E-SAFETY POLICY

January 2017

Adopted by FGB: 11th January 2017
Review Period: 3 yearly
Minute No: 17/1/16/4
Review Date: January 2020

Development/Monitoring/Review of this policy

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the Governing Body on:	
The implementation of this e safety policy will be motivated by the:	Senior Leadership Team, e-safety coordinator, Governors, school council, Digital Leaders (champions)
Monitoring will take place at regular intervals	Annually
The governing body will receive a report on the implementation of the e-safety policy generated by the monitoring of this group (which will include anonymous details of e-safety incidents) at regular intervals	Annually
The E-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 e-safety or incidents that have taken place. The next anticipated review date will be:	July 2018
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	ICT Coordinator, SLT, Head teacher, Social Care, Police – where advised

The school will monitor the impact of the policy using:

- My Concern safeguarding tool
- Surveys / questionnaires of students / pupils/ parents
- Feedback from parents /carers
- Feedback/training requests from staff
-

Scope of Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school IT systems, both in and out of the school. At Wimborne First School we strive to keep all children safe with their use of technology and educate them accordingly. Alongside this, we recognise the importance of providing support to parents/carers about the potential risks here, at home and in the wider community. Technology has many potential benefits that impact the lives of everyone; it transforms the way that schools teach and children learn. With technology developing at a fast rate the use of it at home is changing the way children live and socialise. Although technology has many beneficial elements it also brings many risks and potential dangers to children and staff. These are a few:

- Access to a range of harmful or inappropriate content
- Unauthorised access to personal information or private data
- Grooming by those with whom they make internet contact
- Unauthorised sharing/distribution of personal images
- Inappropriate communication with others
-Cyberbullying
- Access to unsuitable videos and games
- Copyright infringement
- Illegal downloading

Wimborne First School Aims:

At Wimborne First School the safety of all our children is important; we strive to implement a safe environment where they can experience the opportunities to use technology in beneficial ways. We believe it is important to educate all children, parents, carers and staff on the potentials risks and dangers of using the internet inappropriately. To achieve these our aims are as follows:

- We aim to develop our ICT teaching and learning through the supervised use of the Internet and a range of other software which is provided to enhance learning across curriculum areas.
- It is the policy of the school that all children shall receive equal opportunities regardless of gender, ability or ethnic background. Where possible, opportunities should be given to children without access to computers at home to be able to use school computers outside of usual curriculum times (ICT club). Children's social, moral, spiritual and cultural understanding will be developed and enhanced through the use of the Internet, carefully monitored by the ICT Subject Leader and class teachers. Any issues that arise will be recorded on the safeguarding system 'My Concern' and will also be reported to the school e-safety officer, Miss G Allen and Headteacher, Mrs S Hartley.
- It is essential to ensure that children understand the way ICT affects their lives and why it is important to be able to use the Internet confidently and safely. We therefore aim to ensure regular supervised access to the Internet at KS2 with confident and competent teachers or teaching assistants available to guide their use.

Roles and Responsibilities

This section outlines the e-safety Roles and Responsibilities of individuals and groups within Wimborne First School

Governors:

Governors are responsible for the approval of the E-safety policy and for reviewing the effectiveness of the policy. This will be carried out by the governors receiving termly information about e-safety incidents and monitoring reports. A member of the governing body has taken on the role of e-safety Governor. The role of the E-safety Governor/director will include:

- Regular meeting with the E-safety co-ordinator
- Regular monitoring of E-safety incident logs
- Regular monitoring of filtering
- Reporting to relevant governors

The nominated E Safety Governor is Mrs Ingrid Fido

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, through the day to day responsibilities for e-safety which will be delegated to the E-safety Co-ordinated.
- The Headteacher and (at least) another member of the Senior Leadership team should be aware of the procedures to be followed in the event of a serious E-safety allegation being made against a member of staff.
- The Headteacher/Senior Leadership Team are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher/Senior Leadership Team will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

E-Safety Coordinator

The role of the E Safety Co-ordinator is to:-

- Lead on e-safety issues across all year groups.
- Take on day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents
- Ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- Provide training and advice for staff
- Liaise with the Local Authority/relevant body
- Liaise with school ICT provider (SWGFL and SchoolCare)
- Receive reports of e-safety incidents and creates a log of incidents to inform future e- safety developments
- Meet regularly with E-Safety Governor to discuss current issues, review incident logs and filtering/change control logs
- Attend relevant meetings regarding E safety

The E safety Co-ordinator is also responsible to liaise with the schools bought in professional ICT services. At present this is provided by SchoolCare. The E safety co-ordinator will ensure that….

- The school's technical infrastructure is secure and is not open to misuse or malicious attack
- The school meets required e-safety technical requirements and any Local Authority/other relevant body E-safety Policy/Guidance that may apply
- Users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role
- Use the network/internet/remote access/email is regular monitored in order that misuse/attempted misuse can be reported to the Headteacher/E-safety Coordinator
- Monitoring software/systems are implemented and updated as agreed

Teaching and Support Staff

They are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety matters and of the current school e –safety policy and practices
- They have read, understood and signed the staff acceptable use agreement
- They report any suspected misuse or problem to the Headteacher/E-safety Coordinator
- All digital communications with pupils/parents/carers should be on a professional level and only carried out using official school systems

- E – safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the e-safety and acceptable use agreements
- 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 unsuitable material that is found in internet searches

All pupils/staff use the Hector Protector screen-saver

Child Protection/Safeguarding Designated Person:

The Child Protection/Safeguarding Designated Person should be trained in e-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

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 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 e-safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good e-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/VLE and on-line student records.

Students – Digital Leaders (Year 4)

A selection of Year 4 children will meet once a half term with the IT Leader to discuss e-safety issues and have a hands on approach to promoting good e-safety throughout the school. The Digital leaders will be responsible for:

- Promoting good e-safety throughout the school
- Discussing ways to ensure everyone is a e-safety champion
- Work with younger children to promote e-safety
- Create presentations/posters
- Suggest possible software/hardware which might be useful
- Celebrate achievements for e-safety champions

Community Users/Visitors:

Community Users/visitors who access school systems / website as part of the wider *school* provision will be expected to sign a Community User AUP before being provided with access to school systems.

Education – Pupils

The education of *pupils* in e-safety is an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety is a primary-focus in all areas of the curriculum and the staff is expected to reinforce e-safety messages across the curriculum. The e-safety curriculum must be broad, relevant and progressive, with opportunities for creative activities. This is provided in the following ways (drawing upon the resources of the SWGL, CEOP and 'think-u-know', Safer Internet Day and beyond:

• A planned e-safety curriculum is provided as part of Computing / PHSE / other lessons and should be regularly revisited;

• Key e-safety messages are reinforced as part of a planned programme of assemblies every half term and pastoral activities (eg E- Safety posters, posted around the school);

• Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and are guided in their validation of the accuracy of information;

• Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

• Pupils are helped to understand the need for the Pupil Acceptable Use Agreement and are encouraged to adopt safe and responsible use both within and outside school.

• Staff MUST act as good role models in their use of digital technologies, the internet and mobile devices (including social media/Twitter etc);

• In lessons where internet use is pre-planned, it is expected practice that pupils be guided to sites pre-checked as being 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. YOUTUBE is filtered and any use of YOUTUBE by staff is pre-planned and viewed to ensure that the material is genuine and that links are not inappropriate. The use of SAFESEARCH is expected at all times;

• NO PUPIL is permitted to access YOUTUBE or social media sites (including email) when in school; (this will be filtered on all devices)

Wimborne First School E-Safety Motto:

'Safety begins with you and me, following the steps is the key, when online we must take care and always think wisely about what we share!'

Education – Parents/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 their 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, website,
• Parents / Carers evenings / sessions
• High profile events / campaigns eg Safer Internet Day
• Reference to the relevant web sites / publications

Education and training – staff/volunteers

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

• A programme of formal e-safety workshops will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out annually. It is expected that some staff will identify e-safety as a training need within the performance management process.

• All new staff should receive e-safety training/meeting as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
• The E-Safety Coordinator (or other nominated person) will receive regular updates through attendance at external training events (eg from LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
• This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
• The E-Safety Coordinator will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular focus upon those who are members of any sub-committee / group involved in technology / e-safety / health and safety / child protection. This may be offered in a number of ways:

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

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 e-safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- The ICT Leader and Finance Officer 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 and checked fortnightly by SchoolCare.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An incident log/reporting form for users to report any actual / potential technical incident / security breach to the relevant person, is in place.
- 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.

Bring Your Own Device (BYOD):

This is prohibited.

- No member of staff/visiting staff/volunteers are allowed to use their own mobile devices or ipads within the school when pupils are present.
- No member of staff is allowed to take a camera of ipad from school premises and these should be locked away in the cabinet at the end of the day. Each device should be signed out. Laptops may be taken for use at home. Any photographs downloaded to laptops should be saved in a file on shared resources and not accessed from home. Digital images/videos of children's learning should not be saved in documents on any log in.
- Parents/carers are allowed to take digital images and videos of their children at school events for their own personal use with permission from the school. Everyone's privacy must be respected and protected therefore these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving their children in digital/video images.
- Any member of staff leaving the school must hand over all laptops to the Headteacher at the end of their contract.

Use digital and video images:

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is 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 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.

- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students / pupils are taken or published on the school website
- Pupil's work can only be published with the permission of the pupil and parents or carers.
-

Private personal use

Private personal use is permitted as long as such use does not interfere with their work and does not conflict with other aspects of this code of practice. Priority for computer usage should always be given to the core functions of the school. Use for business purposes or personal gain is not permitted.

Data Protection:

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

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.

- Don't disclose any information to a third party
- Don't risk accidental disclosure
- Don't leave your computer unattended when logged into a system
- Do protect your computer by logging off or locking it if you leave it
- Do keep your password secure
- Do change your password regularly
- Don't use obvious passwords anywhere – don't use surnames etc letters and numbers required
- Don't disclose your password
- Do use a mix of letters and numbers to make difficult to guess your password
- Don't allow anyone else to use your user account
- Don't use anybody else's user account
- Do prevent unauthorised access to sensitive personal data (e.g. password-protect spreadsheets and other documents)
- Be aware of schools backup procedures and take appropriate precautions in the light of these. Back up on your server or memory stick.
- Keep data secure when it is kept on other storage devices (e.g. CD, USB memory stick)

Communications:

A wide range of rapidly developing communications technologies has the potential to enhance learning.
When using communication technologies the school considers the following as good practice:
• The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
• Users must immediately report to the HeadTeacher– in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
• Any digital communication between staff and parents/carers (email, chat, etc) must be professional in tone and content.
• Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
• Personal information should not be posted on the school/ website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity:

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.
The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:
• Training to include: acceptable use; social media policy; checking of settings; data protection; reporting issues.

• Clear reporting guidance, including responsibilities, procedures and sanctions.

• Risk assessment, including legal risk.

School staff should ensure that:

• No reference should be made in social media to students, 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 or local authority.

See Social Networking Policy for more detail

Appropriate and Inappropriate Use by Staff or Adults:

- Staff members have access to the network so that they can obtain age appropriate resources for their classes and create folders for saving and managing resources.
- They have a password to access a filtered internet service and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in.

- All staff should receive a copy of the E-Safety Policy, social networking policy and a copy of the Acceptable Use Agreement, which they need to sign, return to the school, to keep under file with a signed copy returned to the member of staff.
- The Acceptable Use Agreement will be displayed in the staff room as a reminder that staff members need to safeguard against potential allegations and a copy of this policy is provided to all staff for home use.
- When accessing the ICT Learning Platform from home, the same Acceptable Use Agreement will apply. The acceptable use should be similar for staff to that of the children and young people so that an example of good practice can be established.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- The school's use of social media is prohibited.

In the Event of Inappropriate Use

If a member of staff is believed to misuse the internet or learning platform in an abusive or illegal manner, a report must be made to the Headteacher/Senior Designated Person immediately and then the Managing Allegations Procedure and the Safeguarding and Child Protection Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

Appropriate and Inappropriate Use by Children or Young People:

Acceptable Use Agreements detail how children and young people are expected to use the internet and other technologies within school, including downloading or printing of any materials. The agreements are there for children and young people to understand what is expected of their behaviour and attitude when using the internet. This will enable them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another child, or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

- School should encourage parents/carers to support the agreement with their child or young person. This can be shown by signing the Acceptable Use Agreements together so that it is clear to the school/education setting or other establishment that the agreement are accepted by the child or young person with the support of the parent/carer. This is also intended to provide support and information to parents/carers when children and young people may be using the Internet beyond school/education setting or other establishment.
- Further to this, it is hoped that parents/carers will add to future rule amendments or updates to ensure that they are appropriate to the technologies being used at that time and reflect any potential issues that parents/carers feel should be addressed, as appropriate.
- The downloading of materials, for example, photographs need to be appropriate and 'fit for purpose' based on research for work and be copyright free.
- File sharing via e-mail, weblogs or any other means online should be appropriate and be copyright free when using the learning platform in or beyond school/education setting or other establishments.

In the Event of Inappropriate Use

Should a child or young person be found to misuse the online facilities whilst at school, the following consequences should occur:

- Any child found to be misusing the internet by not following the Acceptable Use Agreement may have a letter sent home to parents/carers explaining the reason for suspending the child or young person's use for a particular lesson or activity.
- Further misuse of the agreement may result in further sanctions which could include not being allowed to access the internet for a period of time.
- A letter may be sent to parents/carers outlining the breach in Safeguarding Policy where a child or young person is deemed to have misused technology against another child or adult.

