



## **E-safety (NON-STATUTORY)**

Review Date:	Reviewed by:	Amended?	Ratified:
Policy Week 2-6 October 2017			

<p><b>Other Information:</b> Links to the following policies: - Safeguarding - Allegations of abuse against staff</p>	
---	--

## Scope of the Policy

This SOP applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school. The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place outside 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. Ladybridge will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

## Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups at Ladybridge Primary 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 Sub Committee receiving 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 is combined with that of the Child Protection / Safeguarding Governor).

The role of the E-Safety Governor will include:

- Meetings with the Computing Team
- Monitoring of e-safety incident logs
- Monitoring of filtering / change control logs

### Headteacher and Senior Leaders:

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 Computing Team. 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 is responsible for ensuring that the Computing Team 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 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.

### Computing Team:

- leads the e-safety committee
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- provides training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- meets regularly with the E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meetings

### Network Manager / Technical staff:

- 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 policy, in which passwords are regularly changed
- the filtering policy (if it has one), 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 / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies

## **Teaching and Support Staff are responsible for ensuring that:**

- they have an up to date awareness of 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 / Deputy Headteacher for investigation / action / sanction
- e-safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the e-safety 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 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

(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:**

- 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.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that schools 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. Ladybridge will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns /

literature. Parents and carers will be encouraged to support 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

## Community Users

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

## 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 e-safety is therefore 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 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 should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned programme of assemblies / pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

## Education – 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 the children's on-line behaviours. Parents may underestimate how often children come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, web site
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. [www.swgfl.org.uk](http://www.swgfl.org.uk) [www.saferinternet.org.uk/](http://www.saferinternet.org.uk/)  
<http://www.childnet.com/parents-and-carers>

## 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 planned programme of formal e-safety training 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 regularly

- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / key stage meetings / INSET days.
- The Computing Team will provide advice / guidance / training to individuals as required.

## Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any subcommittee 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 or parents (this may include attendance at assemblies / lessons).

## Technical – infrastructure / equipment, filtering and monitoring

- 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 users will be provided with a username and secure password by BOLTON SICT, Miss Cooper will then 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 system, used by the Network Manager must also be available to the Headteacher/Deputy Headteacher and kept in a secure place.

The computing team 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 (Inadequate licensing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs). Licences are kept: \\pri018dcfw\softwareinstalls, older licences are in the licence folder in the Computing Suite.

Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list.

An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed). 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.

The school has provided enhanced / differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users – staff / pupils / students etc.)

## Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring. This list is not exhaustive and a BYOD policy should be in place and reference made within all relevant policies.

- The school has a set of clear expectations and responsibilities for all users
- The school adheres to the Data Protection Act principles
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated

- Where possible these devices will be covered by the school's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Mandatory training is undertaken for all staff
- Pupils receive training and guidance on the use of personal devices
- Regular audits and monitoring of usage will take place to ensure compliance
- Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy
- Any user leaving the school will follow the process outlined within the BYOD policy

## Use of 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 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. 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.
- 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 is 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 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 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 pupils are published on the school website.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

## Data Protection

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

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

### Ladybridge must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of 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 ensure that such 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 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.

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
- 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

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 and pupils should therefore use only the school email service to communicate with others when in school, or on school systems.*
- **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 pupils or parents / carers (email, chat, VLE etc) 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.*
- *Whole class / group email addresses may be used at KS1, while pupils at KS2 and above will be provided with individual school / academy email addresses for educational use.*
- *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.*

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:

	Staff and other adults			Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission
<b>Communication Technologies</b>							
Mobile phones may be brought to school	✓					✓	
Use of mobile phones in lessons		✓		✓			
Use of mobile phones in social time	✓			✓			
Taking photos on mobile phones / cameras		✓			✓	✓	
Use of other mobile devices eg tablets, gaming devices					✓	✓	
Use of personal email addresses in school, or on school network		✓		✓			
Use of school email for personal emails							
Use of messaging apps							
Use of social media	✓						
Use of blogs	✓						

## Social Media - Protecting Professional Identity

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, cyber bully, 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 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.

## Unsuitable / inappropriate activities

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:

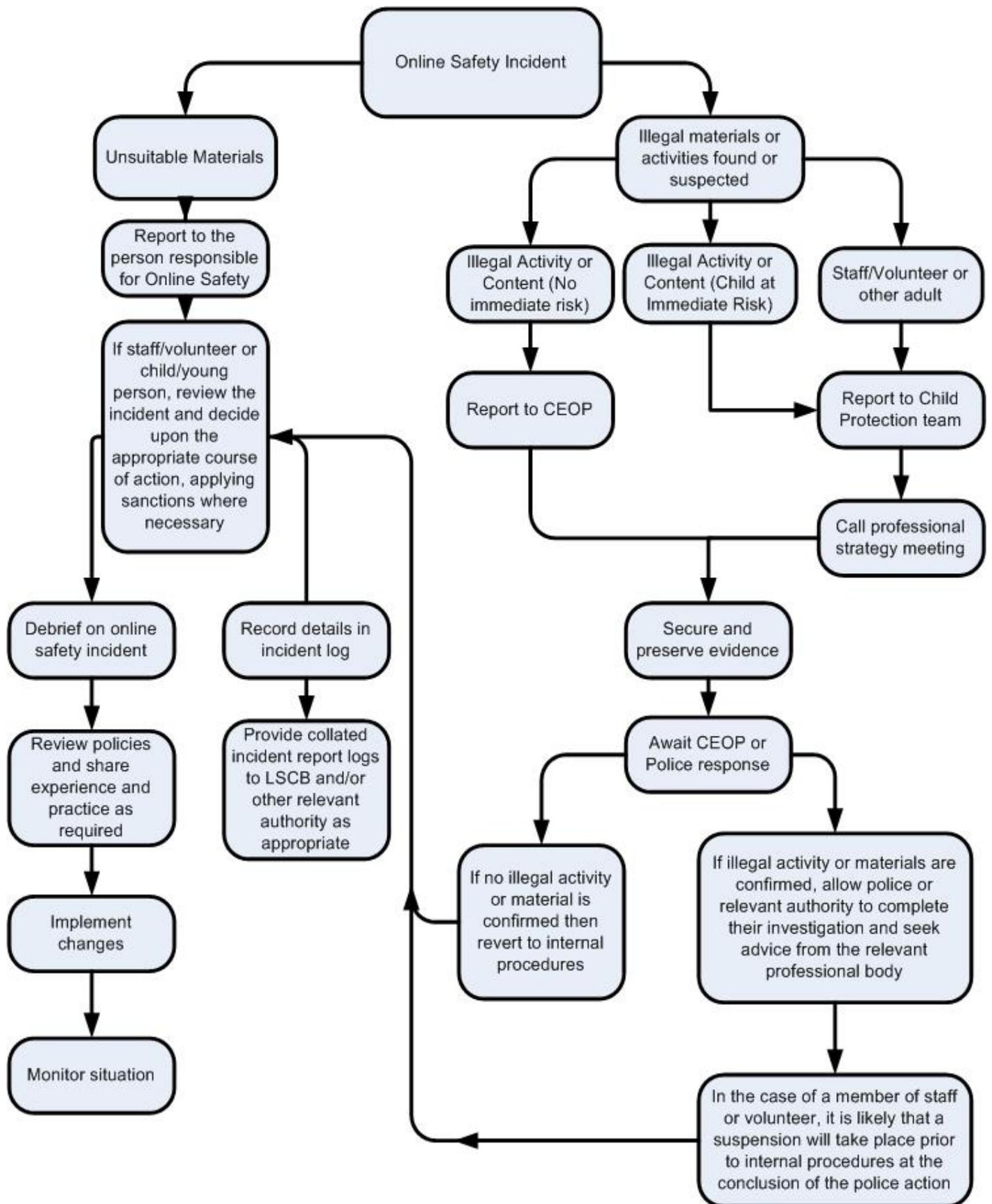
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	

## Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above)

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

It is important that all of the above steps are taken as they will provide an evidence trail for the school 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 and 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 behaviour / disciplinary procedures.

