Oratory R.C. Primary and Nursery School

'Shine as to be a light to others'

Online Safety Policy

Last Review Date of this Policy:	Date of this Policy:	Reviewed by:	Date to be ratified by FGB	Date for next review:	Date to be next ratified by FGB:	Review Frequency
	March 2022	• Strategic Leadership Team Sept 18 • School Staff Sept 2018		September 2022	September 2022	Annually
How will Governors assure the Oratory community that this policy is being implemented:		Governors to monitor and evaluate implementation through: • Nominated Governor Safeguarding visits to the school • Nominated Safeguarding Governor reports to the FGB • Safeguarding Team minutes • Safeguarding Team Termly Report to Safeguarding, Health and Safety and Premises Committee • HT's Report to Governors				

N.B. This Online Safety policy has been written using a template provided by the South West Grid

SWGfL Education that Clicks

UK Safer Internet Centre

360 degree safe

Mission Statement

‘Shine as to be a light to others’

Blessed John Henry Newman

Our School’s Mission

At the Oratory R.C. Primary and Nursery School every aspect of school life is founded on Gospel Values. Our choice of Mission Statement, “Shine as to be a light to others”, is inspired by the writing and teaching of the Blessed John Henry Newman, an advocate of personalised learning, and of Saint Philip Neri, who believed that “cheerfulness strengthens the heart and makes us persevere in a good life; therefore the servant of God ought always to be in good spirits.”

We are committed to providing a safe, nurturing and happy immersive learning environment, based upon the living tradition of the Church, drawing continually upon current educational research.

Our School prepares children to meet the opportunities and challenges of life in contemporary Britain and within a fast changing technological and globalised world through an innovative curriculum that is tailored to meet the needs of all.

A community of lifelong learners, our School and Governing Body work in close partnership with: our families, the Fathers and Brothers of the Oratory, our local parish, the local and wider community, and external consultants. We work together to enable all to fulfill their spiritual, academic, emotional and social potential. We are a team, and together we make a difference.

Our School’s Vision

Christ is at the centre of all we do.

Our School is a learning community for all: pupils, staff, governors, parents and carers, outside agencies, and the local and wider community.

Ours is a strong culture of unconditional support for one another’s learning, where all listen respectfully and welcome constructive criticism and challenge.

We offer a vibrant and exciting curriculum and learning experience, ensuring that all pupils, from whatever point they start on entering our School, make at least good progress.

We aim to help our children discover and develop their God-given talents and to encourage them to grow in responsibility for themselves and for others.

We believe that everyone has a right to equal access and opportunity, and equal freedom to work and learn, and freedom from unjust discrimination and from prejudice.

Our practices promote the right of all to participate in school life by actively promoting equality and social inclusion without distinction of culture, religion, language, ethnic background or race.

Our School's context and culture

Our School mission is based on the belief that every human being is a unique person created in the image and likeness of God, with a God-given potential for growth and an eternal destiny in heaven. Our staff have a special vocation to make sure that all our children receive the very best educational experience in order to grow in the love and knowledge of God, their neighbour, themselves and the created world.[1] We see this as integral to our Catholic ethos.

As a school we work together to embed and sustain this ethos. The word "ethos" can be defined as: "a way of living, behaving and doing things by people who, though diverse, follow common values and are linked by a shared vision of life."[5] Our School's Catholic ethos promotes and helps to shape a strong set of values.

Development of this Policy

This Online Safety policy has been developed by a working group made up of:

- Head Teacher
- Strategic Leadership Team
- Safeguarding Team
- Online Co-ordinator
- Link 2ICT consultant
- Safeguarding, Premises and Health and Safety Committee

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Board of Governing Body on:	March 2022
The implementation of this Online Safety policy will be monitored by the:	Online Safety Lead Phase Leaders Computing Lead Safeguarding Governor
Monitoring will take place at regular intervals	
The Safeguarding, Premises and Health and Safety 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:	Termly
The Online Safety Policy will be reviewed annually however minor changes will be made as and when required or in the light of new legislation or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	September 2022
Should serious online safety incidents take place, the following external persons / agencies should be informed:	Head Teacher Chair of Governors LA Safeguarding Officer, LADO, Police

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity
- Surveys / questionnaires of students / pupils, parents / carers and staff

Scope of the Policy

This policy applies to all members of the Oratory community (including staff, pupils, volunteers, parents / carers and 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 Head Teachers 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 Expectations Policy.