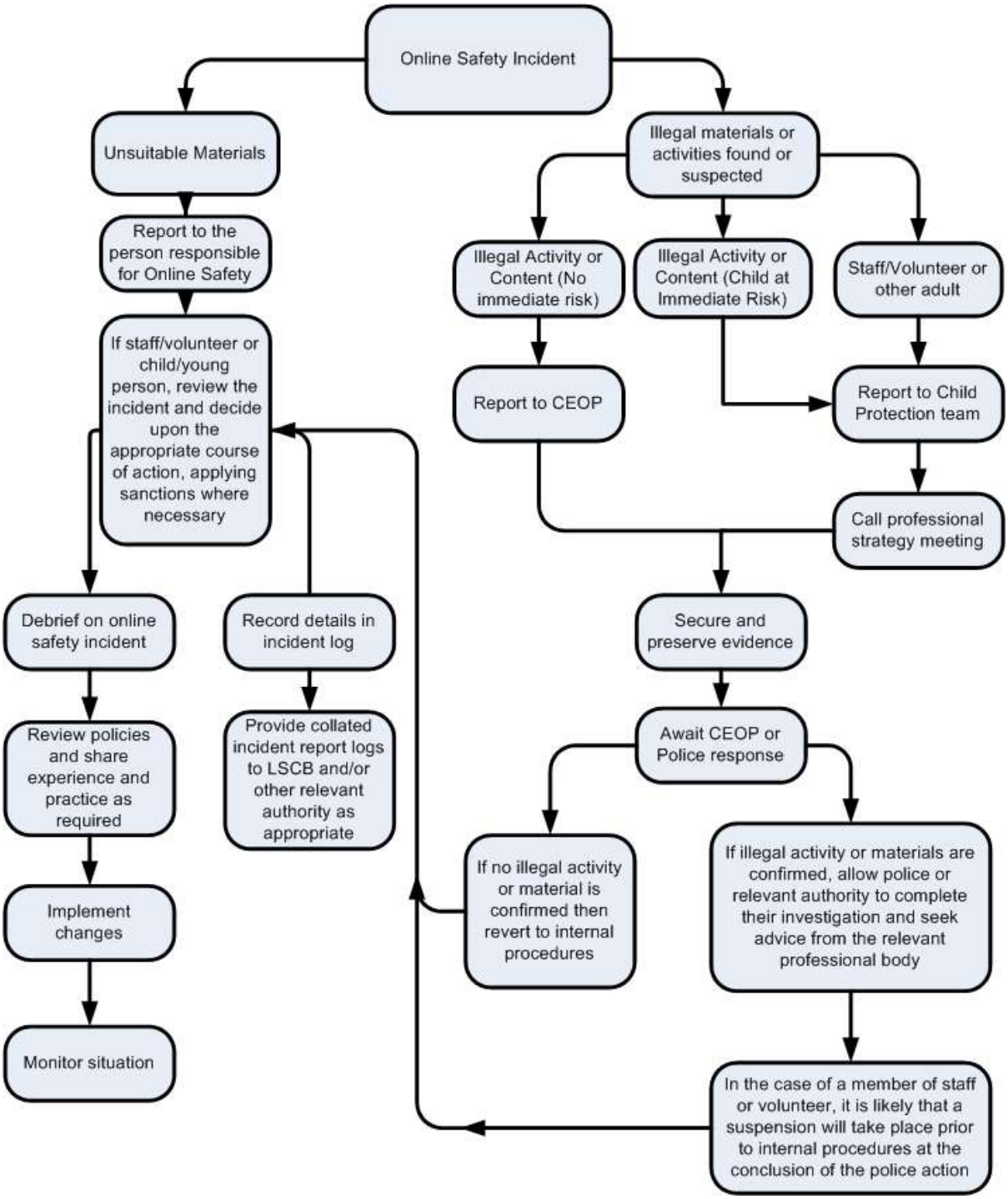
In the event that a child or young person **accidentally** accesses inappropriate materials the child should report this to an adult immediately and take appropriate action to hide the screen or close the window, so that an adult can take the appropriate action. Where a child or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice. The issue of a child or young person deliberately misusing online technologies should also be addressed by the establishment.

Children should be taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials to websites, for example, as this may have legal implications.

Responding to incidents of misuse – flow chart

Illegal Incidents

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



Other Incidents:

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

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

• Have more than one senior member of staff / 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.
• Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not.

<u>If it does then appropriate action will be required and could include the following</u>:

• 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 ESSENTIAL that all of the above steps are taken as they will provide an evidence trial for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes.

ICT Leader: Miss G Allen