# Appendices

Can be found on the following pages:

- Pupil Acceptable Use Agreement template (Key Stage Two)
- Pupil Acceptable Use Agreement template (EYFS/Key Stage One)
- Parents / Carers Acceptable Use Agreement template
- Staff and Volunteers Acceptable Use Agreement Policy template
- Community Users Acceptable Use Agreement template
- Responding to incidents of misuse – flowchart
- Record of reviewing sites (for internet misuse)
- School Reporting Log template
- School Training Needs Audit template
- Glossary of terms

**Acceptable Use Policy - Year 5 and Year 6 Pupils**

 My Learning	<ul style="list-style-type: none"> <li>• I will use school devices (PCs, laptops, tablets/ ipads) for my learning.</li> <li>• I will ask a teacher before using a device and ask for help if I can't work the device.</li> <li>• I will only use activities that a teacher has told or allowed me to use.</li> <li>• I will ask a teacher if I am not sure what to do or I think I have done something wrong.</li> <li>• I will look after the school's computing equipment and tell a teacher if something is broken or not working properly.</li> <li>• When logging on using my own username and password, I will keep it safe and secret.</li> <li>• I will save only school work on the school computer and will check with my teacher before printing.</li> <li>• I will log off or shut down a computer when I have finished using it.</li> </ul>
 Using the Internet @school	<ul style="list-style-type: none"> <li>• I will only visit sites that are appropriate to my learning at the time</li> </ul> <p><b>My School Accounts</b></p> <ul style="list-style-type: none"> <li>• I will keep my username and password safe and secure - I will not share it.</li> <li>• I will not try to use any other person's username and password.</li> <li>• I understand that I should not write down or store a password where it is possible that someone may steal it.</li> </ul> <p><b>My role as a Digital Citizen.</b></p> <ul style="list-style-type: none"> <li>• I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online to a trusted adult.</li> <li>• I will respect other people's work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.</li> <li>• I will not take or distribute images of anyone without their permission.</li> </ul>
 Using the Internet @home	<ul style="list-style-type: none"> <li>• I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, school details)</li> <li>• I will not arrange to meet people off-line that I have communicated with on-line.</li> <li>• I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line, to a trusted adult or online agencies e.g.: CEOP, Childnet, Childline, Barnardos.</li> </ul> <p><b>My Communications (Including texting and messaging)</b></p> <ul style="list-style-type: none"> <li>• I will be aware of "stranger danger", when I am communicating online.</li> <li>• I will be polite and responsible when I communicate with others.</li> <li>• I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions</li> <li>• I will not take or distribute an image of anyone without their permission.</li> </ul> <p><b>My use of Social Media and Gaming</b></p> <ul style="list-style-type: none"> <li>• I understand that certain sites and games have age restrictions to keep me safe.</li> <li>• I understand that by accessing such sites and games, I maybe putting myself at risk of accessing inappropriate content and cyberbullying.</li> </ul>

I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).

I understand that these rules, help me to stay safe and I agree to follow them.

I also understand that if I break the rules I might not be allowed to use school computing equipment.

My parents/carers understand that keeping me safe on the internet at home is their responsibility.

