Date Written/reviewed February 2017	Date for Review *Review is undertaken by the Principal, SLT and LGB*
Principal Signature: **LGB Chair Signature:**	*This policy will be amended to reflect any changes in the practice described in this document.*

St. Katharine's Church of England Primary School

Internet and Online Safety Policy

From Little Acorns Great Oaks Grow

1. Leadership and Management

The Headteacher has a duty of care for ensuring the safety (including e-safety) of all members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator.

1.1 Developing a policy

Our online policy has been written by the school, building on the Wiltshire online template policy, the SWGfL (South West Grid for Learning) template policy and government guidance. It has been agreed by the senior management and approved by governors. It will be reviewed annually.

1.2 Authorised Access

- The school receives Internet Service Provision (ISP) from SWGfL and has a service which proactively monitors Internet usage for attempts to access illegal (child abuse and incitement for racial hatred) content and will notify the local police and Wiltshire Council in these instances.
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date; for instance if a pupil's access is withdrawn.
- Upon starting the school parents and children are asked to sign the Responsible Use Policy and guidance for sound, image and video for publication online.
- In reception and year 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved online materials wherever possible.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Access to the school network is through individual user accounts with a password. Pupils are encouraged to select strong passwords through e-safety sessions. Children in Hazel and Oak class have individual accounts but no passwords. Policies are in place to grant users appropriate levels of access. Pupils cannot access staff, governor or other pupils work areas.
- The admin password is held by the computing/e-safety coordinator and is also stored in the school safe should it be required in his absence.

1.3 Filtering and Monitoring

Despite careful design, filtering systems cannot be completely effective due to the speed of change of web content. Levels of access and supervision will vary according to the pupil's age and experience. Internet access must be appropriate for all members of the school community from the youngest pupil to staff.

Date Written/reviewed February 2017	Date for Review *Review is undertaken by the Principal, SLT and LGB*
Principal Signature: **LGB Chair Signature:**	*This policy will be amended to reflect any changes in the practice described in this document.*

- A log of all staff with unfiltered access to the Internet will be kept and regularly reviewed.
- A designated member of staff (Computing coordinator) will review the popular permitted and banned sites accessed by the school.
- The school will work in partnership with parents, Wiltshire Council, DFE and its ISP, and Excalibur Academies Trust to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (web address) and content must be reported to the Internet Service Provider via the online safety lead.
- Website logs will be regularly sampled and monitored by a nominee of the school and reported to the head teacher.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal or may place an individual at risk must be referred to the appropriate authorities i.e. Head teacher, LADO, Police, Internet Watch Foundation.

1.4 Risk Assessment

As the quantity and breadth of the information available through the Internet continues to grow it is not possible to guard against every undesirable situation. The school will address the issue that it is difficult to remove completely the risk that pupils might access unsuitable materials via the school system.

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Wiltshire Council can accept liability for the material accessed, or any consequences of Internet access.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The head teacher will ensure that the Internet policy is implemented and compliance with the policy monitored.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

2. Teaching and Learning

2.1 The Curriculum

The Internet is an essential resource to support teaching and learning. The statutory curriculum requires pupils to be responsible, competent, confident and creative users of technology. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources, e-mail and mobile learning. Computer skills are vital to access life-long learning and employment; indeed computing is now seen as an essential life-skill.

- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, ensure wellbeing, to support the professional work of staff and to enhance the school's management information and business administration systems.
- Whilst Internet access is an entitlement, users will need to show a responsible and mature approach to its use or this privilege may be removed.

Date Written/reviewed February 2017	Date for Review *Review is undertaken by the Principal, SLT and LGB*
Principal Signature: **LGB Chair Signature:**	*This policy will be amended to reflect any changes in the practice described in this document.*

- The Internet is an essential part of everyday life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience. The school has put considerable resources into providing a better internet connection and continues to pursue options for high speed internet access.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- E-safety should be a focus through all areas of the curriculum. The e-safety curriculum should be broad, relevant and provide progression.
- E-safety at St Katharine's is taught through the SWGfL Digital Literacy units which provide staff across the school with progressive, age appropriate materials for each class.

2.2 Parents and carers

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

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

- *Curriculum activities*
- *Letters, newsletters, web site*
- *Parents / Carers evenings / sessions*
- *High profile events / campaigns eg Safer Internet Day*
- *Reference to the relevant web sites / publications eg* www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

2.3 Enhancing Teaching and Learning

Benefits of using the Internet in education include:

- Access to a variety of worldwide educational resources.
- Inclusion in the National Education Network which connects all UK schools.
- Educational and cultural exchanges between pupils worldwide.
- Vocational, social and leisure use in libraries, clubs and at home.
- Access to experts in many fields for pupils and staff.
- Professional development for staff through access to national developments.
- Educational materials and effective curriculum practice.
- Collaboration across networks of schools, support services and professional associations.
- Improved access to technical support including remote management of networks and automatic system updates.
- Access to learning wherever and whenever convenient.

2.4 Evaluating Content

- Pupils will be taught to be critically aware of the materials they read and how to validate information before accepting its accuracy.
- Pupils will use age-appropriate tools to research Internet content.

Date Written/reviewed February 2017	Date for Review *Review is undertaken by the Principal, SLT and LGB*
Principal Signature: **LGB Chair Signature:**	*This policy will be amended to reflect any changes in the practice described in this document.*

- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.
- If staff or pupils discover unsuitable site or content they consider to be inappropriate, the machines should be secured and reported to the designated online safety lead.
- Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils will be taught to acknowledge the source of information used and to respect individuals and intellectual property when using Internet material in their own work.

3. Communication and Content

3.1 Website Content

- The point of contact on the school website should be the school address, school e-mail and telephone number. Staff or pupils' personal information will not be published.
- Written permission from individuals, parents or carers will be obtained before photographs of pupils are published on the school website. Photographs will be selected carefully and will not enable individuals to be clearly identified.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- The nature of all items uploaded will not include content that allows the pupils to be identified, either individually or through aggregated pieces of information.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies, copyright and GDPR.

3.2 Learning Platforms & Blogs

The school uses SEESAW to share learning with parents

- All users will be required to use an age appropriate password to access the relevant content of the LP which must not be shared with others.
- SLT and staff will regularly monitor the usage of Seesaw by pupils and staff in all areas, in particular message and communication tools and publishing facilities.
- Pupils/staff will be advised about acceptable conduct and use when using an online tool for learning.
- Only members of the current pupil and staff community will have access to the class accounts.
- All users will be mindful of individual and intellectual property and will upload only appropriate content to the platform.
- When a user leaves the school their account or rights to relevant content areas will be disabled.

3.3 Managing e-mail

- Pupils below year 6 will only use emails through a class email account, when appropriate, and will not have personal email accounts.
- Year 6 may be granted an individual school email account in readiness for secondary school and to allow for the use of collaborative learning tools which require individual logins.

- Pupils will sign an acceptable use agreement before being granted an individual school email account. Use of the account will be revoked if the agreement is breached.
- Pupils should use email in an acceptable way. Sending images without consent, explicit images, messages that cause distress and harassment to others are considered significant breaches of school policy and will be dealt with accordingly.
- Where class or individual child email accounts are used for a project, school staff will monitor and moderate messages sent and received.
- Staff and governors must use official school provided email accounts for all professional communications.
- E-mail sent to an external organisation should be written carefully and where appropriate, authorised before sending, in the same way as a letter written on school headed paper.

3.4 On-line communications and Social Media.

On-line communications, social networking and social media services may be filtered in school by their ISP but are likely to be accessible from home.

The Friends of St Katharine's have a Facebook page which is designed as a way of communicating and sharing information. There are two governors (chair and staff governor) who are members and are able to monitor this. The text below is the description included on the page.

> "IMPORTANT - PLEASE READ! This group is endorsed by St Katharine's School, run by the PTA and available to all current members of the school only. It is a private group, meaning that only members will be able to see what is posted here. It is intended as an informal place to share, or check on, information relating to school life. It can also be used as a way of inviting people for social events. We welcome your questions and look forward to seeing our community flourish. Please note that this page is not intended as a forum for concerns or feedback about the school itself. These are welcomed by the school, but should be directed towards the teachers or headteacher directly, and so comments that fall into this category will be removed by administrators of the page without warning. Also, any photographs have to be sent to Mrs Stagg for approval before uploading - please email them to her and she will confirm approval. Thank you for being part of our school community and we hope you find this page a useful resource"

All staff should be made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They should be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

Pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published. Schools have a key role to teach young people about the importance of how to communicate safely and respectfully online, keeping personal information private.

- Pupils will be taught about how to keep personal information safe when using online services. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.

- Pupils will be taught about the dangers of revealing personal details of themselves or others in online communication, including the tagging of photos or video, or to arrange to meet anyone.
- Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.
- Staff official blogs or wikis should be password protected and only operate with approval from the SLT.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupil will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- No member of the school community should publish specific and detailed private thoughts about the school, especially those that may be considered threatening, hurtful or defamatory.
- Parents wishing to photograph or video at an event should be made aware of the schools expectations and be required to comply with the schools RUP as a condition of permission to photograph or record.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Responsible Use Policy and in the staff code of conduct.
- In line with, 'Guidance for Safer Working Practice for Adults who Work with Children and Young People' it will not be considered appropriate for staff to engage in personal online communications with children and young people, parents or carers. Express care is also to be taken regarding the use of social networking sites.

3.5 Mobile Devices (Including Bring You Own Device-BYOD)

Mobile devices refer to any device that provides access to the internet or internal network for example, tablet (Apple Android, Windows, and other operating systems) e-readers, mobile phone, iPad, iPod touch, digital cameras.

This section covers the use of school iPads and BYOD devices.

The use of mobile devices is permitted in school, and is subject to the following key principles:

- All individuals are protected from inappropriate material, bullying and harassment
- Users have access to resources to support learning and teaching
- Users should be given clear boundaries on responsible and professional use

- Mobile devices that are brought in to school remain the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items.
- Any pupil using their own device in school will need to sign a copy of the schools BYOD policy (see supporting documents)

- School staff authorised by the Head teacher may search pupils or their possessions, and confiscate any mobile device they believe is being used to contravene school policy, constitute a prohibited item, is considered harmful, or detrimental to school discipline. If it is suspected that the material contained on the mobile device relates to a criminal offence, the device will be handed over to the Police for investigation.
- Sending abusive or inappropriate messages or content is forbidden by any user within the school community.
- Mobile devices may be used during lessons or formal school time as part of approved and directed curriculum based activity.
- Mobile devices are not permitted to be used in certain areas or situations within the school site e.g. changing rooms or toilets, situations of emotional distress etc.
- Where staff may need to contact children, young people and their families within or outside of the setting in a professional capacity, they should only do so via an approved school account (e.g. e-mail, phone, social media) In exceptional circumstances (of school activities) there may be a need to use their own personal devices and account; this should be notified to a senior member of staff ASAP.
- Staff should be provided with school equipment for the taking photos or videos of pupils linked to an educational intention.
- Where staff may have images of school or children on a school laptop or iPad used at home the images remain the property of the school and are protected by the data protection act. Staff cannot publish or use these images for any purpose other than educational and classroom based.
- For the safeguarding of all involved, users are encouraged to connect mobile devices through the school wireless provision and service that allows the ability to filter any device that uses the school Internet connection, without having to configure the user's device.
- The school will take steps to monitor responsible use in accordance with the Responsible Use Policy

3.5.1 Mobile Phones

- Children are not permitted to bring mobile phones into school and these may be confiscated and returned to their parent at the end of the day if found.
- Staff may bring their mobile phones into school but these must remain in either the school offices or staffroom and be used during break time / after school except in exceptional circumstances when a plan will have been agreed with the Headteacher.
- During off site activities, staff mobile phones form an important part of our risk assessment and safeguarding procedures. Therefore staff will have their phone on them but should only use their device if required for educational / safeguarding purposes.

3.6 Video Conferencing

- Video conferencing may include FaceTime, Skype, Lync as well as other sites.
- Staff must refer to any Responsible Use agreements prior to children taking part in video conferences.
- All video conferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Pupils will ask permission from a teacher before making or answering a video conference call.
- Video conferencing will be supervised.

3.7 Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Date Written/reviewed February 2017	Date for Review *Review is undertaken by the Principal, SLT and LGB*
Principal Signature: **LGB Chair Signature:**	*This policy will be amended to reflect any changes in the practice described in this document.*

3.8 Cyber Bullying

Cyber bullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet, to deliberately hurt or upset someone" DCSF 2007.

Cyber bullying (along with all other forms of bullying) of or by any member of the school community will not be tolerated. Full details are set out in the school's behaviour, anti-bullying and child protection policies, which should include:

- Clear procedures set out to investigate incidents or allegations of cyber bullying.
- Clear procedures in place to support anyone in the school community affected by cyber bullying.
- All incidents of cyber bullying reported to the school will be recorded.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the ISP and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyber bullying and the school's e-Safety ethos.

3.9 Data Protection

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. The Data Protection Act 1998 gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information.

Schools will already have information about their obligations under the Act; this section is a reminder that all data from which people can be identified is protected. For advice and guidance relating to a contravention of the Act, contact www.wiltshire.gov.uk

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
-

3.9.1 Digital Images

- **When using digital images, staff should inform and educate students / 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 eg on social networking sites.**
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use 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 students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.*
- *Students / pupils must not take, use, share, publish or distribute images of others without their permission*
- *Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.*
- *Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.*
- *Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website*

3.9.2 Cloud Based Storage

The increasing use of cloud based technologies has a place in education but the use of any cloud storage solution or apps and websites that store data 'in the cloud' must be part of the e-safety leads audit of cloud storage. To be approved as safe, following current guidance, the company concerned privacy policy must state that data is stored within the Europe Union or is subject to the 'Safe Harbour Agreement', although these may change in time.

4 Implementation

4.1 Policy in Practice - Pupils

- All users will be informed that network and Internet use will be monitored.
- Online Safety teaching should be integral to the curriculum and raise the awareness and importance of safe and responsible internet use amongst pupils.
- Online Safety teaching will be included in PSHE, Citizenship and/or ICT and cover safe use at school and home.
- Online Safety rules and/or copies of the Responsible Use Policy will be on display in all rooms with Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.

4.2 Policy in Practice – Staff

- The Online Safety Policy will be provided to and discussed with all members of staff and Responsible User Policy signed for compliance
- Staff should be aware that Internet traffic is monitored (and automatically reported by the SWGfL) and can be traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- Staff will be asked to sign an acceptable use policy covering school laptops and iPads
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- Staff training in the form of INSET and staff meetings will be used to keep staff upto date with developments within e-safety. The e-safety lead will attend formal CPD events and briefings and

disseminate this information and any resources to staff. Where relevant, if a need is identified individual members of staff may attend e-safety training events.

- Guidance will be given to staff as part of training events on protecting their online professional identity.

4.3 Policy in Practice - Parents

- Parents' attention will be drawn to the Online Safety Policy and Responsible User Policy RUP in newsletters, school prospectus and Website.
- A partnership approach with parents will be encouraged. This could include offering parent evenings, demonstrations, practical sessions and suggestions for resources and safer Internet use at home.
- Regular information will be provided to parents about how to ensure they can work with the school to ensure this resource is used appropriately both within school and home.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

4.4Handling of complaints

- Responsibility for handling incidents will be delegated to the computing coordinator.
- Any complaint about staff misuse must be referred to the head teacher.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

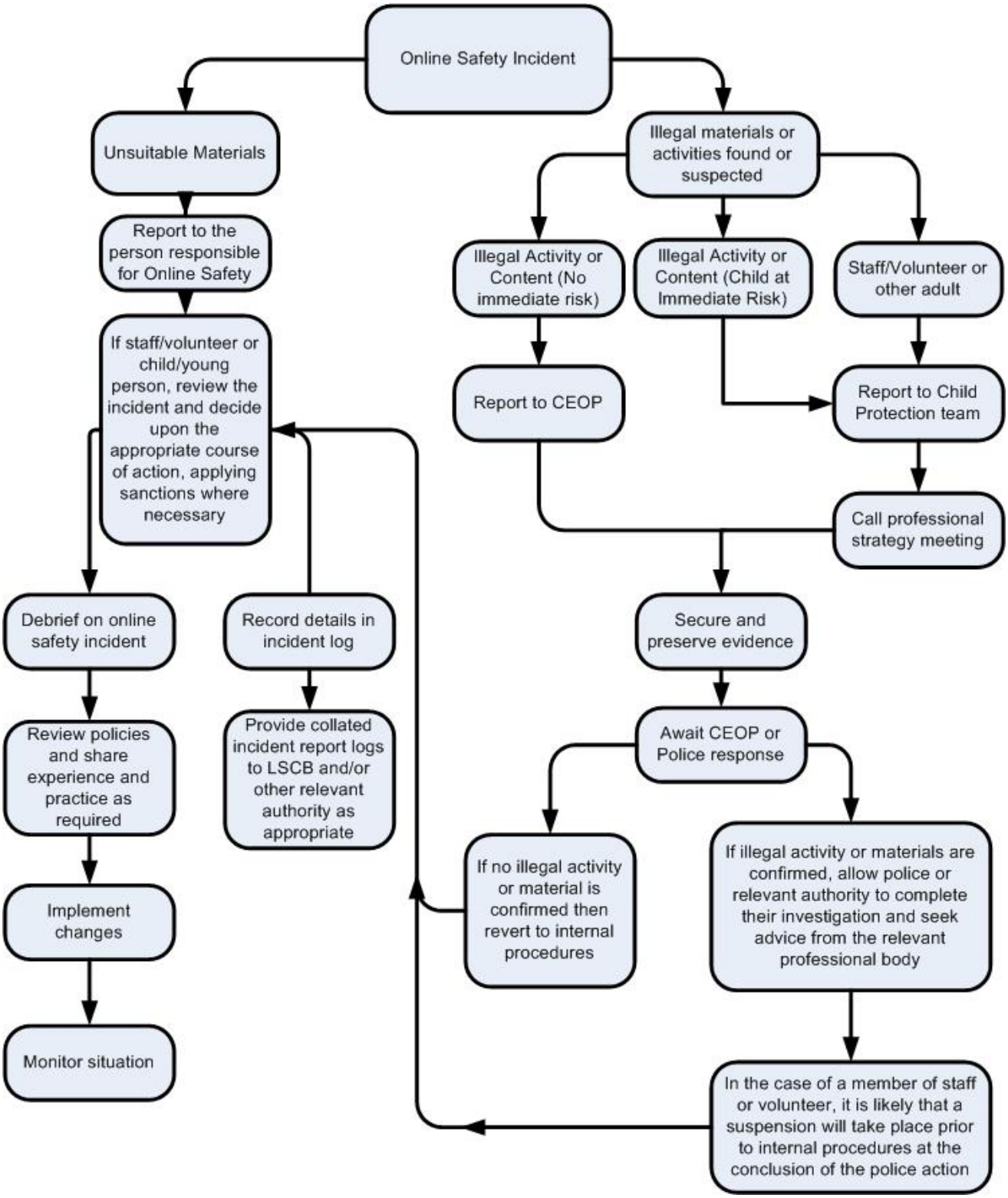
4.5 Responding to incidents of misuse

On the discovery of any images or content that cause concern the device concerned should be secured (a laptop's lid closed or an iPad's screen turned off. Do not close the device down as this may lose the image and prevent any further action being taken.

4.5.1 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.

Date Written/reviewed February 2017	Date for Review *Review is undertaken by the Principal, SLT and LGB*
Principal Signature: **LGB Chair Signature:**	*This policy will be amended to reflect any changes in the practice described in this document.*



Date Written/reviewed February 2017	Date for Review *Review is undertaken by the Principal, SLT and LGB*
Principal Signature: **LGB Chair Signature:**	*This policy will be amended to reflect any changes in the practice described in this document.*

4.5.2 Other Incidents

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

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

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action
- **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

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

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with

Date Written/reviewed **February 2017**	**Date for Review** *Review is undertaken by the Principal, SLT and LGB*
Principal Signature: **LGB Chair Signature:**	*This policy will be amended to reflect any changes in the practice described in this document.*

It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures