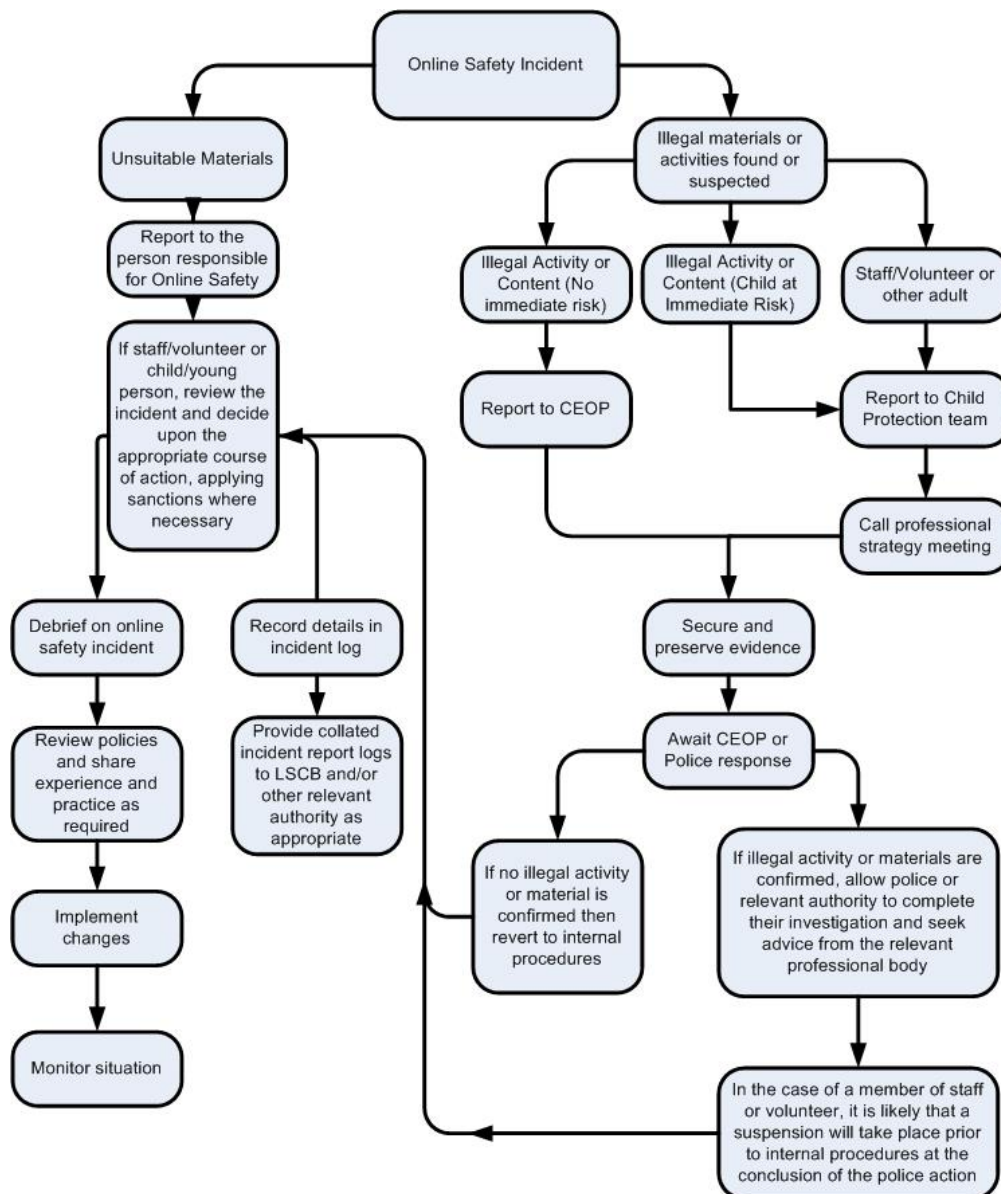
On-line gambling				X	
On-line shopping / commerce				X	
File sharing				X	
Use of social media		X			
Use of messaging apps		X			
Use of video broadcasting e.g. YouTube			X		

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) 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 / academy 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 / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.



- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
 - Internal response or discipline procedures
 - Involvement by Local Authority or national / local organisation (as relevant).
 - Police involvement and/or action
- **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
 - incidents of 'grooming' behaviour
 - the sending of obscene materials to a child
 - adult material which potentially breaches the Obscene Publications Act
 - criminally racist material
 - 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 child protection purposes. The completed form should be retained by the group 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:



Staff

Actions / Sanctions

Incidents:	Refer to line manager	Refer to Headteacher	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							
Unauthorised downloading or uploading of files	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			
Careless use of personal data eg holding or transferring data in an insecure manner		X				X		
Deliberate actions to breach data protection or network security rules						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							
Actions which could compromise the staff member's professional standing	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							
Deliberately accessing or trying to access offensive or pornographic material						X	X	X
Breaching copyright or licensing regulations	X							
Continued infringements of the above, following previous warnings or sanctions						X	X	X



Appendices:

1. Acceptable Use Policies- Pupils, Staff and Volunteers
2. School Technical Support Policy
3. Filtering Policy
4. School Policy – Online safety Committee Terms of Reference



Appendix 1

School Acceptable Use Policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These 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. 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 digital 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.

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.

Acceptable Use Policy Agreements

Pupil Acceptable Use Policy Agreement – for KS1 pupils

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 and iPads.

I will only use activities that a teacher or suitable adult has told or allowed me to use.

I will take care of the computer, iPads 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 or iPad.

Signed (parent):



Pupil Acceptable Use Policy Agreement – for KS2 pupils

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

This is how we stay safe when we use computers:

I will keep my username and password safe and secure, I will not share it nor will I try to use another person's username and password.

I will ask a teacher or suitable adult if I want to use the computers and iPads.

I will only use activities that a teacher or suitable adult has told or allowed me to use.

I will be aware of stranger danger when communicating online.

I will not disclose or share personal information about myself or others when online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, etc.)

I will not arrange to meet with anyone I have communicated with online, if somebody asks to meet me online I will tell a responsible adult.

I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.

I will not download anything in school UNLESS directed by an adult.

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 opinion.

I will not take or distribute images of anyone without their permission.

I will not try to upload, download or access any material that is inappropriate nor will I try to get around the school's filtering system.

I will report any damage or faults involving equipment or software as soon as I become aware of them.

I will not try to alter computer settings.

I know that if I break the rules I might not be allowed to use a computer or iPad.

Signed (pupil):

Signed (parent):



Parent / Carer Acceptable Use Agreement

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 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 Form

Parent / Carers Name

Pupil Name

As the parent / carer of the above pupils, I give permission for my son / daughter to have access to the internet and to Computing systems at school.

KS2:
I know that my son / daughter has signed an Acceptable Use Agreement and 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.

KS1:
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 COMPUTING 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 COMPUTING 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.

Signed



Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media,

The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people can not be identified by the use of their names.

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 *students / pupils* in the digital / video images.

Parents / carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents / carers to agree

Digital / Video Images Permission Form

Parent / Carers Name

Student / Pupil Name

As the parent / carer of the above pupil, I agree to the school taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

Yes / No

I agree that if I take digital or video images at, or of, – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Yes / No

Signed

Date



Use of Cloud Systems Permission Form

The school uses Google Apps for Education for **pupils** and staff. This permission form describes the tools and pupil responsibilities for using these services.

The following services are available to each **pupil** and hosted by Google as part of the school's online presence in Google Apps for Education:

Using these tools, **pupils** collaboratively create, edit and share files and websites for school related projects and communicate via email with other pupils and members of staff. These services are entirely online and available 24/7 from any Internet-connected computer. Examples of student use include showcasing class projects, building an electronic portfolio of school learning experiences, and working in small groups on presentations to share with others.

