


Mission
Together we love, learn, follow Jesus
Vision
At St Joseph’s Catholic Primary School, through an open and generous heart, we learn together as a family in faith, following the gospel values of love.
Values
Hope Thankfulness Collaboration Compassion Friendship Resilience Empathy Creativity Justice Respect

Development / Monitoring / Review of this Policy

This Online Safety policy has been developed and shared with other staff and governors via the:

- Headteacher
- Online Safety Subject Leader
- Computing Governor

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Governing Body on:	
The implementation of this Online Safety policy will be monitored by the:	Headteacher – Miss Dewhurst Online Safety Lead – Miss Bottomley
Monitoring will take place at regular intervals:	Annually or as required
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:	September 2024
Should serious online safety incidents take place, the following external persons / agencies should be informed:	Parents Governors Police via PCSOs LADO if appropriate

Scope of the Policy

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

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

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

This policy will be regulated through:

- Logs of reported incidents using CPOMS
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity
- discussions / questionnaires of
 - pupils
 - parents / carers
 - staff

Roles and Responsibilities

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

Headteacher/DSL (Miss Dewhurst)– Monitoring, recording, reviewing and presenting all aspects in relation to this policy.

Assistant Headteacher/DSL (Miss Bottomley)– Monitoring and reporting online safety concerns or breaches of the policy.

Computing Subject Leader (Miss Bottomley)– Monitoring, recording, reviewing and presenting all aspects in relation to this policy.

School ICT Technician – Monitoring and updating the school’s network systems to ensure they comply with local and national standards.

Computing Governor: Darren Cranshaw and Chair of Governors: Kate Armstrong – liaising with the online safety lead, DSLs and updating governors.

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- regular contact with the Online Safety Lead who will report on incidents of online safety that have had to be recorded, monitoring of filtering / change control logs
- reporting to relevant Governors

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Lead.
- The Headteacher and the Senior Leadership Team are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – “Responding to incidents of misuse” and relevant *Local Authority/ other relevant body* disciplinary procedures).
- The Headteacher/ Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive weekly monitoring reports from the ICT Technician and these will be reported to Governors in the termly headteacher report.

Online Safety Lead

- 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/ governors
- liaises with the Local Authority / MAT / relevant body where appropriate
- liaises with school ICT support staff
- Monitors online safety incidents through use of CPOMS and informs staff (when needed) of future online safety developments.
- Updates Senior Management Team **immediately for any urgent breaches of policy or termly through the headteacher** report to governors for routine updates, review of any incident logs and filtering.
- attends relevant meeting / committee of Governors
- Completes the filtering and monitoring audit on a regular basis with the support of the school's ICT technician.

Network Manager / Technical staff

The Computing Subject Leader and Senior Leadership team are responsible for ensuring the following checks are made each term.

The school's technical infrastructure is secure and is not open to misuse or malicious attack.
The school meets required online safety technical requirements and any Local Authority / MAT / other relevant body Online Safety Policy / Guidance that may apply.
Users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed (annually).
The filtering policy is applied and updated on a regular basis through use of Surf Protect.
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.
The use of the network / internet / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Online Safety Lead, and if necessary a member of the Senior Leadership Team for investigation / action / sanction that monitoring software / systems are implemented and updated as agreed in school policies.

This will be monitored termly by both the Computing Lead, SLT and IT Technician to ensure all appropriate procedures are in place and up to date. Each item will be displayed as a checklist and it will be signed off and monitored through use of the table shown above.

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 Code of Conduct / Acceptable Usage Agreement.
- They report any suspected misuse or problem to the *Headteacher Senior Leader; Online Safety Lead* for investigation / action / sanction.
- All digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems.
- Education in relation to online safety (4s) are embedded in all aspects of the curriculum and other activities.
- Pupils understand and follow the Online Safety Policy and Acceptable Usage policies.
- Educating the pupils to ensure that they have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulation (determine whether the materials they access online are safe).
- 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 used, it is pre-planned and pupils should be guided to sites that have been checked and deemed as suitable for their use.
- The pupils are aware of the processes are in place for dealing with any unsuitable material that is found in internet searches (do not close off the page, share it with an adult straight away).

Designated Safeguarding Lead

Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

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

Online Safety Group

The Online Safety Group consists of; the Online Safety Lead, Headteacher, Computing Governor and ICT Technician. The aim is to provide a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the Online

Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body.