---

**Child's Signature**

---

**Date**

**Acceptable Use Policy - Year 3 and Year 4 Pupils**

 <p>My Learning</p>	<ul style="list-style-type: none"> <li>• I will use school devices (PCs, laptops, tablets/ iPads) for my learning.</li> <li>• I will ask a teacher before using a device and ask for help if I can't work the device.</li> <li>• I will only use activities that a teacher has told or allowed me to use.</li> <li>• I will ask a teacher if I am not sure what to do or I think I have done something wrong.</li> <li>• I will look after the school's computing equipment and tell a teacher if something is broken or not working properly.</li> <li>• When logging on using my own username and password, I will keep it safe and secret.</li> <li>• I will save only school work on the school computer and will check with my teacher before printing.</li> <li>• I will log off or shut down a computer when I have finished using it</li> </ul>
 <p>Using the Internet @school</p>	<ul style="list-style-type: none"> <li>• I will only visit sites that are appropriate to my learning at the time</li> </ul> <p><b>My School Accounts</b></p> <ul style="list-style-type: none"> <li>• I will keep my username and password safe and secure - I will not share it.</li> <li>• I will not try to use any other person's username and password.</li> <li>• I understand that I should not write down or store a password where it is possible that someone may use it.</li> </ul> <p><b>My role as a Digital Citizen.</b></p> <ul style="list-style-type: none"> <li>• I will report any inappropriate material or messages or anything that makes me feel uncomfortable when I see it online to a trusted adult.</li> <li>• I will respect other people's work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.</li> </ul>
 <p>Using the Internet @home</p>	<ul style="list-style-type: none"> <li>• I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, school details)</li> <li>• I will immediately report any inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line, to a trusted adult or online agencies e.g.: CEOP, Childnet, Childline, Barnardos</li> </ul> <p><b>My Communications</b></p> <ul style="list-style-type: none"> <li>• I will be aware of the "SMART" rules, when I am communicating online.</li> <li>• I will be polite and responsible when I communicate with others.</li> <li>• I will not use inappropriate language and I understand that others may have different opinions.</li> </ul> <p><b>My use of Social Media and Gaming</b></p> <ul style="list-style-type: none"> <li>• I understand that certain sites and games have age restrictions to keep me safe.</li> <li>• I understand that by accessing such sites and games, I may be putting myself at risk of accessing inappropriate content and cyberbullying.</li> </ul>

I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).

I understand that these rules help me to stay safe and I agree to follow them.

I also understand that if I break the rules I might not be allowed to use school computing equipment.

My parents/carers understand that keeping me safe on the internet at home is their responsibility.

---

**Child's Signature**

---

**Date**

## Acceptable Use Policy - Year 1 and Year 2

 My Learning	<ul style="list-style-type: none"> <li>• I will use school devices (PCs, laptops, tablets/ ipads) for my learning.</li> <li>• I will ask a teacher before using a device and ask for help if I can't work the device.</li> <li>• I will only use activities that a teacher has told or allowed me to use.</li> <li>• I will ask a teacher if I am not sure what to do or I think I have done something wrong.</li> <li>• I will look after the school's computing equipment and tell a teacher if something is broken or not working properly.</li> </ul>
 My Online Safety	<ul style="list-style-type: none"> <li>• I will always use what I have learned about Online Safety to keep myself safe.</li> <li>• I will tell a teacher if I see something that upsets me on the screen.</li> </ul>
 Using the Internet @school	<ul style="list-style-type: none"> <li>• I will only use the internet when the teacher says I can.</li> <li>• I will only go on websites that my teacher allows me to.</li> <li>• I will tell my teacher if I go on a website by mistake.</li> </ul>
 Using the Internet @home	<ul style="list-style-type: none"> <li>• I will not share personal information about myself when on-line (names, addresses, telephone numbers, age, gender, school details)</li> <li>• Where I have my own username and password, I will keep it safe and secret.</li> <li>• I will tell a trusted adult if I see something that upsets me on the screen.</li> </ul> <p><b>My use of Social Media and Gaming</b></p> <ul style="list-style-type: none"> <li>• I understand that certain sites and games have age restrictions to keep me safe.</li> <li>• I understand that by accessing such sites and games, I maybe putting myself at risk of accessing inappropriate content and cyberbullying.</li> </ul>

I understand that these rules help me to stay safe and I agree to follow them.  
 I also understand that if I break the rules I might not be allowed to use the school's computing equipment.

I understand that these rules, help me to stay safe and I agree to follow them.  
 I also understand that if I break the rules I might not be allowed to use school computing equipment.