The school believes that use of the tools significantly adds to your child's educational experience.

As part of the Google terms and conditions we are required to seek your permission for your child to have a Google Apps for Education account:

Parent / Carers Name

Student / Pupil Name

As the parent / carer of the above pupil, I agree to my child using the school using Google Apps for Education.

Yes / No

Signed

Date



Staff (and Volunteer) Acceptable Use Policy Agreement School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools 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 internet access at all times.

This Acceptable Use Policy 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 Computing 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 Computing in their everyday work.

The school will try to ensure that staff and volunteers will have good access to Computing 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 Computing systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the Computing systems and other users. I recognise the value of the use of Computing for enhancing learning and will ensure that pupils receive opportunities to gain from the use of Computing. I will, where possible, educate the young people in my care in the safe use of Computing 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 Computing systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school Computing systems (eg laptops, email etc) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school Computing 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.
- 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* Computing 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 (eg 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 chat and social networking sites in school in accordance with the school's policies.
- 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.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (PDAs / laptops / mobile phones) 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 Computing 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 ensure that my data is regularly backed up, in accordance with relevant school policies.
- 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 is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy (or other relevant 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 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 the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school Computing equipment in school, but also applies to my use of school Computing 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 Policy Agreement, I could be subject to disciplinary action. This could include 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 Computing 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.