This policy is also based on the Department for Education's (DfE) statutory safeguarding guidance, **Keeping Children Safe in Education (September 2022)**, and its advice for schools related to online safety.

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.

The 4 Key Categories of Risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism

- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

Roles and Responsibilities

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

Full Governing Body

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 Safeguarding, Premises and Health and Safety Committee receiving regular information about online safety incidents and monitoring reports. The Safeguarding governor has taken on the role of Online Safety. The role will include:

- regular meetings with the Head Teacher and Computing Lead
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to the Full Governing Body should any severe incidents occur

Head Teacher and Senior Leaders

- The Head Teacher 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 Securas Monitoring Service.
- The Head Teacher and Safeguarding Team are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Head Teacher is responsible for ensuring that the Computing Lead, Safeguarding Team 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 Head Teacher and Safeguarding Team will receive regular monitoring reports from Securas Central Monitoring Service.

The Online Safety Lead (Head Teacher in unison with Safeguarding Team)

- leads Online Safety awareness and management through the Safeguarding Team
- is responsible for ensuring 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 investigated / actioned / sanctioned.
- 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, meets regularly with the Safeguarding Governor and Chair of Safeguarding, Premises and Health and Safety Committee

- to discuss current issues, review incident logs and filtering / change control logs
- reports regularly to the Strategic Leadership Team and Safeguarding, Premises and Health and Safety Committee

Securus Monitoring Service in collaboration with the Online Safety and Computing Leads are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority 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 provided by CSE is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the monitoring software (Securas) is implemented and updated as agreed in school / academy 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 / Agreement (AUP)
- they report any suspected misuse or problem to the Head Teacher or Deputy Head Teacher for investigation / action / sanction
- **all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems**
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, 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 **will 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

For searching the Internet, in accordance with the Computing Curriculum, we do allow safe searching with a suitable set of key words. Children are expected to use Safe Search Kids http://www.safesearchkids.com/ (which is powered by Google with safe search enabled

Designated Safeguarding Lead and Safeguarding Team

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

Online Safety is a key remit of the School Safeguarding Team

The Safeguarding Team provides opportunities for pupils, parents and carers to discuss and consider ways to keep our school community safe online. The team has responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives.

Members of the team will assist the Online Safety Lead and Computing Lead with:

- the production / review / monitoring of the school Online Safety Policy / documents.
- 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
- monitoring improvement actions identified through use of the 360 degree safe self-review tool

Pupils:

- are responsible for using the school's digital technology systems in accordance with the Pupil Acceptable Use Agreement
- have a good understanding of research skills and the need to uphold copyright regulations
- will be expected 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 and Carers

Parents and 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 Learning Together Day, newsletters, letters, website / Learning Platform and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school / academy in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- their children's personal devices in the school (where this is allowed)

Community Users

Community Users who access the school website / Learning Platform as part of the wider school provision will be expected to sign a Community 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 alongside the school's scheme 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 tutorial / 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 supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- ***Staff MUST 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 MUST 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 (eg racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. **Any request to do so, should be auditable, with clear reasons for the need.**

Education – Parents and Carers

Parents and carers may 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 and carers 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, Learning Platform
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers (See appendix for further links / resources)

Education and Training – Staff and 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. It is expected that some staff will identify online safety as a training need within the performance management process.

- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school's Online Safety Policy and Acceptable Use Agreements.
- The Online Safety Lead and Safeguarding Team members will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff / phase meetings / INSET days.
- The Online Safety Lead 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 the Safeguarding, Premises and Health and Safety Committee. This may be offered in a number of ways:

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

Technical – infrastructure / equipment, filtering and monitoring

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

- **School technical systems will be managed in ways that ensure that the school meets recommended technical requirements**
- **There will be regular reviews and audits of the safety and security of school / technical systems**
- **Servers, wireless systems and cabling must be securely located and physical access restricted**
- **All users will have clearly defined access rights to school technical systems and devices.**
- **All users at will be provided with a username and password by** the Computing Lead *who will keep an up to date record of users and their usernames.* **Users are responsible for the security of their username and password** *and will be required to change their password every academic year.*
- The "administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Head Teacher and kept in a secure place (eg school safe)

- The Senior Office Manager together with the Computing Lead 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 **I**
- **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 by CSE daily monitoring service. There is a clear process in place to deal with requests for filtering changes through CSE.
- **Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.**
- Appropriate security measures are in place by CSE 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.
- A daily username is provided for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems. This profile is restricted.

Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

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 cyber bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- **When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.**
- **Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website / social media / local press**.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school / academy 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 / made publicly available on social networking sites,

nor should parents / carers comment on any activities involving other *students / 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 / academy into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the / 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.

Unlicensed or personal software must not be installed on the school's hardware or connected in any way to the school's equipment or systems. If software is deemed to be of use to the school then it should be duly acquired by the school under licence.

Where data of a personal nature such as: school reports, IEPs, correspondence and assessment data is taken home on a school laptop or other portable storage media, it must be recognised that this data comes under the Data Protection Act and is subject to the school's Safeguarding and Child Protection Policy. Care must therefore be taken to ensure its integrity and security. It should be removed from any portable device including USB pens and memory cards as soon as possible.

Where authorisation has been given to a specific user to use a potable storage medium (e.g. memory stick) it is his/her responsibility to ensure that it does not transmit any viruses onto the school's network. It is recommended that pupils refrain from using such media unattended.

Staff are encouraged to use the drives on the school network as a central repository for documents such as policy and planning files. Confidential pupil data may be safely stored here as access is only permissible through login by a member of school staff.

All pupil work is stored in their own personal folder on the network. Children's files cannot be moved or deleted whilst logged onto a machine as a pupil user.

The servers containing these networked drives are locked away each night as an extra security measure to prevent against theft.

Data Backups

Data stored on the school's networked drives are backed up regularly so that copies of files may be recovered if the original becomes either lost or damaged.

Communications

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

	Staff and other adults				**Pupils**			
	Not allowed	Allowed	Allowed at certain places/times	Allowed for selected staff	Not allowed	Allowed (Year 6)	Allowed at certain times	With staff supervision
Mobile phones may be brought to school			X Staffroom only			X Put into safety deposit box each am		
Use of mobile phones in social time (break and lunchtimes in Staff / room)			X		X			

Use of mobile phones in lesson time	X				X			
Taking photos on mobile phones/cameras		X Camera not mobile phone			X			
Use of other mobile devices e.g. tablets, gaming devices			X				X	X
Use of personal email addresses in school or on the school network	X				X			
Use of school email for personal emails	X				X			
Use of messaging apps	X				X			
Use of social media e.g. Twitter			X				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.
- Users must immediately report, to the nominated person – in accordance with the school / academy 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, social media, chat, blogs, VLE etc) 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.
- All 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 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* liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

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

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or school
- 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

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	
	Promotion of extremism or terrorism					X
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)			X			
On-line gaming (non-educational)					X	
On-line gambling					X	

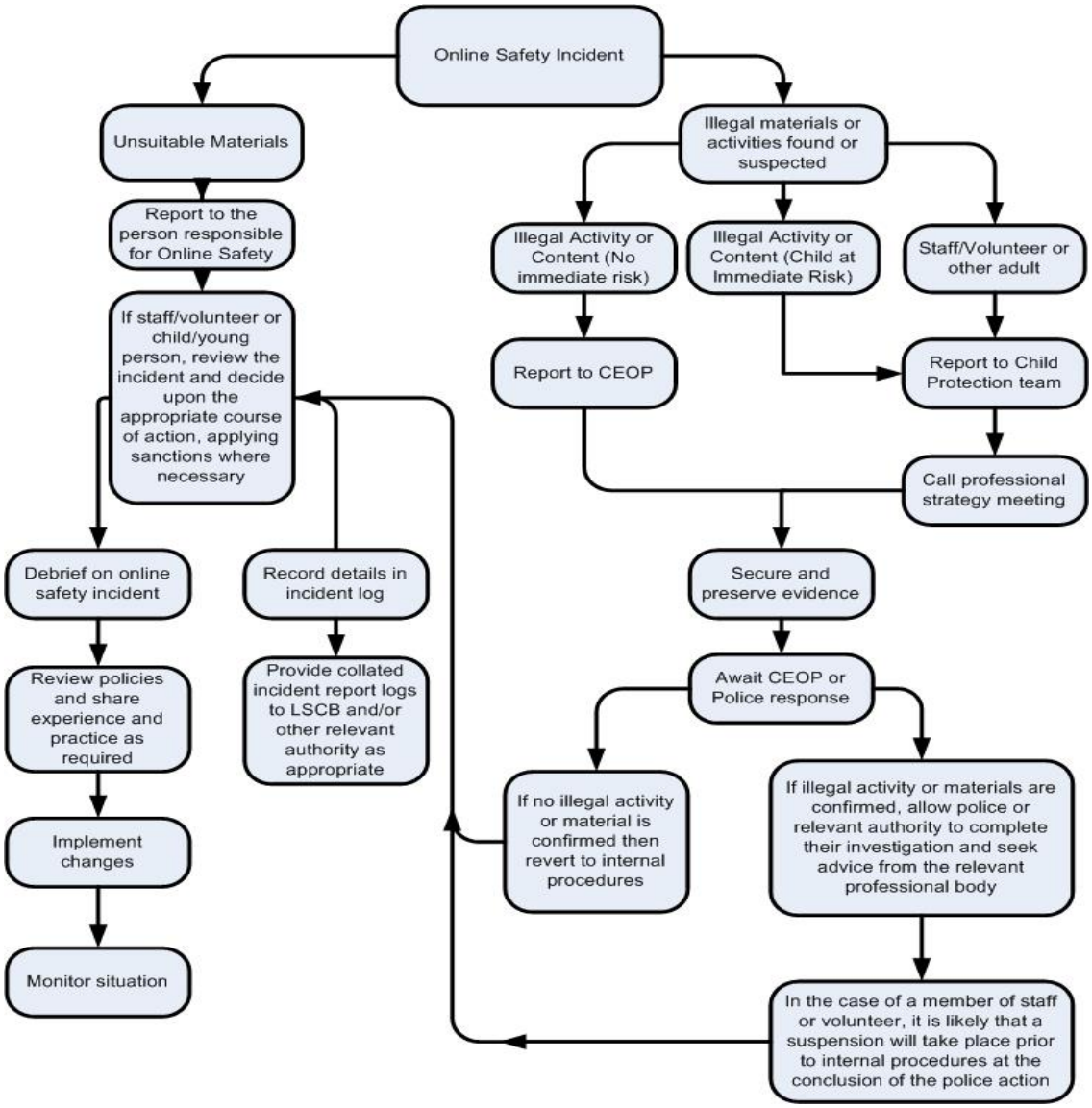
On-line shopping / commerce (Best Value)		X			
File sharing			X		
Use of social media (Twitter/Blog)		X			
Use of messaging apps (Twitter)		X			
Use of video broadcasting e.g. Youtube		X			

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


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff 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
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials

- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the *school* and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions and Sanctions

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

Pupil Incidents	Actions / Sanctions								
	Refer to class teacher / tutor	Refer to Head of Department / Year / other	Refer to Head Teacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons	X	X				X			
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	X	X	X	X		X		X	
Unauthorised / inappropriate use of social media / messaging apps / personal email	X	X	X			X	X	X	X
Unauthorised downloading or uploading of files		X	X						
Allowing others to access school / academy network by sharing username and passwords	X							X	
Attempting to access or accessing the school / academy network, using another student's / pupil's account			X		X	X	X		X

Attempting to access or accessing the school / academy 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	X	X
Continued infringements of the above, following previous warnings or sanctions						X			X
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school			X		X				
Using proxy sites or other means to subvert the school's / academy's filtering system	X	X	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
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			X						

	Actions / Sanctions							
Staff Incidents	Refer to line manager	Refer to Head Teacher	Refer to Local Authority /	Refer to Police	Refer to Technical Support Staff for action re filtering	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
Inappropriate personal use of the internet / social media including Facebook / personal email		X	X	X		X	X	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 e.g. holding or transferring data in an insecure manner	X					X		
Deliberate actions to breach data protection or network security rules		X					X	X
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, past pupils, parents,		X	X	X			X	X

carers and ex staff who have links with parents or carers.								
Actions which could compromise the staff member's professional standing		X	X				X	X
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy		X	X				X	X
Using proxy sites or other means to subvert the school's / academy's filtering system			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
Breaching copyright or licensing regulations	X						X	
Continued infringements of the above, following previous warnings or sanctions			X				X	X

Appendix 1: General Data Protection Regulation (GDPR) compliant consent

Images and Videos Parental and Carer Consent Form

Please read this document in the line with the Oratory GDPR Privacy Notice for our children and families.

This form explains the reasons why and how the Oratory R.C. Primary and Nursery School may use images and videos of your child. **Please read the form thoroughly and outline your agreement as appropriate.**

Consent is not needed for group images or videos. This applies to groups of 6 or more. Consent is needed for **small groups or individuals (SG/I)** for images and videos. This applies to groups of less than 6.

Where the school uses images of SG/I pupils, only the first name and/or the class of the pupil might be disclosed.

The Oratory R.C. Primary and Nursery School requests the consent of parents and carers to use SG/I images and videos of their child for a variety of different purposes.

Without your consent, the school will not use SG/I images and videos of your child. Similarly, if there are only certain conditions under which you would like SG/I images and videos of your child to be used, the school will abide by the conditions you outline in this form.

Why do we use images and videos of your child?

The Oratory R.C. Primary and Nursery School uses images and videos of individual pupils and as groups of pupils as part of school displays to celebrate school life and pupils' achievements; to promote the school on social media and on the School website; and for other publicity purposes in printed publications, such as newsletters and the prospectus.

In the case where an individual pupil is named in an external publication, a photograph of the pupil may be used to accompany the text. (If, for example, a pupil has won an award and their parent would like their name to be published alongside their image). On these occasions **separate consent** will be obtained prior to this.

Who else uses images and videos of your child?

Occasionally school may be visited by local media or outside providers, who take images or videos of school events, such as our charity event. Pupils will appear in these images and videos, and these may be published in local newspapers, on approved websites or social media.

Where any organisations other than school intend to use images or videos of your child, **additional consent** will be sought before any image or video is used.

What are the conditions of use?

- This consent form is valid for the remainder of your child's time in the Oratory R.C. Primary and Nursery School however reminders about your right to withdrawal will be sent annually.

- It is the responsibility of parents and carers to inform the school, in writing, if consent needs to be withdrawn or amended.
- The school will not use the personal details or full names of any pupil in an image or video, on our website, in our school prospectuses or any other printed publications (unless separate consent has been obtained)
- The school will not include personal emails or postal addresses, telephone numbers on images or videos on our website, in our school prospectuses or any other printed publications.
- The school may use pictures of pupils and teachers that have been drawn by pupils.
- The school may use work created by pupils.
- The school will use group or class images or videos with general labels, e.g. 'sports day'.
- The school will only use images and videos of pupils who are suitably dressed, i.e. it would not be suitable to display an image of a pupil in swimwear.
- The school will take class images of your child which are available to purchase annually.

Duration of consent

This form is valid for the duration of your child's time at our school. Parents and carers will be reminded through the school newsletter about their right for withdrawal.

Consent will be refreshed where any changes to circumstances occur – this can include, but is not limited to, the following:

- New requirements for consent, e.g. an additional social media account will be used to share pupil images and videos
- Changes to a pupil's circumstances, e.g. safeguarding requirements mean a pupil's image cannot be used
- Changes to parental consent, e.g. amending the provisions for which consent has been provided for

Where you would like to amend the provisions for which consent has been provided, you must submit your request in writing to the Head teacher. A new form will be supplied to you to amend your consent accordingly and provide a signature.

Withdrawing your consent

Parents and carers have the right to withdraw their consent at any time. Withdrawing your consent will not affect any images or videos that have been shared prior to withdrawal.

If you would like to withdraw your consent, you must submit your request in writing to the Head Teacher.

Providing your consent for small group and individual (SG/I) images and videos

Please read the following conditions thoroughly and provide your consent as appropriate by ticking either 'Yes' or 'No' for each criteria.

The school will only publish SG/I images and videos of your child for the conditions that you provide consent for.

I provide consent to:	Yes	No
Using **SG/I images** of my child (which may include first name and/or class) on the **school website/ blogs**		
Using **SG/I images** of my child (which may include first name and/or class) on the **school newsletter**		
Using **SG/I videos** of my child or videos made by my child (which may include first name and/or class) on the **school website/ blogs**		
Using **SG/I images** of my child (which may include first name and/or class) for **school displays**		
Using **SG/I images** of my child (which may include first name and/or class) on **school documentation** e.g. reports to Governors		
Using **SG/I images** of my child (which may include first name and/or class) on **Twitter**		
Using **SG/I videos** of my child (which may include first name and/or class) on **Twitter**		
Using **SG/I images** of my child (which may include first name and/or class) in marketing material e.g the school prospectus and activities/events publicised on **our website**		
Sharing my **child's data** with a school-appointed external photography company for official school images. This includes the name, class, roll number		

Name of nominated parent / carer in CAPITALS: (Priority 1 on school contact form)	
Email of Nominated parent / carer:	
Name of Child in CAPITALS:	
Class:	
Signature:	
Date:	

N.B. Please note if parents have separated they must discuss this consent form with each other and decide who will be the nominated parent.

Parent / Carer Consent Declaration

I, _____ (name of parent/carer) have read and understand:

- Why my consent is required.
- The reasons why The Oratory R.C. Primary and Nursery School uses images and videos of my child.
- Which other organisations may use images and videos of my child with my additional separate consent.
- The conditions under which the school uses images and videos of my child.

- I have provided my consent above as appropriate, and the school will use images and videos of my child in line with my requirements.
- I will be required to update consent where any circumstances change.
- I can amend or withdraw my consent at any time and must do so in writing to the Head. The above email I have given is the email address the school will use to communicate with me in regards to my child/ren.

Appendix 2

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 / student responsibilities for using these services.

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

Mail - an individual email account for school use managed by the school

Calendar - an individual calendar providing the ability to organize schedules, daily activities, and assignments

Docs - a word processing, spreadsheet, drawing, and presentation toolset that is very similar to Microsoft Office

Sites - an individual and collaborative website creation tool

Using these tools, *pupils* collaboratively create, edit and share files and websites for school related projects and communicate via email with other pupils / students 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 student / pupil, I agree to my child using the school using Google Apps for Education. Yes / No

Signed: .....

Date: ----------

Appendix 3

Oratory R.C. Primary and Nursery School

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

This Acceptable Use 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 / academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

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

Acceptable Use Policy Agreement

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

For my professional and personal safety:

- I understand that the *school will* monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school. I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using *school* ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies. (
- I will only communicate with pupils and parents and carers using official school systems. Any such communication will be professional in tone and manner.
- **I will not engage in any on-line activity i.e. on Facebook 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 / academy*:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using *school* equipment. I will also follow any additional rules set by the *school* about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems. I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school / academy 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 / academy 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 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 / digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- **I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action.** This could include a warning (written or verbal), a suspension, referral to Governors or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

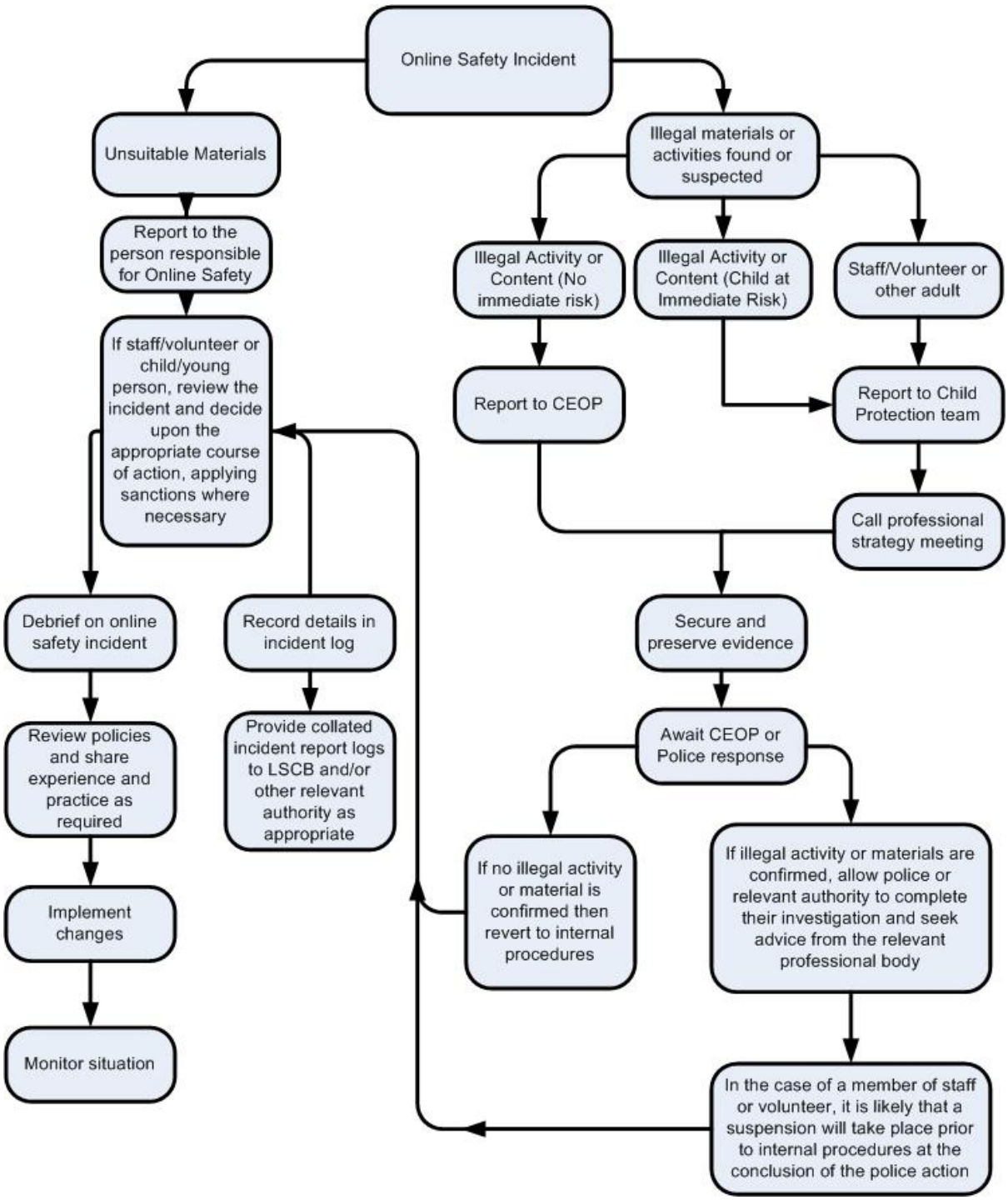
Staff / Volunteer Name: .....

Signed: .....

Date: .....

Appendix 4

Responding to incidents of misuse – flow chart



Appendix 5

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

Group: .....

Date: .....

Reason for investigation: .....

.....

.....

.....

Details of first reviewing person

Name: .....

Position: .....

Signature: .....

Details of second reviewing person

Name: .....

Position: .....

Signature: .....

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

.....

.....

Web site(s) address / device	Reason for concern

Conclusion and Action proposed or taken

Reporting Log

Group: .....

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

Training Needs Audit Log

Group: .....

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

Legislation

Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety

is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harrassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social

workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. (see template policy in these appendices and for DfE guidance - http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation)

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent / carer to use Biometric systems

The School Information Regulations 2012

Requires schools to publish certain information on its website:

https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

Links to other organisations or documents

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

UK Safer Internet Centre

Safer Internet Centre – http://saferinternet.org.uk/
South West Grid for Learning - http://swgfl.org.uk/
Childnet – http://www.childnet-int.org/
Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
Internet Watch Foundation - https://www.iwf.org.uk/

CEOP

CEOP - http://ceop.police.uk/
ThinkUKnow - https://www.thinkuknow.co.uk/

Others

INSAFE - http://www.saferinternet.org/ww/en/pub/insafe/index.htm
UK Council for Child Internet Safety (UKCCIS) - www.education.gov.uk/ukccis
Netsmartz - http://www.netsmartz.org/

Tools for Schools

Online Safety BOOST – https://boost.swgfl.org.uk/
360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/

Bullying / Cyberbullying

Enable – European Anti Bullying programme and resources (UK coordination / participation through SWGfL & Diana Awards) - http://enable.eun.org/
Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
Scottish Government - Better relationships, better learning, better behaviour - http://www.scotland.gov.uk/Publications/2013/03/7388
DfE - Cyberbullying guidance - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf
Childnet – new Cyberbullying guidance and toolkit (Launch spring / summer 2016) - http://www.childnet.com/new-for-schools/cyberbullying-events/childnets-upcoming-cyberbullying-work
Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm

Social Networking

Digizen – Social Networking
UKSIC - Safety Features on Social Networks
SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people
Connectsafely Parents Guide to Facebook

Facebook Guide for Educators

Curriculum

SWGfL Digital Literacy & Citizenship curriculum
Glow - http://www.educationscotland.gov.uk/usingglowandict/
Teach Today – www.teachtoday.eu/
Insafe - Education Resources

Mobile Devices / BYOD

Cloudlearn Report Effective practice for schools moving to end locking and blocking
NEN - Guidance Note - BYOD

Data Protection

Information Commissioners Office:

Your rights to your information – Resources for Schools - ICO
Guide to Data Protection Act - Information Commissioners Office
Guide to the Freedom of Information Act - Information Commissioners Office
ICO guidance on the Freedom of Information Model Publication Scheme
ICO Freedom of Information Model Publication Scheme Template for schools (England)
ICO - Guidance we gave to schools - September 2012 (England)
ICO Guidance on Bring Your Own Device
ICO Guidance on Cloud Hosted Services
Information Commissioners Office good practice note on taking photos in schools
ICO Guidance Data Protection Practical Guide to IT Security
ICO – Think Privacy Toolkit
ICO – Personal Information Online – Code of Practice
ICO Subject Access Code of Practice
ICO – Guidance on Data Security Breach Management
SWGfL - Guidance for Schools on Cloud Hosted Services
LGfL - Data Handling Compliance Check List
Somerset - Flowchart on Storage of Personal Data
NEN - Guidance Note - Protecting School Data

Professional Standards / Staff Training

DfE - Safer Working Practice for Adults who Work with Children and Young People
Childnet / TDA - Social Networking - a guide for trainee teachers & NQTs
Childnet / TDA - Teachers and Technology - a checklist for trainee teachers & NQTs
UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure / Technical Support

Somerset - Questions for Technical Support
NEN - Guidance Note - esecurity

Working with parents and carers

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

Research

EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011
Futurelab - "Digital participation - its not chalk and talk any more!"
Ofcom – Children & Parents – media use and attitudes report - 2015

Glossary of Terms

AUP / AUA	Acceptable Use Policy / Agreement – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
FOSI	Family Online Safety Institute
ES	Education Scotland
HWB	Health and Wellbeing
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by NAACE
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)

SWGfL South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW

TUK Think U Know – educational online safety programmes for schools, young people and parents.

VLE Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,

WAP Wireless Application Protocol

UKSIC UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.

Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in April 2016.