---

**Child's Signature**

---

**Date**

## Acceptable Use Policy - EYFS

 <p>My Learning</p>	<ul style="list-style-type: none"> <li>• I will use school devices (PCs, laptops, tablets/ ipads) for my learning.</li> <li>• I will ask a teacher before using a device and ask for help if I can't work the device.</li> <li>• I will only use activities that a teacher has told or allowed me to use.</li> <li>• I will ask a teacher if I am not sure what to do or I think I have done something wrong.</li> <li>• I will look after the school's computing equipment and tell a teacher if something is broken or not working properly.</li> </ul>
 <p>My Online Safety</p>	<ul style="list-style-type: none"> <li>• I will always use what I have learned about Online Safety to keep myself safe.</li> <li>• I will tell a teacher if I see something that upsets me on the screen.</li> </ul>
 <p>Using the Internet @school</p>	<ul style="list-style-type: none"> <li>• I will only use the internet when the teacher says I can.</li> <li>• I will only go on websites that my teacher allows me to.</li> <li>• I will tell my teacher if I go on a website by mistake.</li> </ul>
 <p>Using the Internet @home</p>	<ul style="list-style-type: none"> <li>• I will tell a trusted adult if I see something that upsets me on the screen.</li> </ul>

I understand that these rules help me to stay safe and I agree to follow them.  
 I also understand that if I break the rules I might not be allowed to use the school's computing equipment.

---

**Child's Signature**

---

**Date**

## Parent / Carer Acceptable Use Agreement

Parent / Carers Name

Pupil Name

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

### **This Acceptable Use Statement of Practice is intended to ensure:**

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

Ladybridge will ensure that pupils have access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

- As the parent / carer of the above pupil/s, I give permission for my son / daughter to have access to the internet and to ICT systems at school.
- I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.
- I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
- I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Agreement.
- I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Signed

Date

## Parent / Carer Use of Digital / Video Images

Parent / Carers Name

Pupil Name

The use of digital / video images play an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons. Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media.

The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

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 is 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 pupils in the digital / video images.

Parents / carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents / carers to agree

As the parent / carer of the above pupil, I agree to the school taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

Yes / No

I agree that if I take digital or video images at, or of, – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Yes / No

Signed

Date

# **Staff (and Volunteer) Acceptable Use Agreement**

## **School SOP**

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

### **This Acceptable Use SOP is intended to ensure:**

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school ensure that staff and volunteers have good access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

## **Acceptable Use SOP Agreement**

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

### **For my professional and personal safety:**

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, VLE etc) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident; I become aware of, to the appropriate person.

### **I will be professional in my communications and actions when using school ICT systems:**

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

### **The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:**

- When I use my mobile devices (laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses

- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data, to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

**When using the internet in my professional capacity or for school sanctioned personal use:**

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

**I understand that I am responsible for my actions in and out of the school:**

- I understand that this Acceptable Use SOP applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use SOP Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date

## Acceptable Use Agreement for Community Users

### **This Acceptable Use Agreement is intended to ensure:**

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential risk in their use of these systems and devices

### **Acceptable Use Agreement**

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school

- I understand that my use of school systems and devices and digital communications will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident; I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school systems / devices