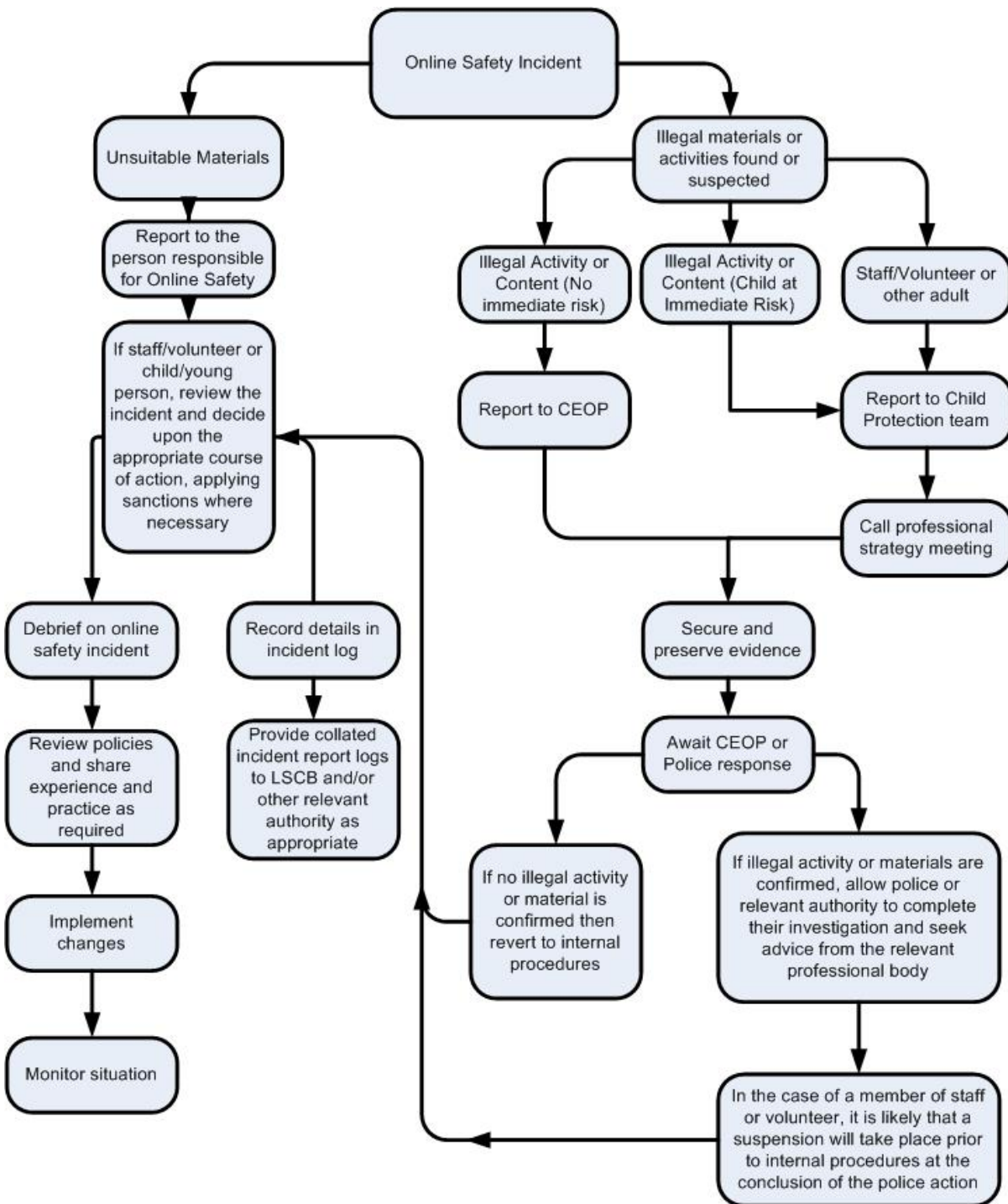
Staff / Volunteer Name

Signed

Date



Responding to incidents of misuse – flow chart





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

Web site(s) address / device	Reason for concern

Conclusion and Action proposed or taken



Appendix 2

School Technical Security Policy (including filtering and passwords)

School's Internet provider- BT. (See Service Level Agreement)

Smoothwall provided by MGL. (See Service Level Agreement)

Technical Security

Policy statements

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people will receive guidance and training and will be effective in carrying out their 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 academy technical systems**
- **Servers, wireless systems and cabling must be securely located and physical access restricted**
- **Appropriate security measures are in place (to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.**
- **Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff.**
- **All users will have clearly defined access rights to school technical systems. Details of the access rights available to groups of users will be recorded by the Network Manager / Technical Staff and will be reviewed, at least annually, by the Online safety Committee.**
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security. *(See Password section below).*
- MGL technician is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- *Mobile device security and management procedures are in place.*
- *School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement. (Appendix 1)*
- *Remote management tools are used by staff to control workstations and view users activity.*
- *An appropriate system is in place for users to report any actual / potential technical incident to the Online safety Coordinator / Network Manager / Technician.*
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school system.
- *An agreed policy is in place regarding the restricted use of removable media (eg memory sticks) by users on school devices.*
- *The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc.*
- *Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.*



Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, and email.

Policy Statements

- All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the Online safety Committee (or other group).
- **All school / academy networks and systems will be protected by secure passwords that are regularly changed**
- **The “master / administrator” passwords for the school systems, used by the technical staff must also be available to the Headteacher or other nominated senior leader and kept in a secure place eg school safe. Consideration should also be given to using two factor authentication for such accounts.**
- The school will never allow one user to have sole administrator access.
- *Passwords for new users, and replacement passwords for existing users will be allocated by MGL. Any changes carried out must be notified to the manager of the password security policy (above).*
- All users (adults and young people) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Users will change their passwords at regular intervals – as described in the staff and pupil sections below.
- Requests for password changes should be authenticated by (MGL) to ensure that the new password can only be passed to the genuine user.

Staff passwords:

- **All staff users will be provided with a username and password by MGL who will keep an up to date record of users and their usernames.**
- *the password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters*
- *must not include proper names or any other personal information about the user that might be known by others*
- *the account should be “locked out” following six successive incorrect log-on attempts*
- *temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on*
- *passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)*
- *passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school*
- *should be changed at least every 60 to 90 days should not re-used for 6 months and be significantly different from previous p the last four passwords cannot be re-used passwords created by the same user.*
- *should be different for different accounts, to ensure that other systems are not put at risk if one is compromised*
- *should be different for systems used inside and outside of school.*



Pupil passwords

- All users at **KS1&KS2** will be provided with a username and password for Purple Mash, Education City, My Maths and Reading Plus by MGL who will keep an up to date record of users and their usernames.
- Users will be required to change their password every year.
- Pupils will be taught the importance of password security.
- The complexity (ie minimum standards) will be set with regards to the cognitive ability of the children.

Training / Awareness

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's online safety policy and password security policy
- through the Acceptable Use Agreement

Pupils will be made aware of the school's password policy:

- in lessons, in Computing Curriculum, online safety awareness days.
- through the Acceptable Use Agreement

Audit / Monitoring / Reporting / Review

The responsible person (MGL) will ensure that full records are kept of:

- User Ids and requests for password changes
- *User log-ons*
- *Security incidents related to this policy*



Appendix 3

Filtering

Introduction

See MGL Online Provider Agreement

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by **MGL**. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

All users have a responsibility to report immediately to the Computing Team any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- *The school has provided enhanced / differentiated user-level filtering through the use of the Smoothwall filtering programme.*

Education / Training / Awareness

Pupils will be made aware of the importance of filtering systems through the online safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- *the Acceptable Use Agreement*
- *induction training*
- *staff meetings, briefings, Inset.*

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through online safety awareness sessions / newsletter etc.



Changes to the Filtering System

The Computing Team should be aware of any requests for changes to the school's filtering system. Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the Computing Team who will decide whether to make school level changes (as above).

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School Online safety Policy and the Acceptable Use Agreement.

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- *Online safety Group*

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.



Appendix 4

School Policy - Online safety Committee Terms of Reference

1. PURPOSE

To provide a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the online safety policy including the impact of initiatives.

2. MEMBERSHIP

2.1 The online safety committee will seek to include representation from all stakeholders.

The composition of the group should include:

- SLT member/s
- Child Protection/Safeguarding officer
- Teaching staff member
- Support staff member
- Online safety coordinator (not Computing coordinator by default)
- Governor
- COMPUTING Technical Support staff (MGL)

2.2 Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the committee to provide advice and assistance where necessary.

2.3 Committee members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.

2.4 Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature

2.5 When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities

3. CHAIRPERSON

The Committee should select a suitable Chairperson from within the group. Their responsibilities include:

- Scheduling meetings and notifying committee members;
- Inviting other people to attend meetings when required by the committee;
- Guiding the meeting according to the agenda and time available;
- Ensuring all discussion items end with a decision, action or definite outcome;
- Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary

4. DURATION OF MEETINGS

Meetings shall be held biannually. A special or extraordinary meeting may be called when and if deemed necessary.

5. FUNCTIONS

These are to assist the Online safety Co-ordinator (or Safe Guarding Officer) with the following:

- To keep up to date with new developments in the area of online safety
- To (at least) annually review and develop the online safety policy in line with new technologies and incidents
- To monitor the delivery and impact of the online safety policy
- To monitor the log of reported online safety incidents (anonymous) to inform future areas of teaching / learning / training.



- To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of online safety. This could be carried out through:
- Staff meetings
- Pupil forums (for advice and feedback)
- Governors meetings
- Surveys/questionnaires for pupils, parents / carers and staff
- Parents evenings
- Website, school app, Newsletters
- Online safety events
- Internet Safety Day (annually held on the second Tuesday in February)
- To ensure that monitoring is carried out of Internet sites used across the school
- To monitor filtering / change control logs (e.g. requests for blocking / unblocking sites).
- To monitor the safe use of data across the school
- To monitor incidents involving cyberbullying for staff and pupils.

6. AMENDMENTS

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all committee members, by agreement of the majority

The above Terms of Reference for Blessed Sacrament Catholic Primary School have been agreed

Signed by (SLT):

Date:

Date for review: Summer 2019