All Souls' Catholic
PRIMARY SCHOOL

ONLINE SAFETY POLICY

MAY 2022

All Souls' Catholic Primary School

Online Safety Policy

Rationale

The Internet is becoming as commonplace as the telephone or television and its effective use is an essential skill in everyday life. In preparing children for the adult world ahead, schools have a duty to embrace new technology and harness the potential learning experiences that it offers. Unmediated Internet access, however, does bring with it the possibility of placing pupils in embarrassing, inappropriate, incriminating and even dangerous situations. Therefore, it is crucial that strategies are in place to safeguard all users of the Internet within schools as well as to protect the ICT infrastructure from potential harm.

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Governing Body / Governors Sub Committee on:	*18/05/2022*
The implementation of this Online Safety policy will be monitored by the:	*SLT*
Monitoring will take place at regular intervals:	*Yearly*
The Board of Directors / Governing Body / Governors Sub Committee will receive a report on the implementation of the Online Safety Policy generated by SLT (which will include anonymous details of online safety incidents) at regular intervals:	*Reported temly to Governor meeting / sub-committee meeting*
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 2023*
Should serious online safety incidents take place, the following external persons / agencies should be informed:	*LA Safeguarding Officer, 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
    - pupils
    - parents / carers
    - staff

Scope of the Policy

This policy applies to all members of All Souls Catholic Primary School (including staff, pupils, volunteers, parents / carers, visitors) who have access to and are users of school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within All Souls Catholic Primary School

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 / Sub Committee receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

Online Safety Governor: **Shirley Langford**

- regular meetings with the Online Safety Lead
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors Committee meeting

Headteacher / SLT:

- 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 shared with Mrs Roisin McGrath.

- The Headteacher and SLT 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 – "Responding to incidents of misuse"). Online Safety BOOST includes an 'Incident Response Tool' that outines the steps (and forms to complete) any staff facing an issue, disclosure or report, need to follow. More information is available at: https://boost.swgfl.org.uk/

- The Headteacher / SLT 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 / SLT 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.

Online Safety Lead:

Online safety lead: Mr Andrew Cooke

- 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 Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors

Network Manager:

Network Manager: Mr Robert Youson

The Network Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority Online Safety Policy / Guidance that may apply.
- the filtering policy 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 use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Online Safety Lead for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

• they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices

• they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)

• they report any suspected misuse or problem to the Headteacher / SLT 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 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

Designated Safeguarding Lead

The school DSL: Mr Andrew Cooke

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

• sharing of personal data

• access to illegal / inappropriate materials

• inappropriate on-line contact with adults / strangers

• potential or actual incidents of grooming

• cyber-bullying

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 the website

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

Aims

- To provide a clear framework for the acceptable use of computers and the Internet within school.
- To support the ICT curriculum policy in ensuring that technology is widely available and used to enhance the curriculum and provide learning opportunities that without Internet use, would be impossible.
- To protect all members of the school from potential harm resulting from misuse of technology.
- To instil confidence in teachers to deliver ICT enriched lessons.
- To provide clear guidance on procedure in the instance of misuse.
- To ensure that online safety remains a high priority within the curriculum and that children learn to become 'responsible' Internet users.
- To make explicit the roles and responsibilities of all adults within school with regards to safe use of technology.

Implementation

Pupils' use of the Internet as part of the curriculum

Within all aspects of the curriculum, the Internet has much to offer pupils and an important role to play. Teachers are expected to ensure that 'new technologies', including the Internet, are used effectively to enhance teaching and learning and so pupils will have regular access to the Internet within lessons in many different contexts:

- Visiting specific websites selected by the teacher
- Using search engines to research topics
- Using information provided by the teacher, sourced from the Internet
- Multimedia content – i.e. video clips, sounds and images

Education of Children

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

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

- A planned online safety curriculum should be provided as part of PHSE lessons and should be regularly revisited.
- Key online safety messages should be reinforced as part of a planned programme of activities both during Computing and PSHE lessons, and through assemblies and events, such as Safer Internet Day

- 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
- Students / 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.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

Education of Parents/Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.
All Souls will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters and nationally available materials
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Links available through the Online Safety area of the school website

Education and Training for Staff

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

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements
- The Online Safety Lead 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 meetings / INSET days.
- The Online Safety Lead

Education and Training for Govenors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any subcommittee involved in online safety or safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association
- Participation in school training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure 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:

- Internet access is filtered for all users. This is achieved through Smoothwall web-filtering and online safety solutions. The network manager and Internet Safety lead regularly update and manage lists of site that are blocked / unblocked.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet
- 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. Impero software is used for the purposes of monitoring
- Agreed policies are also in place for the use of removable storage devices, installing applications on school computers and personal use of school computers

Whilst through the local authority firewall and filtering service, the vast majority of potentially offensive content is blocked, it is impossible to guarantee that no inappropriate material could be accessed. To minimise the possibility of pupils accessing such content, teachers should, where possible stringently vet all websites which they are asking pupils to view.

Before pupils are given access to the Internet, teachers should make them aware that they may come across inappropriate content and that if they do, they should inform a school adult immediately or if they felt too embarrassed, their parents. Parents should be made aware that if their child discloses that they were exposed to inappropriate material at school, and haven't spoken to a member of staff, then they should notify the school of this incident. Equally, if an incident is reported to a member of staff, then the parents of that child should be notified by school. All incidents of inappropriate content will be recorded on the school's electronic recording system.

Increasingly, children may use email as part of the curriculum, particularly in KS2. In these instances, pupils will use only the email accounts issued to them by the school and will only be allowed to use these accounts within directed teaching sessions at school. Children should be aware that they may receive SPAM or emails from people that they do not recognise. Again, these instances should be reported and recorded as described above. In addition, to ensure that children themselves are using

email appropriately, the network manager should routinely undertake random monitoring of email accounts and report to the Headteacher.

Pupils have no access within school to newsgroups or social media sites. Through Internet Safety education we remind children that the vast majority of social media sites operate a policy of only allowing persons over the age of 13 to register, and that registering outside of these terms and conditions is illegal. However, through the school's e-safety and cyber bullying programme we will educate children as to the safe usage and benefits of social media sites and as well as the dangers presented. Although the event of cyber bulling taking place in school is incredibly unlikely, incidents which occur outside of school are more common place. Whilst as a school we are not obliged to deal with incidents occurring outside of the school day and premises, we will always support parents in resolving any issues which we feel may impact children inside of school.

Children should be not be allowed access to chat rooms for any purpose during the school day. Again the relative merits and dangers associated with their use will be discussed with the children as part of the school's e-safety programme.

Children should be educated as to what 'piracy' means and its impact on the wider world.

Use of Mobile Technologies

Mobile technology devices may be school owned or personally owned and might include: smartphone, tablet, laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school cloud based services.

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

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

	School Devices			Personal Devices		
	School owned for single user (e.g. staff laptop)	**School owned for multiple users (e.g. pupil laptops)**	**Authorised devices (e.g. tablets)[1]**	**Pupil owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*	*No***	*Yes*	*Yes**
Full network access	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*

Internet only					*No*	*No**

* with the exception of visitors from agencies/LA where a temporary access code will be granted

** with the exception of Y6 pupils where devices will be kept securely stored in the admin cupboard during the school day and collected as pupils go home

Use of Digital video and images

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

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website / social media / local press.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes, use prior consent is received from the SLT.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs – without express permission being granted by parents. This should be sought each time.

<u>Staff use of the Internet</u>

Staff have access to the same Internet steam as pupils and therefore within the filtering system. Staff should adopt the rule that they should only use the school's Internet facility to support them in successfully fulfilling their role within school. This will include the use of the school email system.

Staff should not make use of personal email, social media sites (e.g. Facebook, twitter etc) or online sites such as eBay and online stores through the school's internet stream, or via their personal mobile devices during directed working hours.

In the instance of staff receiving inappropriate or offensive emails through their school email account, these should be reported to a member of the senior leadership team at the earliest convenience.

Staff also need to be made aware that their behaviour and use of the Internet outside of school needs to fall within the requirements as set out in the teacher standards irrespective of their role or position in school. Under no circumstances should staff make any reference, no matter how insignificant, to any school related business, on the Internet which does not relate to their role or responsibilities within school.

Although not an exhaustive list, staff should adhere to the following specific guidelines:

- Do not, under any circumstances, accept friend requests from a person you believe to be either a parent or a pupil at your school.
- Do not use Internet or web-based communication channels to send personal messages to a child or parent.
- Bear in mind that someone else could post a photo on their profile in which you are named, so think about any photos in which you appear. If you do find inappropriate references to you and/or images of you posted by a 'friend' online, you should contact them and the site to have the material removed so as to protect yourself.
- Be aware that anybody may have access to your profile. Therefore you must mind your language and behaviour such as not to cause offense or lead to complaints against you to your employer.
- Ensure that any comments and or images could not be deemed as defamatory or in breach of copyright legislation or illegal.
- Always make sure that you log out of social media sites after using them.

The school has a subscription to Google Apps for Education. This has a GoogleDrive facility which is the school's primary means of storing and sharing files. All School related files should be stored exclusively within the GoogleDrive and not transported on memory sticks or other insecure portable storage devices.

Staff should also be aware that it is their responsibility to ensure that all of the materials and media that they use, including those sourced on the Internet, are not in breach of copyright legislation.

All staff should be made aware that any personal information or records which they come into contact with at school are strictly confidential and should under no circumstances be disclosed to anyone inside or outside of school without the headteacher's permission.

There are times when school related documents are needed to be shared with third-parties or agencies. In these instances, documents should be password protected and the password sent in a separate email or ideally, via a different means (e.g. phone call).

In the event of any school information or data being lost or stolen, a member of the SLT should be informed immediately. The processes within the school's GDPR policy should then be followed.

Incidents of misuse

All incidents which are not in line with this policy are to be recorded using the school's electronic recording system and reported to governors. In the event of a member of staff disregarding the policy it would be considered as misconduct and would have to be investigated in accordance with the school's disciplinary procedures.

Internet safety education

Through both ICT and PSHE lessons, children are education in the safe use of technology. The teaching of safety should precede any use of technology within lessons. The school makes use of the resources produce by the CEOP and use the national 'Internet Safety Week' to further promote safe internet use. The SLT keep up to date with good practice guidance and legislation and ensure that teaching staff are updated through staff meetings and INSET.

Home/School Agreement

Through the Home/School agreement, children and parents subscribe to this policy and accept their roles and responsibilities in relation to Internet safety.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

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

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing"
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)

Staff must ensure that they:

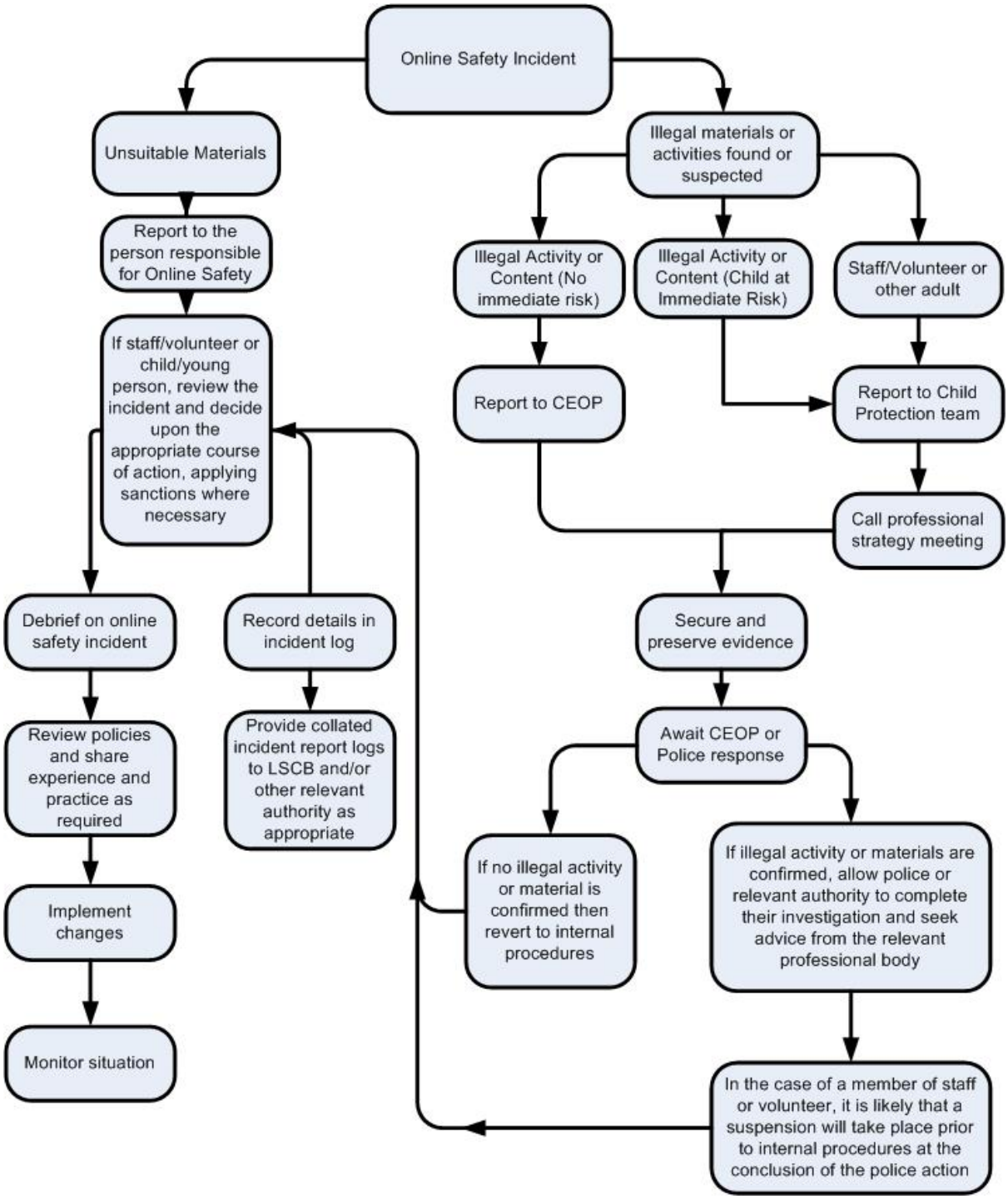
- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.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

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

If there is any suspicion that an incident involves illegal activity (or suspected illegal activity, refer to the right hand side of the Flowchart (below) and report immediately to the police. For details of what is defined as ‘illegal’ use of technology, please refer to https://ceop.police.uk/

In this instance, the technology in question should be isolated so as to preserve its state for police investigation.



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. These incidents should be dealt with in accordance with the flow chart above, and in particular, the left-hand side.

Actions and Sanctions for incidents of Misuse

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

Accidentally accessing offensive or pornographic material and failing to report the incident	X				X			
Deliberately accessing or trying to access offensive or pornographic material	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	

Staff Incidents

	Refer to Governors / LA safeguard lead	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Investigation/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
Inappropriate personal use of the internet / social media / personal email	?	?		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	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software				X	X	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	?		X	X	?
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils	X	?		X	X	?
Actions which could compromise the staff member's professional standing	?			X	X	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X			X	X	

Using proxy sites or other means to subvert the school's / academy's filtering system	?			X	X	?
Accidentally accessing offensive or pornographic material and failing to report the incident	?				X	
Deliberately accessing or trying to access offensive or pornographic material	X			X	X	X
Breaching copyright or licensing regulations	?			X	X	?
Continued infringements of the above, following previous warnings or sanctions	X					X

Acknowledgements

All Souls would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this Policy:

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

Monitoring and Review

It is the responsibility of the SLT to ensure that this policy is updated, adhered to and made widely available. It is the headteacher's responsibility to report on the effectiveness of the policy and any breaches of safety.

This policy should be reviewed annually or in the instance of legislative changes.