Elm Tree Community Primary School
Elmers Wood Road
Tanhouse
Skelmersdale
WN8 6SA
Tel: 01695 50924
Email: admin@elmtree.lancs.sch.uk
Headteacher: Mr D Lamb

E-Safety Policy

Reviewed - November 2016

Development / Monitoring / Review of the policy

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

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

The school will deal with such incidents within the policy and policies and will, where known, inform parents / carers of incidents of inappropriate e-safety conduct that take place out of school.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and group within the 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 regular information about e-safety incidents and monitoring reports.

Headteacher

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

- **The Headteacher 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.** (See flow chart on dealing with e-safety incidents – included in a later section – “Responding to incidents of misuse and relevant Local Authority HR / other relevant body disciplinary procedures).

- The Headteacher are responsible for ensuring that the E-Safety Coordinator and other relevant staff received suitable training to enable them to carry out their e-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 e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Headteacher is responsible for ensuring that incidents and sanctions are managed in accordance with this policy.
- The Senior Leadership Team will received regular monitoring reports from the E-Safety Co-ordinator.
- The Headteacher is responsible if safety concerns regarding apps, websites and any programs are identified. They will make a judgement regarding this and should concerns remain, the school will contact the Safer Internet Centre via http://www.saferinternet.org or 08448002382 for further advice and act on this accordingly.

E-safety coordinator Mr M Taylor (Deputy Headteacher)

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents under the supervision of the Headteacher.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place. Mr Taylor must be informed.
- Coordinates training and advice for staff.
- Liaises with the Local Authority / relevant body.
- Liaises with the school technical staff.
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- Meets regularly with the Headteacher to discuss current issues, review incident logs and filtering / change control logs.

ICT Network Coordinator / ICT Technician

The ICT Network Coordinator / ICT technician is responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required e-safety technical requirements and any Local Authority / other relevant body E-Safety Policy / Guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection.
- The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- That the use of the network (including remote access), use of the internet and email Is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / E-Safety Coordinator for investigation / action / sanction.
- That monitoring software / systems are implemented and updated as agreed in school policies.

Teaching and Support staff

Teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
- They have read, understood and signed the Staff Internet and Email acceptable Use Policy
- They report any suspected misuse or problem to the Line Manager 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.
- E-Safety issues are embedded in all aspects of the curriculum and other activities.
- Students / pupils understand and follow the e-safety and acceptable use policies.
- Students / 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 students / 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 Senior Leader for Child Protection

The Designated Senior Person for child Protection 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

(NB: it is important to emphasise that these are child protection issues, not technical issues. Simply that the technology provides additional means for child protection issues to develop.)

Pupils / Students

Pupils and students:

- Are responsible for using the school digital technology systems in accordance with the Pupils / Student Internet and Email Acceptable Use Policy.
- Have an 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.
- Some will be expected to have an understanding of policies on the use of mobile devices and digital cameras. Some will also know and understand policies on taking / use of images and on cyber-bullying.

- Some will have an understanding of the importance of adopting good e-safety practice when suing digital technologies out of school and realis that the school's E-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 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

N.B. Pupils are not permitted to use personal devices in school

Education – pupils / students

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils / students to take a responsible approach. The education of pupils / students in e-safety is therefore an essential part of the schools 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 should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum is provided as part of Computing / PSHCE lessons and is taught discreetly for at least half a term every year where appropriate to the developmental level of the pupil.
- Key e-safety messages are reinforced as part of a planned programme of assemblies and tutorial / pastoral activities.
- Pupils / students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils / students are helped to understand the need for the Pupils / Students Internet and email Acceptable Use agreement and are encouraged to adopt safe and responsible use both within and outside school.
- Staff act as good role models in their use of digital technologies the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that pupils / students 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.
- **At no time do pupils / students have un-restricted access to the internet.** Where pupils / students are allowed to 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, pupils / students may need to research topics (e**.**g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can

request that the ICT Network Coordinator or ICT Technician temporarily remove those sites form the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

- It is accepted that from time to time, for good educational reasons pupils / students may need to access social networking websites (e.g. Facebook, Twitter, Instagram, Snapchat) that would normally result in internet searches being blocked. In such a situation, staff can request that the ICT Network Coordinator or ICT Technician can temporarily remove those sites/apps 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 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 conducts. 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 evening / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant websites / publications e.g. www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education & Training – Staff / Volunteers

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

- Formal e-safety training will be made available to staff when required. This will be regularly updated and reinforced.
- All new staff – including trainee teachers, will receive e-safety training as part of their induction programme, ensuring that they have read and signed they fully understand the Safer Internet Use Policy the school Internet and Email Acceptable Use Policy.
- The E-Safety Coordinator will receive regular updates through attendance at external training events 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 meetings / INSET days.
- The E-safety Coordinator will provide advice / guidance / training to individuals as required.

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school 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.
- All classes will be provided with a username and secure password by the ICT Network Coordinator / ICT Technician 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 network, used by the ICT Network Coordinator must also be available to the Headteacher and kept in a secure place (e.g. school safe).
- The ICT Network Coordinator is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband 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.
- The school has provided enhanced / differentiated user-level filtering.
- School technical staff regularly monitor and record that activity of users on the school technical systems and users are made aware of this in the Internet and Email Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed). Users will report breaches directly to the ICT Network Coordinator and 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.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupil's 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 cyber-bullying 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. 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 will 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 e.g. on social networking sites.

- In accordance with guidance from the Information Commissioner's office and our own school Child Protection Policy parents / carers are not permitted to take photographs and videos at community day events.
- 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 this will be included within the Consent Form signed by parents or carers at the start of the academic year.
- Student's / Pupil's work can only be published with the permission of the student / pupil and / or parents or carers.

Data Protection

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

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

The school ensures that:

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

- It has clear and understood arrangement for the security, storage and transfer of personal data.
- Data subjects have rights to access and there are clear procedures for this to be obtained.
- There are clear and understood policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from information risk incidents.
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties.
- There are clear policies about the use of cloud storage / cloud computing which ensures that the data storage meets the requirements laid down by the Information Commissioner's Office.

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 computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

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

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

Communications

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

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

- The official school email service may be regarded as safe and secure ad is monitored. Users should be aware that email communications are monitored. Staff and students / pupils should therefore use only the school, or on school systems (e.g. by remote access).
- Users must immediately report, to the nominated person – 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 students / pupils or parents / carers (email, chat etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems.

- Whole class / group email addresses, text messaging or social media must not be used for these communications.
- Whole class / group email addresses may be used across the school and pupils / students may be provided with individual school email addresses for educational use.
- Students / 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 suing digital technologies.
- Personal information should not be posted on the school website and only office email addresses should be used to identify members of staff.

Social media – Protecting Professional Identify

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies 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 risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk.

School staff should ensure that:

- No reference should be made in social media to students / 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 or local authority
- 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 for professional purposes will be checked regularly to ensure compliance with the Social Media Data Protection, Communications, Digital Image and Video Policies.

Unsuitable / inappropriate activities

Any activities e.g. distributing racist material is illegal and is obviously banned from school and all other technical systems, in addition the school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

ICT Acceptable Use Policy for Staff/Governors/Volunteer's

1. Introduction

As use of the internet by staff and volunteers becomes more widespread, for the protection of the organisation, young people and the staff and volunteers it is necessary to set out some guidelines for internet use. Staff and volunteers should read these guidelines carefully, in conjunction with the e-safety Policy. Abuse of the internet may lead to disciplinary action being taken.

The use of electronic communication and information retrieval is no more than the addition of another medium. **The same behavioural and professional standards are expected of staff and volunteers as are the case with traditional written communications, the telephone and face to face meetings.**

The internet as a resource is constantly changing. These guidelines will be updated in the light of experience and developments of the internet itself.

2. Acceptable Uses

As a general principle, internet access is provided to staff and volunteers to support work related activities. The following list is not intended to be a definitive list, but sets out broad areas of use that the organisation considers to be acceptable uses of the internet:

- To provide communication within the organisation via email or the organisation website
- To provide communication with other organisations for educational purposes
- To distribute electronic copies of the weekly newsletter
- To distribute details regarding organisation meetings
- To provide electronic methods of communication
- Any other use that directly supports work related functions.

3. Unacceptable Uses

The following uses will be regarded as not acceptable:

- Using the computer to perpetrate any form of fraud, or software, film or music piracy
- Use for racial, sexual, homophobic or other harassment.
- Use of non-educational games.
- To access pornographic, obscene or illegal material.
- To solicit personal information with the intent of using such information to cause harm.
- Entering into a commitment on behalf of the organisation (unless you have explicit permission to do this).
- Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence.
- Hacking into unauthorised areas.
- Publishing defamatory and/or knowingly false material about the organisation, your colleagues and/or our young people on social networking sites, 'blogs' (online journals), 'wikis' and any online publishing format.
- Revealing confidential information about the organisation in a personal online posting, upload or transmission - including financial information and

information relating to our young people, staff and/or internal discussions
- Use of personal email to communicate with or about any child
- Undertaking deliberate activities that waste staff effort or networked resources.
- Introducing any form of malicious software into the corporate network
- To disrupt the work of other users. This includes the propagation of computer viruses and use of the internet.
- Use of any Bit torrent systems
- Use for personal or private business purposes.

4. Netiquette

The following general principles should be adopted:

- Be polite. Do not be abusive in messages to others.
- Use appropriate language. Remember that you are a representative of the organisation and that you are using a non-private network.

5. Email

- Whenever e-mail is sent, it should be from an official work email address which includes the sender's name, job title and organisation's name.
- Every user is responsible for all mail originating from their user ID (e-mail address).
- Forgery or attempted forgery of electronic mail is prohibited.
- Attempts to read, delete, copy or modify the e-mail of other users are prohibited.
- Attempts to send junk mail and chain letters are prohibited. If you receive e-mail from outside the organisation that you consider to be offensive or harassing, speak to your line manager (harassing internal e-mail will be dealt with under the organisation's guidelines).
- You should be aware that, in the event of the organisation being involved in legal proceedings, any relevant e-mails (including internal e-mail) may have to be disclosed, on the same basis as is the case for written documents.
- Email should be accessed via organisation ICT equipment only, if you wish to use a personal device to download organisation emails, you must check with your line manager first. You will need to ensure that your device is secured by a password at all times, that this password is not shared with any other person and that all reasonable care is taken to prevent unauthorised access to confidential information.

6. Social Networking Sites

Social media applies to blogs, microblogs like Facebook, Twitter, Bebo, LinkedIn, videos, Snapchat, Instagram, social networks, discussion forums, wikis, and other personal webspace. This organisation permits the use of internet and social media on work premises, outside of work time, but only where it meets the following guidelines. This is usually outside normal working hours and must not interfere with your or others day-to-day duties. Personal access should not be in view of any young people, and you are reminded to log out or 'lock' the screen immediately upon leaving your mobile phone or PC, even if only for a short while.

- Do not "speak" for the organisation unless you have express permission to do so, this covers all comments relating to the organisation
- Protect yourself from identity theft
- If you can be linked to the organisation, act appropriately. This includes photos and status updates
- Remember that colleagues, prospective employers, parents and children may

see your online information

- The organisation policy is that you are not allowed to be 'friends' with young people with whom you work or have worked with in the past unless there are exceptional circumstances, e.g. child, sibling etc Please choose your 'friends' carefully, especially in light of the last above. Ensure your settings are on private and only you and YOUR friends can see them.
- If in doubt, please seek advice in organisation.

7. Disciplinary Action

Disciplinary action may be taken against staff and volunteers who contravene these guidelines, in accordance with the organisation's disciplinary procedures.

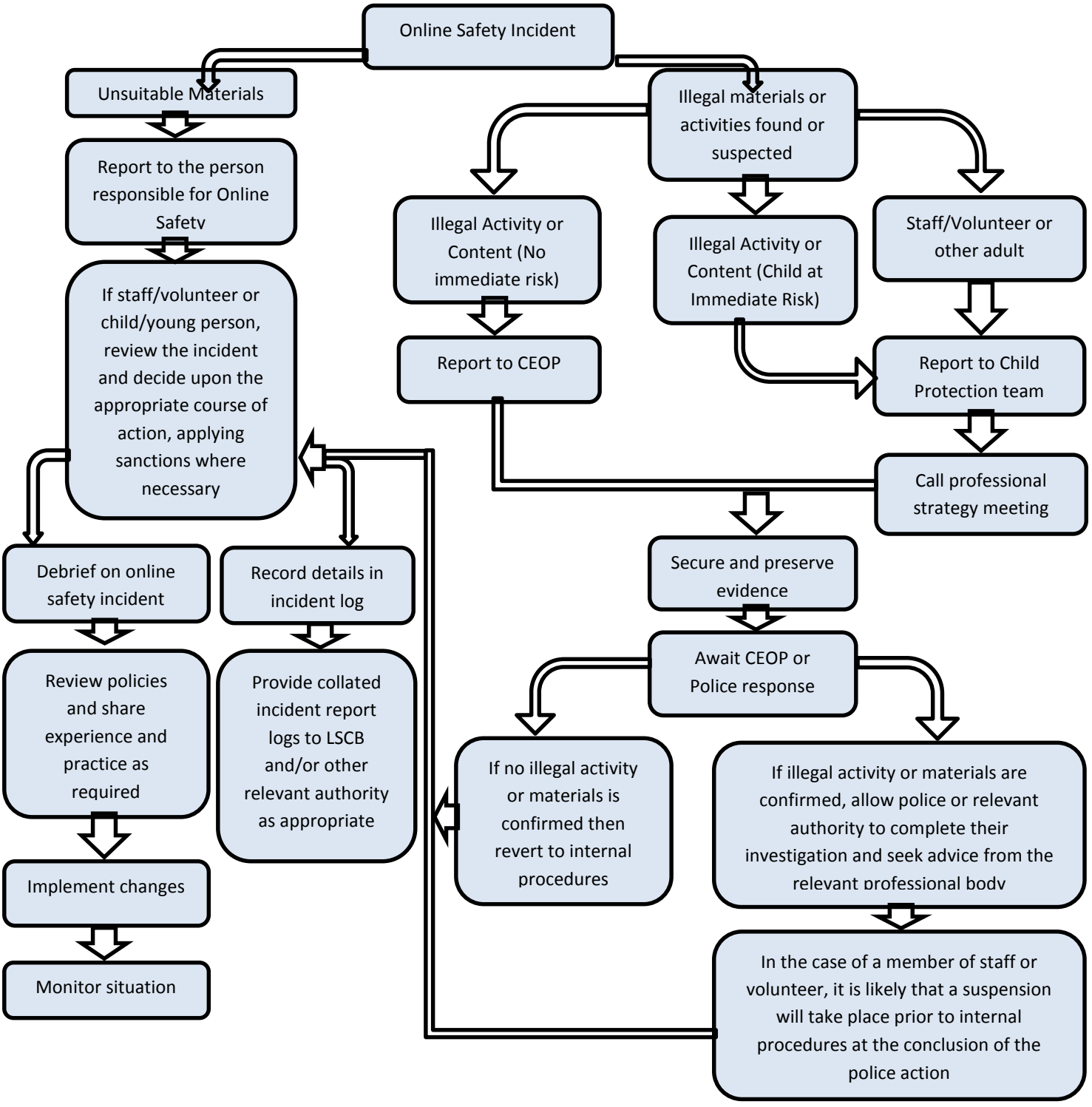
ICT Acceptable Use Policy for Children

These are the rules I agree to follow when using any digital technology:

- I will ask permission from a teacher before using ICT equipment and will use only my own login and password.
- To protect myself and other pupils, if I see anything I am unhappy with or receive messages I do not like, I will immediately close the page and tell a teacher or adult.
- I will not access other people's files or send pictures of anyone without their permission.
- I will not bring CDs or memory sticks into school unless I have permission and they have been checked to ensure that they are virus free.
- I will only e-mail people I know, or that my parent/teacher has approved and the messages I send will be polite and sensible.
- I will not give my home address or phone number, or arrange to meet someone I have met online. When I am using the internet to find information, I will check that the information is accurate as I understand that the work of others may not be truthful.
- Where work is protected by copyright, I will not try to download copies (including music and videos). I will not use my mobile phone in school for any reason.
- I understand that the school may check my computer files and may monitor the Internet sites I visit.
- If I am involved in incidents of inappropriate behaviour that involve members of the school community (e.g. cyber-bullying, using images/information without permission), the school will take action according the E-Safety Policy.
- I understand that if I do not follow these rules I may not be allowed to use ICT in school and my parents/carers may be contacted.

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, thorough 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 / governor 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’ conduct
    - 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 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. It is intended that incidents of misuse will be dealt with through normal conduct / disciplinary procedures as follows:

Pupil / Students **Actions / Sanctions**

Incidents:	Refer to class teacher	Refer to Head of Department / Head of Year	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internal access rights	warning	Further sanction.
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on suitable / inappropriate activities).		X	X	X	X	X	X		
Unauthorised use of non-educational sites during lessons	X				X			X	
Unauthorised use of mobile phone / digital camera / other mobile device		X						X	
Unauthorised use of social media / messaging apps / personal email		X			X			X	
Unauthorised downloading or uploading files		X			X	X		X	
Allowing others to access school network by sharing username and password **N/A**									
Attempting to access or accessing the school network, using another student's / pupil's account **N/A**									
Attempting to access or accessing the school network, using the account of a member of staff			X		X	X			X
Corrupting or destroying the data of other users			X		X	X	X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			X		X	X			X
Continues infringements of the above, following previous warnings or sanctions			X		X	X			X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			X		X	X	X		X
Using proxy sites or other means to subvert the school's filtering system			X		X	X	X		X
Accidentally accessing offensive or pornographic material and failing to report the incident			X		X	X	X	X	
Deliberately acceding or trying to access offensive or pornographic material			X		X	X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			X		X	X	X		X

Staff **Actions / Sanctions**

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on suitable / inappropriate activities).		X	X	X	X		X	X
Inappropriate personal use of the internet / social media / personal email	X				X	X		
Unauthorised downloading or uploading files	X				X	X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X				X	X		
Careless use of personal data e.g. holding or transferring data in an insecure manner		X			X	X		
Deliberate actions to breach data protection or network security rules		X	X		X			X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X		X		X	X
Sending an email, text or message that is regarded as offensive, harassment or of bullying nature		X	X		X			X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		X	X			X		X
Actions which could compromise the staff member' professional standing		X	X			X		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X	X					X
Using proxy sites or other means to subvert the school's filtering system		X	X					X
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X					X
Deliberately accessing or trying to access offensive or pornographic material		X	X				X	
Breaching copyright or licensing regulations		X	X	X			X	
Continued infringements of the above, following previous warnings or sanctions		X	X				X	