Members of the Online Safety Group will assist the Online Safety Lead (or other relevant person, as above) with:

- the production / review / monitoring of the school Online Safety Policy / documents.
- the production / review / monitoring of the school filtering policy and requests for filtering changes.
- mapping and reviewing the online safety / digital literacy curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting parents / carers and the pupils about the online safety provision
- ensuring that technology has the appropriate security settings

Pupils:

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

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website

- their children's personal devices in the school (where this is allowed)

Policy Statements

Education –Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety / digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons, where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Pupils will also be taught about wellbeing, health and relationships and how online activity can adversely affect these aspects of life e.g. over-usage of technology can have impact on both your mental and physical health.
- The children will be taught about their digital footprint and how their actions online can impact future careers and relationships.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit and encourage them to add KS1, KS1 or for kids into their search.

- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need. In such cases, teaching staff would always provide a QR code for the children to scan and access a site that has already been checked.

Education – Parents / Carers

The online world develops and changes at a great speed. New opportunities, challenges and risks are appearing all the time. This can make it difficult for parents to stay up to date with the latest devices, platforms, apps, trends and related threats.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters and website.
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. [swgfl.org.uk](http://www.swgfl.org.uk)
www.saferinternet.org.uk/ <http://www.childnet.com/parents-and-carers>

Education & Training – Staff / Volunteers

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

- 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 annually.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Lead will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations e.g. Teaching Online Safety in School DFE.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff / team 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 any group involved in technology / online safety / health and safety / safeguarding. This may be offered in a number of ways:

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

Technical – infrastructure / equipment, filtering and monitoring

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

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems (termly).
- Servers, wireless systems and cabling is securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure 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 “master / administrator” passwords for the school ICT systems, used by the Network Manager (or other person) must also be available to the Headteacher and Computing Lead these will be kept in a secure place.
- 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.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider (EXA Networks – Surf Protect).
- There is a clear process in place to deal with requests for filtering changes – weekly reports sent to ICT Technician and forwarded on to Online Safety Lead.
- Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.

- The school has provided differentiated user-level filtering (allowing different filtering levels for pupils, guests and staff).
- 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 (CPOMS) for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- Temporary visitors e.g trainee/supply teachers are provided with a temporary login during their time in school. They do not have access to the school email system. Long term supply staff may be provided with their own login and email address during their time in school.
- An agreed policy is in place Acceptable Usage Policy regarding the extent of personal use that users (staff / pupils / community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place (Acceptable Usage Policy) that forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data will not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. If removal media (USB sticks) are used staff are obliged to regularly complete anti-virus scans.

Mobile Technologies

Both pupils and staff should understand that the primary purpose of the use mobile devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school policies including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme.

- The school Acceptable Use Agreements for staff, pupils and parents / carers will give consideration to the use of mobile technologies
- The school allows:

	School Devices	Personal Devices
--	----------------	------------------

	Classroom Based Computers	Staff iPads	Pupil PCs	Pupil iPads	*Pupil owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Full network access	Yes	No	No	No	No	No	No
Access to School WiFi	Yes	Yes	Yes	Yes	No	Yes	No

***These devices are allowed in school when written parental consent has been provided.**

School owned / provided devices:

- Each class teacher has a school iPad and this is recorded on Acceptable Use Agreement to ensure staff agree to accept responsibility for appropriate usage
- iPads can be used to access the internet and take photos of the children in school and for any planned out of school experiences e.g class trips, sporting events, residential.
- School iPads should not be used for taking personal photos or personal use.
- School laptops may have access to network e.g resources when used in school.
- Class teachers do have permission to install any appropriate apps for school use on ipads.
- Technical support will only be provided for school provided devices – permission should be obtained from SLT if technical support is required for any other personal devices.
- It is staff responsibility to ensure appropriate content is accessed if devices are used out of school where a filtering device is not present.
- Access to cloud services provided by school only e.g One Drive
- It is staff responsibility to ensure that Data Protection requirements are followed at all times
- Images of children can be taken in school/planned out of school events and can be stored on the ipad. They should be removed from the ipad and saved on the school network/deleted to as soon as possible and certainly by the end of each half term.
- When a staff member leaves school any school devices are handed over to the Computing Lead and the Acceptable Use Policy signed to confirm receipt of equipment and that any data relating to school will be deleted from personal computers at home. Email addresses are terminated from the day staff leave school.
- Liability for damage is normally covered under school insurance.
- Staff training will include the points mentioned in this section of the policy.

Personal devices:

- Staff are all informed that personal devices should not be used in the classrooms/areas of school when children are present/during teaching time school time unless permission has been obtained from SLT.
- Visitors to school are advised to turn mobile phones off when they enter school and not to use them when children are present.
- Staff can use mobile phones in the staffroom or in classrooms out of school hours. Staff are advised that it is not appropriate to make calls in the staffroom when other staff are present and that the office can be used if a call needs to be made.
- All staff are advised that phones need to be on silent and stored safely away during working hours. The only exception for phones to be used in class is if the DSL needs the CPOMS verification code to access the secure system.
- Staff are encouraged to take mobile phones on out of school visits but these should only be used for emergency contact with the visit leader or school.
- Office staff should have mobile phones on silent and be stored securely away during work hours e.g in handbags or cabinet in the office.
- The headteacher may occasionally need to have access to mobile phone for verification code for CPOMS, contact for staff on school visits or some other valid work reason. Wherever possible, the phone will only be used when children are not present.
- Staff do have access to their work email on personal devices and only this address should be used for school business.
- Access to the internet in school is permitted on personal devices out of working hours and when children are not present.
- Technical support is only available for personal devices if related to a school issue.
- Data Protection requirements need to be followed at all times.
- Staff are made aware through the Acceptable Use and Behaviour Policy that SLT have the right to take, examine and search users devices in the case of misuse.
- Staff are made aware that personal devices are not to be used for taking images and that school iPads should be used.
- School is not for any loss/damage or malfunction following access to the network.
- All school iPads will be labelled to identify them as school property.
- Visitors are informed about turning mobile phones off through signs in reception and by office staff reminding them when they sign in. Other visitors e.g supply staff/trainee teachers will be informed through Induction.
- Our Children and staff are reminded about the safe and responsible use of mobile devices at Safeguarding Briefings and through Online Safety education programmes.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is statutory for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website / social media / local press.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other *pupils* in the digital / video images. Parents/ carers will be made aware of this at every available opportunity.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Data Protection

With effect from 25th May 2018, the data protection arrangements for the UK change following the European Union General Data Protection Regulation (GDPR) announced in 2016. Following this, personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

As a school we ensure that:

- We hold the minimum personal data necessary to enable us to perform our function and we will not hold it for longer than necessary for the purposes it was collected for.
- The data held is accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- We follow the lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice.
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIA) are carried out.
- We have clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.
- There are clear and understood data retention policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
- Consideration has been given to the protection of personal data when accessed using any remote access solutions.
- All staff receive data handling awareness / data protection training and are made aware of their responsibilities.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

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

Communications

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

Communication Technologies	Staff & other adults				Students / Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the school	X					X		
Use of mobile phones in lessons				X				X
Use of mobile phones in social time	X							X

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

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the DSL – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- Any digital communication between staff and pupils or parents / carers (email, 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.
- Staff should not have any correspondence online linked with school and the wider community using personal accounts.
- Staff should not be friends with parents via social media platforms – this links back to the staff Code of Conduct.
- 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, local authorities have a duty of care to provide a safe learning environment for pupils and staff, all aspects of this are outlined and agreed to through use of the Acceptable Usage Agreement.

Schools, MATs and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

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

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

School staff should ensure that:

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

When official school social media accounts are established there should be:

- 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 disciplinary procedures

Personal Use:

- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to private social media sites outside working hours.

Monitoring of Public Social Media

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

The school's use of social media for professional purposes will be checked regularly by the Headteacher and Online Safety Lead to ensure compliance with the school policies.

Dealing with unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in / or outside the school / when using school equipment or systems. The school policy restricts usage for all staff 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					X

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

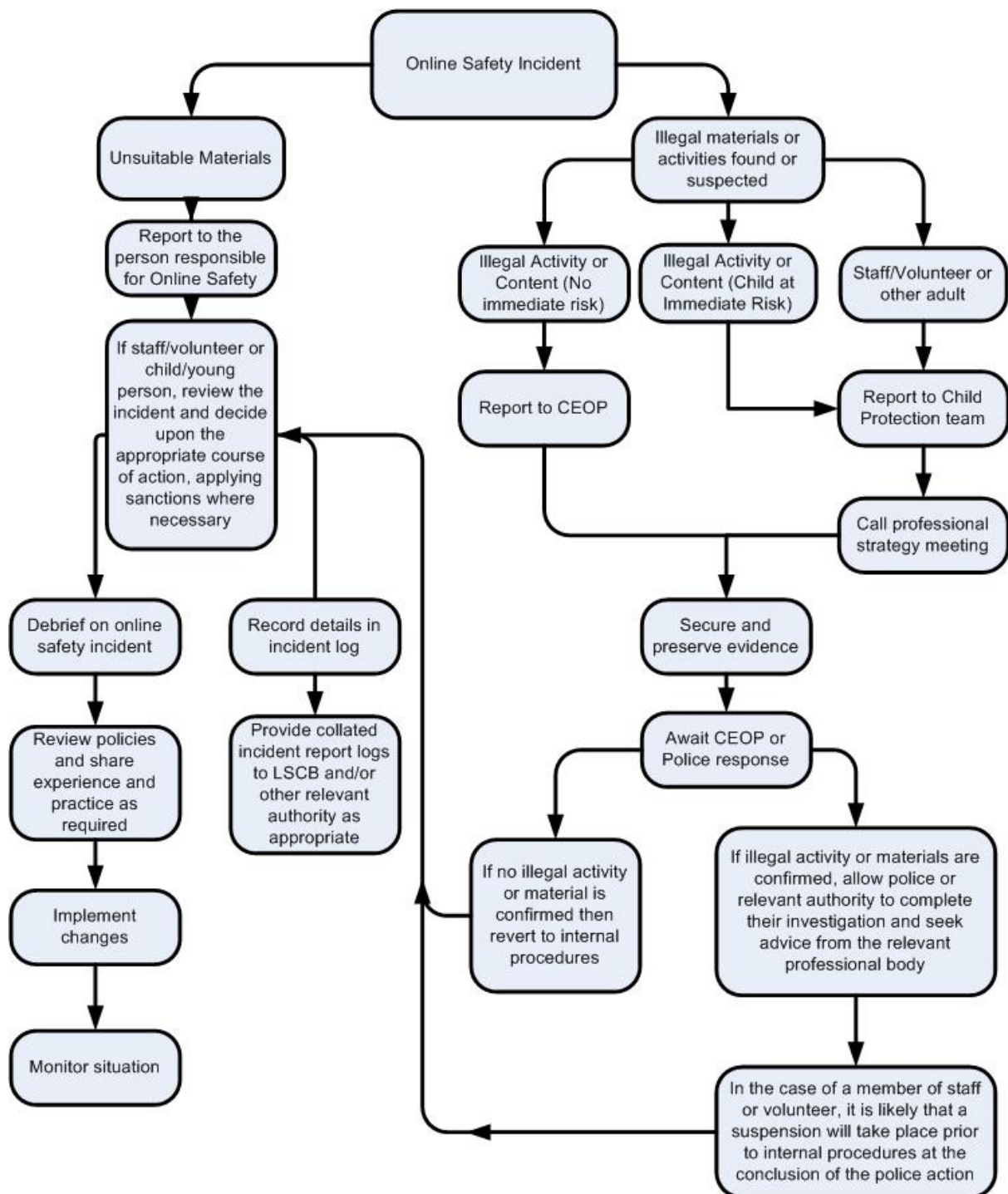
Use of video broadcasting e.g. Youtube (non-educational)		X			
--	--	---	--	--	--

Responding to incidents of misuse

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

Illegal Incidents

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



Other Incidents

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

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

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
 - Internal response or discipline procedures
 - Involvement by Local Authority 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.

Attempting to access or accessing the school network, using another student's / pupil's account	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
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X				X	
Continued infringements of the above, following previous warnings or sanctions	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	
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

Staff Actions / Sanctions

	Refer to Headteacher	Refer to Local Authority	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary Action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X			X	X
Inappropriate personal use of the internet / social media / personal email	X				X		

Unauthorised downloading or uploading of files	x			x	x		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	x			x	x		
Careless use of personal data e.g. holding or transferring data in an insecure manner	x				x		
Deliberate actions to breach data protection or network security rules	x			x	x		
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		
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils	x				x		x
Actions which could compromise the staff member's professional standing	x				x		x
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	x				x		x
Accidentally accessing offensive or pornographic material and failing to report the incident	x			x	x		
Deliberately accessing or trying to access offensive or pornographic material	x	x	x				x
Breaching copyright or licensing regulations	x				x		
Continued infringements of the above, following previous warnings or sanctions	x	x					x

Acknowledgements

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

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

© South West Grid for Learning Trust Ltd 2023