St Gregory's Catholic Primary

Online Safety Policy

This Online Safety policy has been developed by a working group, consisting of the Head and Deputy Head teachers, Computing Co-ordinator, Sandwell Online Safety Officer, Staff and members of the Outcomes Academy committee.

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Outcomes Academy Sub Committee on:	22 November 2017
The implementation of this Online Safety policy will be monitored by the:	Head and Deputy Head teachers, Computing Co-ordinator and committee members.
Monitoring will take place at regular intervals:	Annually
The Outcomes Academy Committee will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	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:	November 2018
Should serious online safety incidents take place, the following external persons / agencies should be informed:	LA Safeguarding Officer, Academy Group Officials, LADO, Police

The school will monitor the impact of the policy by monitoring logs of internet activity and Surveys / questionnaires of pupils and staff.

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors,) who have access to and are users of school ICT 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 (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

St Gregory's Catholic Primary 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 St Gregory's Catholic Primary School.

Academy Committee:

The Academy Committee 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 Outcomes Committee receiving regular information about online safety incidents and monitoring reports. Members of the Academy committee have taken on the role of Online Safety Governors. Mr A Potter and Mrs C Lewis.

<u>The Headteacher and Senior Leaders responsibilities:</u>

Headteacher: Mrs Krystyna Bickley

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Deputy Head Teacher.
- The Headteacher and Deputy Head teacher 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 HR* disciplinary procedures).

- The Headteacher is responsible for ensuring that the staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

  Furthermore the Head teacher:

  - 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 / 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
  - attends relevant meetings/ Academy committees and Board of Directors
  - reports regularly to Senior Leadership Team

ICT Technical staff:

The school technician ensures the following:

- School ICT infrastructure is secure and is not open to misuse or malicious attack
- that the *school* meets required online safety technical requirements.
- that users may only access the networks and devices through a properly enforced password protection policy,
- 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

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
- they report any suspected misuse or problem to the Headteacher for investigation.

- all digital communications with pupils, parents and/or carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and acceptable use policies
- staff monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities
- 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
- the production / review / monitoring of the school Online Safety Policy / documents.
- the production / review / monitoring of the school filtering policy (if the school chooses to have one) 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 students / pupils about the online safety provision

Designated Safeguarding Lead

The DSL'S are 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

It is important to emphasise that these are safeguarding issues, not technical issues, simply that the technology provides additional means for safeguarding issues to develop.

Pupils:

- are responsible for using the school digital technology systems.
- 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' workshops, newsletters, letters, website 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

Education – Pupils

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 lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of learning.
- 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 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.
- 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.

Education – Parents / Carers

Parents and carers play an essential role in the education of their children in recognising online safety risks and in monitoring and regulating their 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, newsletters, web site,
- Parents workshops
- Safer Internet Day
- Reference to the relevant web sites / publications e.g. www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers (see appendix for further links / resources)

Education & Training – Staff / Volunteers

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

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school / academy Online Safety Policy and Acceptable Use Agreements.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings.
- Training – Academy Committee. Members should take part in online safety training / awareness sessions, with particular importance for those who are members of any

subcommittee / group involved in technology / online safety / health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by Sandwell SIPs or other relevant organisation
- 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 and network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All staff users are responsible for the security of their username and password *and will be required to change their password regularly.*
- The "master / administrator" passwords for the school ICT system, used by the administrator must also be available to the *Headteacher* and kept in a secure place (eg school safe)
- The ICT 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
- 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. the school adopts the Sandwell LA filtering service see appendix. There is a clear process in place to deal with requests for filtering changes (see appendix for more details)
- **Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.** NB. additional duties for schools / academies under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet. (see appendix for information on "appropriate filtering").
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incidents / security breach to the relevant staff.

- 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 (Acceptable Use Policy) is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors onto the school systems.
- An agreed policy (Acceptable Use Policy) is in place that forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy (Acceptable Use Policy) is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. **Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured**.

Mobile Technologies (including BYOD/BYOT)

BYOD (Bring your own device) /BYOT(Bring your own technology)

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 polices 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 and parents/carers will consider the use of mobile technologies

- The school allows:

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

Aspects that the school may wish to consider and be included in their Online Safety Policy, Mobile Technologies Policy or Acceptable Use Agreements:

- All staff use the school mobile phone when off site (local visits to the swimming baths, church and off site visits.
- Staff are permitted to bring their mobile phones to school but are not allowed to use them in public places or where children are present. They can be used for emergency purposes only in offices/small rooms (where no children are present) in school. Personal staff phones are not permitted for taking photographs in school of children. All staff are allocated mini I pads to support the teaching and learning in school. All images should be stored appropriately on school devices.
- Staff are not permitted to use their phones to access the internet

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning. 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 in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published or 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' full names will not be used anywhere on a website or blog, particularly in association with photographs.

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 / academy 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". (see Privacy Notice section in the appendix)
- It has a Data Protection Policy (see appendix for template policy)
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- 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 transfer / 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.

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

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning.

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.
- 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 through e-mail between staff and parents / carers must be professional in tone and content. These communications may only take place on official school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils IN KS2 have a school e-mail address for educational use and will only use it in school supervised by staff.
- Pupils are taught about online safety issues, such as the risks attached to the sharing of personal details. They are educated in using strategies to deal with inappropriate communications and are reminded of the need to communicate appropriately when using digital technologies.

Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes, clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when publishing any material online.

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

social media as a powerful learning tool and means of communication. It is important that this is carried out in a safe and responsible way.

A checklist of points to be considered is included below.

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies 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 and academy group 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

<u>School staff should ensure that:</u>

- 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

<u>When official school social media accounts are established there should be:</u>

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school / academy disciplinary procedures

Personal Use:

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

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 also be banned and could lead to criminal prosecution.

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

- Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978
- Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.
- Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008
- 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
- Pornography

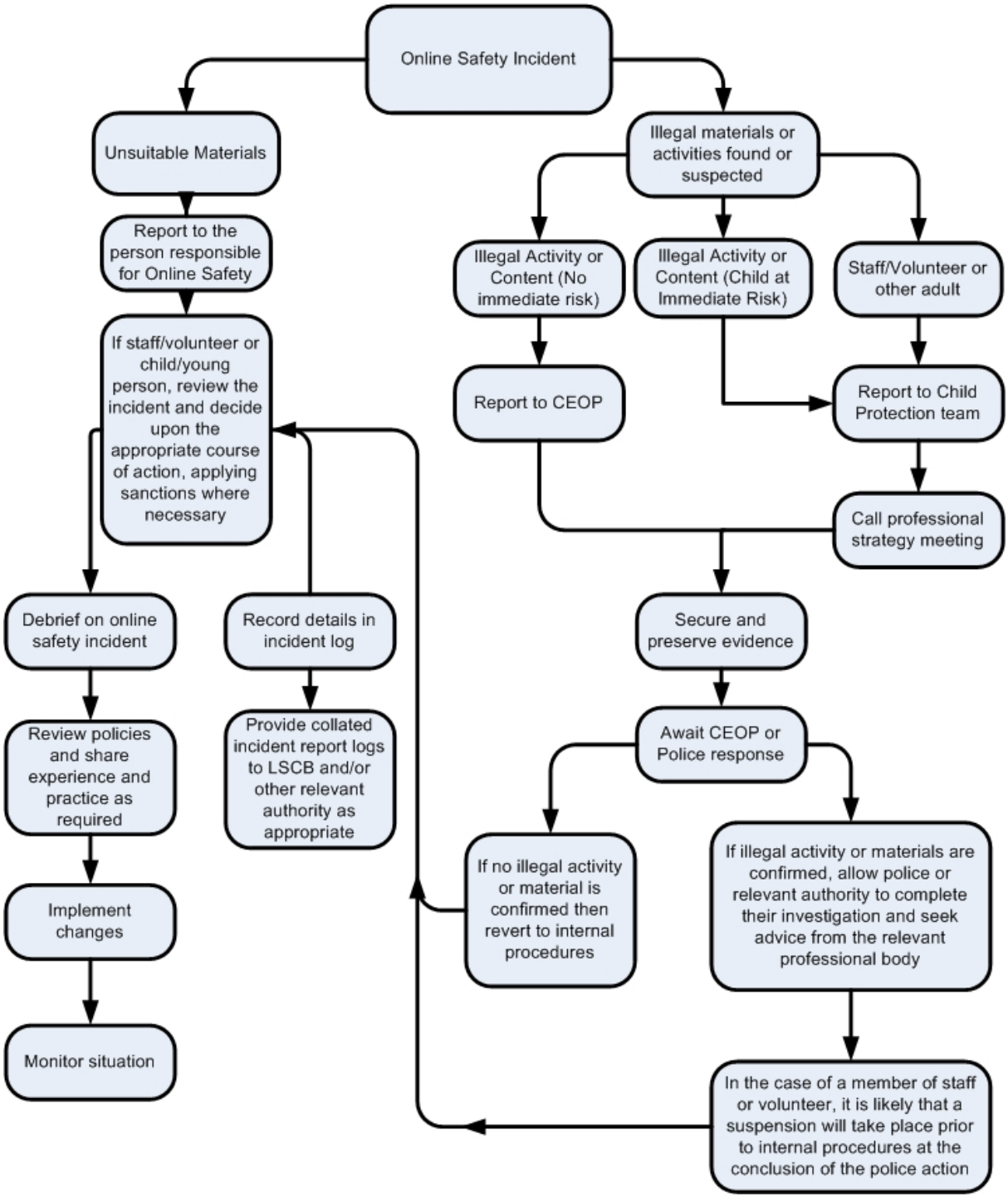
- Promotion of any kind of discrimination
- threatening behaviour, including promotion of physical violence or mental harm
- Promotion of extremism or terrorism
- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute
- Using school systems to run a private business
- Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy
- Infringing copyright
- Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Unfair usage (downloading / uploading large files that hinders others in their use of the internet)
- On-line gaming (educational)
- On-line gaming (non-educational)
- On-line gambling
- On-line shopping / commerce
- File sharing
- Use of messaging apps
- Use of social media
- Use of video broadcasting e.g. Youtube

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

All members of the school community should 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 of the Board of Directors 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 / academy* 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 will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Actions / Sanctions

Students / Pupils Incidents	Refer to class teacher	Refer to SLT	Refer to Head teacher	Refer to Police	Inform parents / carers	Removal of network / internet access rights
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X	X	X	X

Unauthorised use of non-educational sites during lessons	X	X	X		X	
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	X	X	X		X	X
Unauthorised / inappropriate use of social media / messaging apps / personal email	X	X	X	X		
Unauthorised downloading or uploading of files	X	X	X		X	X
Allowing others to access school network by sharing username and passwords	X	X	X		X	X
Attempting to access or accessing the school network, using another student's / pupil's account	X	X	X		X	X
Attempting to access or accessing the school network, using the account of a member of staff	X	X	X		X	X
Corrupting or destroying the data of other users	X	X	X		X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X		X	X
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X	X	X	X
Using proxy sites or other means to subvert the school's filtering system	X	X	X		X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X		X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X

Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X		X	X	

Actions / Sanctions

Staff Incidents	Refer to Board of Directors	Refer to Headteacher	Refer to Local Authority	Refer to Police	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	X	X	X	X
Inappropriate personal use of the internet / social media / personal email	X	X	X		X		X
Unauthorised downloading or uploading of files	X	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		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		X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X	X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X	X	X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils	X	X	X	X	X	X	X

Actions which could compromise the staff member's professional standing	X	X	X		X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X		X	X	X
Using proxy sites or other means to subvert the school's filtering system	X	X	X		X		X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X		X		
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X
Breaching copyright or licensing regulations	X	X	X		X		
Continued infringements of the above, following previous warnings or sanctions	X	X	X		X	X	X

Signed 

K Bickley Head Teacher

Signed *M O'Brien*

M O'Brien Chair of Governors