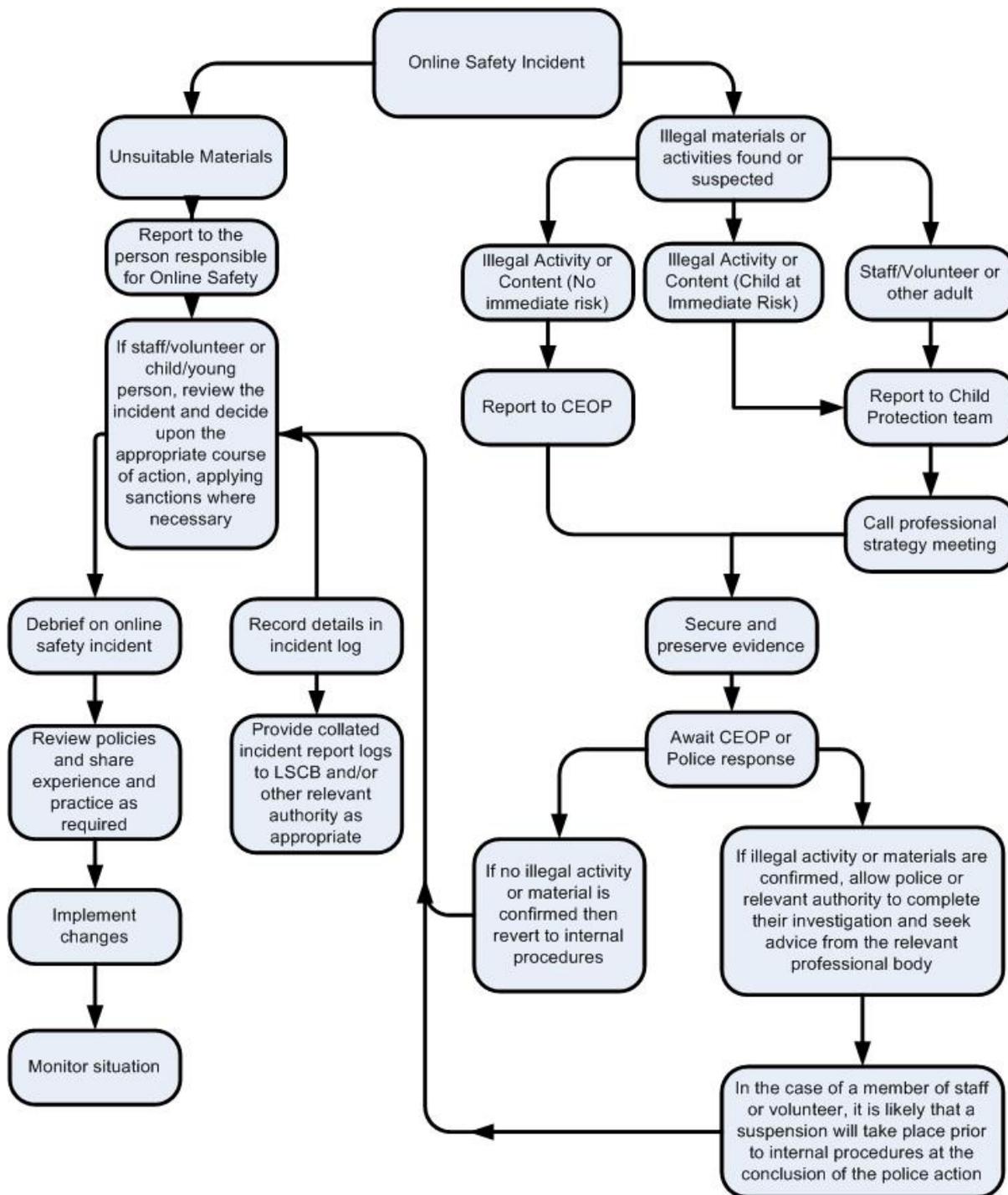
I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name

Signed

Date

## Responding to incidents of misuse – flow chart



**Record of reviewing devices / internet sites (responding to incidents of misuse)**

Group	
Date	
Reason for investigation	

**Details of first reviewing person**

Name	
Position	
Signature	

**Details of second reviewing person**

Name	
Position	
Signature	

**Name and location of computer used for review (for web sites)**

--

**Web site(s) address / device                      Reason for concern**

Web site(s) address / device	Reason for concern

**Conclusion and Action proposed or taken**






## **Glossary of terms**

AUP	Acceptable Use Policy – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes).
CPC	Child Protection Committee
CPD	Continuous Professional Development
FOSI	Family Online Safety Institute
EA	Education Authority
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICT Mark	Quality standard for schools provided by NAACE
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers’ Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
TUK	Think U Know – educational e-safety programmes for schools, young people and parents.
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol