St Elizabeth's Catholic Primary School

On-line safety policy

Adopted-October 2019
Review date-October 2021

St. Elizabeth's Catholic Primary School
On-line safety Policy

'We listen, learn and grow with Jesus'

Mission statement
At St Elizabeth's Catholic Primary School we strive for fullness of life for everyone. Through education and prayer, we listen, learn and grow with Jesus.

Our Aims:

- To encourage the Christian ethos of the school through daily promotion of the Mission Statement, living out the values and teachings of our Catholic faith, in a multi-cultural global community;
- To provide a safe and secure learning environment in which all members of the school community achieve success and realise their full potential;
- To create a caring and supportive atmosphere in which all members of the school are listened to and respected, demonstrating good manners towards each other and developing positive relationships within the wider community;
- To provide a broad and balanced curriculum encouraging children to be independent thinkers and achieve personal success;
- To provide a variety of opportunities for pupils to explore their own learning and develop their interests and abilities.

Development / Monitoring / Review of this Policy

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

- Headteacher
- Senior Leaders
- Computing leader
- Governors

Consultation with the whole school has taken place through a range of formal and informal meetings.

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Board of Governors in:	*October 2019*
The implementation of this Online Safety policy will be monitored by the:	*Senior leadership team* *Safeguarding governor*
Monitoring will take place at regular intervals:	*Termly by senior leaders*
The Leadership and management governors committee will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*Annually*
The Online Safety Policy will be reviewed every 2 years, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or	*October 2021*

incidents that have taken place. The next anticipated review date will be:	
Should serious online safety incidents take place, the following external persons / agencies should be informed:	*Eg, LA Safeguarding Officer, LADO, Police*

The school will monitor the impact of the policy using: Logs of reported incidents

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

Scope of the Policy

This policy applies to all members of the school (including staff, 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 school will deal with any incidents inside and outside of school 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 the 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 leadership and management 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:

- regular meetings with the Online Safety Co-ordinator
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- reporting to relevant Governors / Board / Committee / meeting

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 Computing leader who acts as on-line safety leader also.
- The Headteacher and (at least) another member of the Senior Leadership Team / Senior Management Team should be 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 disciplinary procedures).
- The Headteacher and 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 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. This training has been provided by the local authority to the headteacher and deputy headteacher. The deputy headteacher receives reports of online safety incidents and creates a log of incidents to inform future online safety developments, and will share any concerns with the headteacher.

Online Safety Lead / Computing 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 where needed
- liaises with school technical staff when needed
- liaises with the local authority when needed
- meets with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs where needed
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

Network Manager / Technical staff

The school has a managed ICT services through an outside contractor (Link2ICT) However, it is still the school's responsibility to ensure that our managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school technical staff, as suggested below. It is also important that the managed service provider is fully aware of the school's Online Safety Policy and procedures.

The Network Manager (Link2ICT) alongside the school's computing / on-line safety lead are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that *the school meets* required online safety technical requirements and any Local Authority Online Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy, is applied and updated on a regular basis
- 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 and Senior Leaders, for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school.

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 and computing lead 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

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
- online-bullying

Students / 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 know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on 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 / Learning Platform and on-line student / pupil records

Community Users

Community Users who access school / academy systems / website / Learning Platform as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school / academy systems.

Policy Statements

Education Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety / 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 provided as part of Computing / PHSE lessons
- Key online safety messages reinforced as part of a planned programme of assemblies and pastoral activities
  Pupils being 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 being taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils being 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 being 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 acting 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.
- It is accepted that from time to time, for good educational reasons, students may need to research topics that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents / 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 online 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, Learning Platform
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications

Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's online safety knowledge and experience where appropriate. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety (eg. NSPCC workshops)
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community

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:

- Formal online safety training will be made available to staff through staff meetings. This will be regularly updated and reinforced. Regular updates will be given in weekly staff meetings as part of the standing safeguarding agenda item.
- 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. Where this is the case specific training opportunities will be sought.
- The designated safeguarding leads will receive regular updates through attendance at external training events (eg from SSCB) 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.
- The computing lead and designated safeguarding leads will provide advice / guidance / training to individuals as required.

Training – Governors

Governors will have the opportunity to take part in online safety training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in technology / online safety / health and safety /safeguarding. This may be offered in a number of ways:

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

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / 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. This is supported by the local authority and the school's contract with Link2ICT.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located.
- 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 network manager who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The "master / administrator" passwords for the school ICT systems, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader upon request and kept in a secure place (eg school safe)
- The network manager (Link2ICT) 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 (eg. child sexual abuse images) is filtered by the broadband or filtering provider. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes and permission from the headteacher is required in all instances.
- Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school uses enhanced filtering accessed through Entrust, Staffordshire.
- School 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.
- Users must report any actual / potential technical incident / security breach to the class teacher or headteacher.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems. A specified log in has been created for supply staff when using school equipment.
- School devices should be used for school business and are only to be used by the member of staff to whom they have been allocated.

- The use of removable media (eg memory sticks) by users on school devices is managed through the use of a 'shared area' which can be accessed remotely, removing the need for memory sticks. Personal data cannot be taken off the school site unless safely encrypted or otherwise secured. (see School GDPR Policies for further detail)

Mobile Technologies

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

All users should understand that the primary purpose of the use of 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, Anti-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.

School owned devices

School provide each teacher with a laptop for school use. Each class also has an i-pad for use in the curriculum. There are also i-pads and chrome books which can be used by all classes across the school. The class i-pads and teacher lap tops are solely for the use of the named teacher or class whereas the chrome books and set of i-pads are held centrally. All these devices allow access to the internet in school. The chrome books and i-pads are for use in school only whilst the laptops can be taken from school by the named teacher but remain the responsibility of that teacher at all times.

Staff can request the installation of a specific app to the i-pads to support teaching and learning. However, this must be authorised by the headteacher and managed by the network manager.

Staff can access the 'shared google drive' when using laptops at home in order to avoid the use of memory sticks but must ensure that the school's GDPR policy and procedures are adhered to at all times.

All work on lap-tops, chrome books and i-pads are subject to the same filtering systems as desk top computers and are monitored in the same way.

School acknowledge that there are times when taking photographs of pupils is necessary for curriculum work and for general classroom reasons. However, these images should be deleted at the earliest opportunity and should not be stored on any device any longer than is necessary.

Personal devices

It is acknowledged that staff may wish to bring personal devices such as mobile phones into school. However, for safeguarding reasons, it is important that these are subject to a policy which protects both pupils and staff.

All mobiles phones must be either locked away in individual staff lockers or turned off and kept out of sight in staff bags during the school day. Personal devices such as mobile phones can be used in the staff room or Blake room during the school day. Once pupils have left the school

site, personal mobile phones are able to be used in classrooms. Staff mobile phones can be taken on educational visits for the purpose of emergency contact only.

No mobile phones can be kept in early years classrooms and must remain in staff lockers. When a visitor to school is visiting an early years classroom, they will be asked to hand their phone into the office.

If a member of staff is dealing with an emergency situation and they feel they need additional access to their mobile phone during teaching hours, this must be discussed and agreed by the headteacher.

Ideally, any school business should not be undertaken on personal devices. If a member of staff feels that this is necessary, it should be discussed with the headteacher.

No technical support is available for personal devices.

It is prohibited for any image of a pupil to be taken or stored on a personal device in any circumstance.

Pupils are not encouraged to bring mobile phones into school. However, where parents deem this necessary for safety after school, pupils must leave their phone in the school office and return to collect it at the end of the day. Pupils phones will be signed in and out each day.

It is acknowledged that parents may wish to use mobile devices to photograph their own child at events such as star assemblies or concerts. At these times, parents will be informed that this is permitted but that they are for personal use only and must not be shared on social media. No photography is permitted in Mass.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students / 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.
- 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.

- 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 never 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 students / 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, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

GDPR

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.

Removable device should not be used to transport data unless permission has been granted by the headteacher. If, in exceptional circumstances personal data is stored on any portable computer system, memory stick or any other removable medi. er.):

- The data must be encrypted and password protected.
- The device must be password protected. (many memory sticks / cards and other mobile devices cannot 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 / academy policy (below) once it has been transferred or its use is complete.

Communication

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 should therefore use only the school email service to communicate with others when in school, or on school / (e.g. by remote access).
- Users must immediately report, to the headteacher, 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 parents / carers 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.

- 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.

Social Media - Protecting Professional Identity

All schools have a duty of care to provide a safe learning environment for pupils and staff. 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 liable to the injured party and bring the school into disrepute. 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:

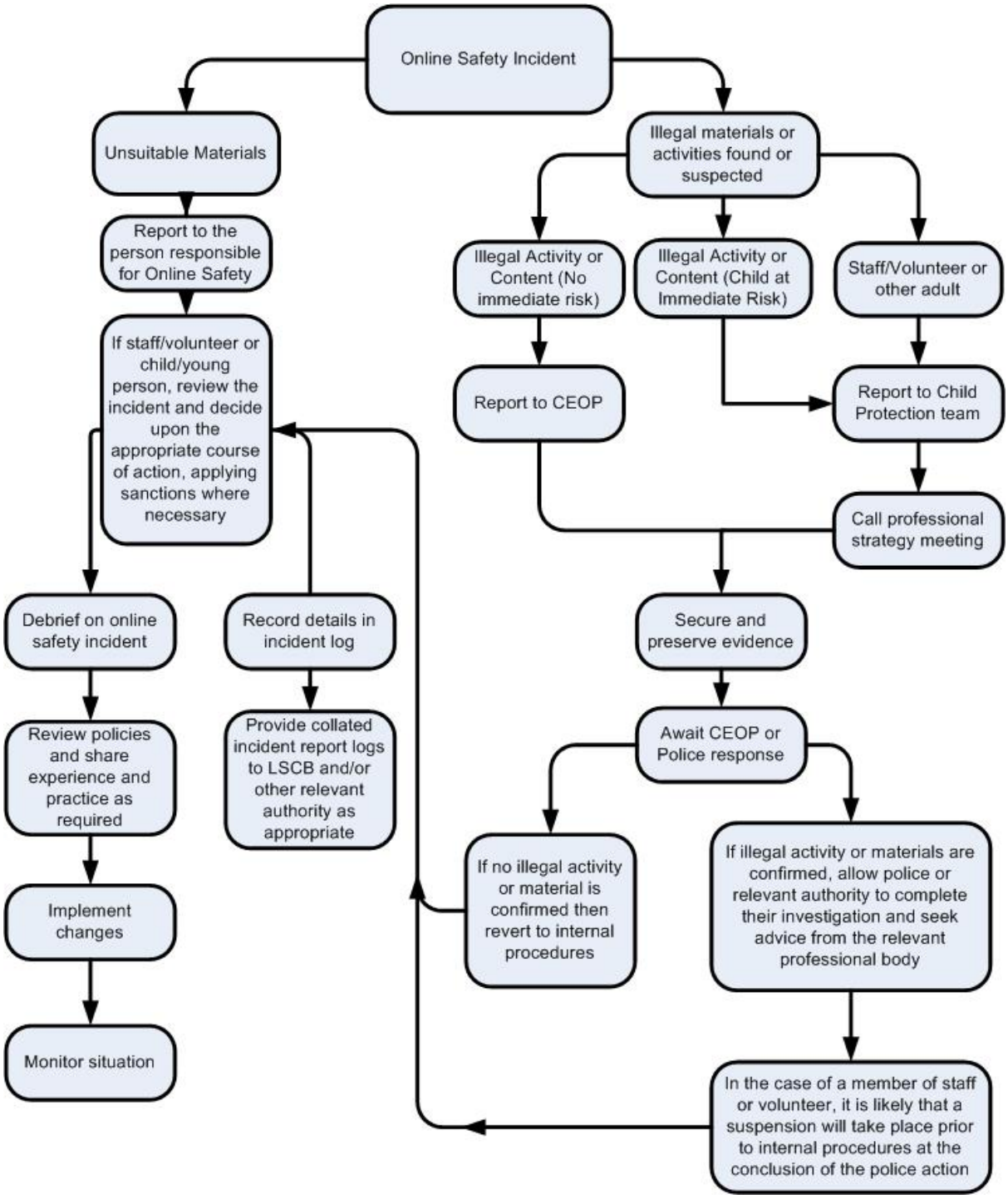
- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference is made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- Where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school.

Illegal Incidents

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


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

Other Incidents

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

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

- Have more than one senior member of staff 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
    - 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.