ULEY C OF E PRIMARY SCHOOL

ONLINE POLICY

Our School Vision

Live – Learn – Flourish

- Live: at home, in school, and in our local community

- Learn: about self, others, and our ever-changing world

- Flourish: be the best we can be in all that we do

Our School Mission

- We give all – pupils and staff – the opportunities and encouragement to be the best that they can be

- We create an environment that has the right balance of challenge and support

- We deliver a curriculum that is right for our school, inspiring and motivating all, and embracing new ideas

- We apply our core Christian Values of Trust, Friendship, Compassion and Wisdom in all that we do

- We develop strong and effective partnerships between pupils, staff, governors, parents and the wider community

- We strive to ensure that all flourish within a moral framework built on Christian values and the Diocesan vision "I have come that they may have LIFE, and have it to the full". (John 10:10)

ETHOS STATEMENT

We believe that everyone should be given the opportunity and encouragement to be the best that they can be. To this end, we strive to create the right environment, deliver the right content, and embrace new ideas. We apply our school values of trust, friendship, compassion and wisdom to enable every individual to flourish within a moral framework built on Christian values. We believe that this can only be achieved by developing partnerships between pupils, staff, governors, parents and the wider community.

Development / Monitoring / Review of this Policy

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

- *Head Teacher*
- *Designated Safeguard Leads*
  - *Health and Wellbeing team*
- *Staff – including Teachers, Support Staff, Technical staff*
- *Governors*
- *Parents and Carers*

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

Schedule for Development / Monitoring / Review

This online policy was approved by the *Governors Sub Committee on:*	
The implementation of this online policy will be monitored by the:	*Head Teacher and Safeguarding Lead Teacher in Charge Safeguarding Leads* IT Leader Chair of Governors Safeguarding Governor
Monitoring will take place at regular intervals:	*Annually in the Autumn*
The *Governors Sub Committee* will receive a report on the implementation of the online policy generated by the monitoring group (which will include anonymous details of online incidents) at regular intervals:	*Three times a year at a Safeguarding meeting and reported to full governor.*
The Online Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online or incidents that have taken place. The next anticipated review date will be:	*Autumn 19*
Should serious online incidents take place, the following external persons / agencies should be informed:	*LA Safeguarding Officer, Police, other children's service*

The school will monitor the impact of the policy using:

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

Spring 2   3

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Head Tteachers 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 online incidents covered by this policy, which may take place outside of the school, but is 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. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

Uley Primary School 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 online behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online roles and responsibilities of individuals and groups within the *school*:

Governors:

Governors are responsible for the approval of the Online Policy and for reviewing the effectiveness of the policy. This will be carried out by the Curriculum and Standards Committee receiving regular information about online incidents and monitoring reports. A member of the Governing Body has taken on the role of Safeguarding Governor which includes online. The role of the Online Governor will include:

- regular meetings with the Online Co-ordinator / Officer
- regular monitoring of online incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governor's meeting

Head Teacher / Principal and Senior Leaders:

- **The Head Teacher has a duty of care for ensuring the safety (including online) of members of the school community**, though the day to day responsibility for online will be delegated to the *Online Subject Leader/Head Teacher.*

- **The Head Teacher and (at least) another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious online allegation being made against a member of staff.**

- The Head Teacher and Senior Leaders are responsible for ensuring that the Online Leader and other relevant staff receive suitable training to enable them to carry out their online roles and to train other colleagues, as relevant.

- The Head Teacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles*.*

- Regular monitoring reports will be reported and held on file.

The Online Safety Lead:

- leads the online within school
- takes day to day responsibility for online issues and has a leading role in establishing and reviewing the school online policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online incident taking place.
- provides training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with school technical staff
- receives reports of online incidents and creates a log of incidents to inform future online developments,

- meets regularly with the Safeguarding Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meetings with a committee of Governors
- reports regularly to Senior Leadership Team/Safeguarding Leads

Technical staff:

The Technical Staff 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 online technical requirements 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**
- that they keep up to date with online technical information in order to effectively carry out their online 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 Head Teacher / Senior Leader for investigation / action / sanction
- that monitoring software and systems are implemented and updated as agreed in the school's policies

Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that:

- **they have an up to date awareness of online matters and of the current school's online policy and practices**
- **they have read, understood and signed the Staff Acceptable Use Policy (AUP)**
- **they report any suspected misuse or problem to the Head Teacher / Senior Leader / Safeguarding Leads for investigation / action / sanction**
- **all digital communications with students / pupils / parents / carers should be on a professional level** and only carried out using official school systems
- online issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the online and acceptable use policies
- pupils, where appropriate, 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

Safeguarding Lead

The Safeguarding Leads should be trained in online 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

Students / pupils:

- **are responsible for using the school's digital technology systems in accordance with the Pupil Acceptable Use Policy (AUP) – KS2 or Foundation/KS1 as applicable**

- 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 online practice when using digital technologies out of school and realise that the school's Online Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local online campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online 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 and on-line communication
- their children's personal devices in the school / academy (where this is allowed)

Community Users

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

Policy Statements

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online is therefore an essential part of the school's online provision. Children and young people need the help and support of the school to recognise and avoid online risks and build their resilience.

Online should be a focus in all areas of the curriculum and staff should reinforce online messages across the curriculum. The online curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:
- **A planned online curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited**
- **Key online messages should be reinforced as part of a planned programme of assemblies and class 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 supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.**
- Pupils should be helped to understand the need for the pupil Acceptable Use Policy 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
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need

Education – parents / carers

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

The school will therefore seek to provide information and awareness to parents and carers through:
- Curriculum activities
- Letters, newsletters, website,
- Parents / Carers evenings / sessions
- High profile events / campaigns eg Safer Internet Day
- Reference to the relevant websites / publications eg www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education – The Wider Community

Uley School will provide opportunities for members of the community to gain from the school's online knowledge and experience. This may be offered through the following:
- Providing families with information in the use of new digital technologies, digital literacy and online
- Online messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online information for the wider community

Education & Training – Staff / Volunteers

It is essential that all staff receive online training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:
- **A planned programme of formal online training (using 360 Boost) will be made available to staff. This will be regularly updated and reinforced. An audit of the online training needs of all staff will be carried out regularly.**
- **All new staff should receive online training as part of their induction programme, ensuring that they fully understand the school online policy and Acceptable Use Policies.**
- The Online Lead will receive regular updates through attendance at training events and by reviewing guidance documents released by relevant organisations.
- This Online policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.
- The Online Lead (Health and wellbeing team) will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in online training / awareness sessions, with particular importance for those who are members of any sub committee / 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 (eg SWGfL).
- Participation in school training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online responsibilities:

- **The school's 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 the school's 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** (at KS2 and above) **will be provided with a username and secure password. An up to date record will be kept of users and their usernames.**
- **The administrator passwords for the school's ICT system, used by the Network Manager (or other person) must also be available to the Head Teacher or other nominated senior leader and kept in a secure place**
- **The Head Teacher 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 or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
- **Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.**
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Policy.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agree.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place regarding the extent of personal use that users (staff / pupils / community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Mobile Technologies (including BYOD/BYOT)

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

All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme.

- **The school Acceptable Use Agreements for staff, pupils/students and parents / carers will give consideration to the use of mobile technologies**
- **The school allows:**

	School Devices	Personal Devices

	School owned for single user	School owned for multiple users	Authorised device[1]	Student owned	Staff owned	Visitor owned
Allowed in school	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*
Internet only				*No*	*Yes*	*No*
No network access						

Personal laptop devices

- Teaching staff are provided with a small laptop to use to support their work, planning and remote learning.
- Staff have responsibility to use their devices in an appropriate manner for education purposes only and need to follow the Acceptable user policy.

Smart Watches and Mobile Phones
Although we encourage children to wear watches in school to be able to tell the time, children are encouraged not to wear a 'smart' watch, or any watch that has the same functionality as a mobile phone or PC, on the school site, this includes before and after school club. This is a child protection requirement of the school and is for the safety and well-being of the school community.

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 cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- **When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.**
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at Uley C of E School events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other *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 or volunteers 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*

---

[1] Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

- *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 – see Use of Digital Images/Video Policy.*

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school must ensure that:

- **It has a Data Protection Policy.**
- **It has paid the appropriate fee to the Information Commissioner's Office (ICO).**
- **It has appointed a Data Protection Officer (DPO).**
- **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.**
- **Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.**
- **The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice.**
- **Where special category data is processed, a lawful basis and a separate condition for processing have been identified.**
- **Data Protection Impact Assessments (DPIA) are carried out.**
- **It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.**
- **Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.**
- **There are clear and understood data retention policies and routines for the deletion and disposal of data.**
- **There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.**
- **Consideration has been given to the protection of personal data when accessed using any remote access solutions.**
- **All schools must have a Freedom of Information Policy which sets out how it will deal with FOI requests.**
- **All staff receive data handling awareness / data protection training and are made aware of their responsibilities.**

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**
- **can recognise a possible breach, understand the need for urgency and know who to report it to within the school**
- **can help data subjects understands their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school**
- **where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected.**
- **will not transfer any school/academy personal data to personal devices except as in line with school policy**
- **access personal data sources and records 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**

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 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:

Communication Technologies	Staff & other adults				Students / Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	x						x	
Use of mobile phones in lessons		x						x
Use of mobile phones in social time	x							x
Taking photos on mobile phones / cameras				x				x
Use of other mobile devices eg tablets, gaming devices				x				x
Use of personal email addresses in school, or on school network				x				x
Use of school email for personal emails				x				x

Use of messaging apps			x				x
Use of social media		x					x
Use of blogs	x					x	

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 students / pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg 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 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. Personal email addresses, text messaging or social media must not be used for these communications.*
- *Pupils should be taught about online issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.*
- *Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.*

Social Media - Protecting Professional Identity

All schools, 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 / academy 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:

- Ensuring that personal information is not published
- 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.

When official school social media accounts are established there should be:

- *A process for approval by senior leaders*
- *Clear processes for the administration and monitoring of these accounts – involving at least two members of staff*
- *A code of behaviour for users of the accounts, including*
- *Systems for reporting and dealing with abuse and misuse*
- *Understanding of how incidents may be dealt with under school disciplinary procedures*

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- *The school permits reasonable and appropriate access to private social media sites*

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

The school's use of social media for professional purposes will be checked regularly by the Headteacher to ensure compliance with the school policies.

Unsuitable / inappropriate activities

Uley C of E Sschool 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:
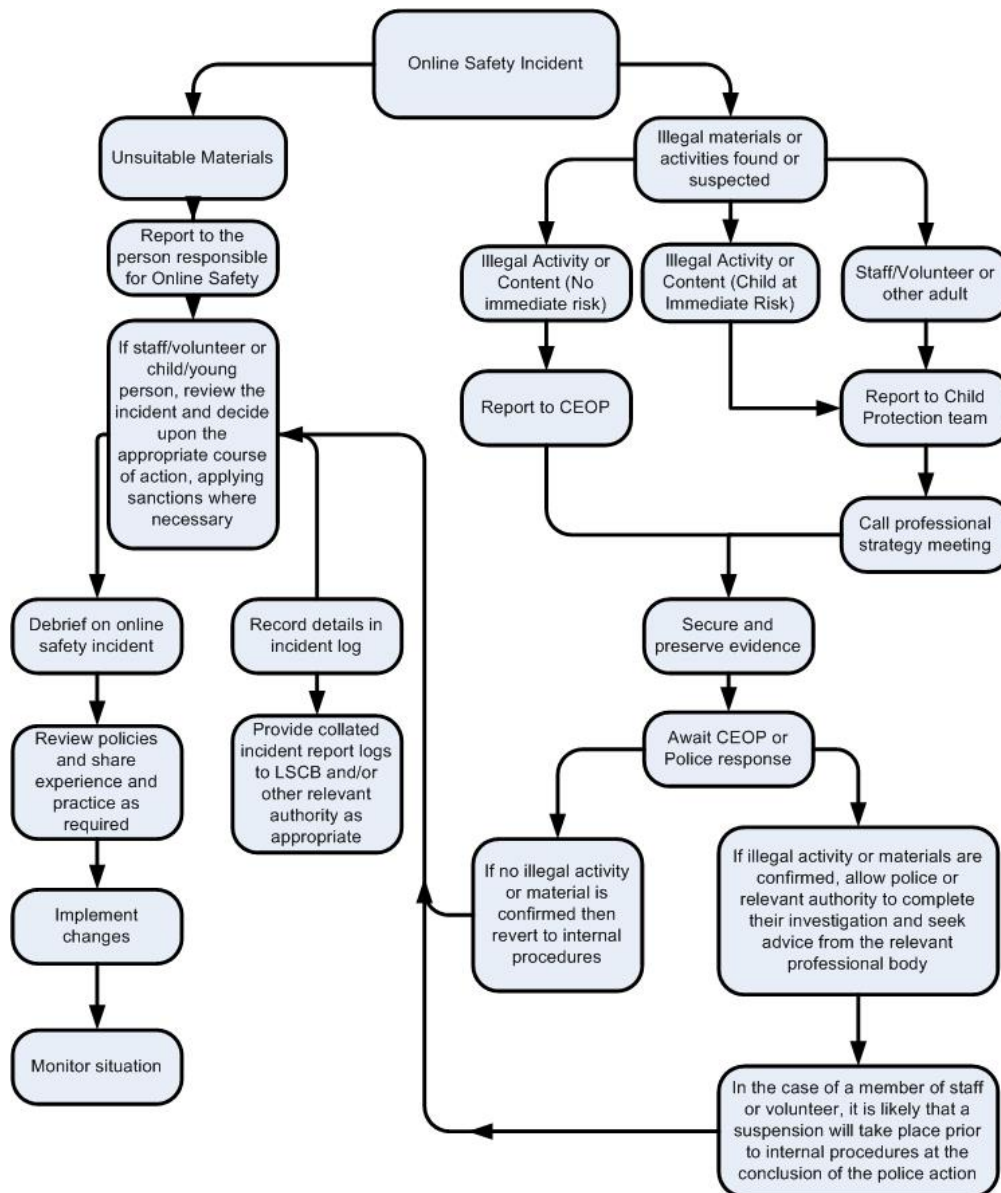
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child 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
On-line gaming (educational)		X	X		
On-line gaming (non educational)				X	
On-line gambling					X
On-line shopping / commerce			X		
File sharing		X			
Use of social media		X			
Use of messaging apps				x	
Use of video broadcasting eg Youtube				x	

Responding to incidents of misuse

Illegal Incidents

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

Online Safety Incident

Unsuitable Materials
→ Report to the person responsible for Online Safety
→ If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
→ Debrief on online safety incident
→ Review policies and share experience and practice as required
→ Implement changes
→ Monitor situation

Record details in incident log
→ Provide collated incident report logs to LSCB and/or other relevant authority as appropriate

Illegal materials or activities found or suspected

Illegal Activity or Content (No immediate risk)
→ Report to CEOP

Illegal Activity or Content (Child at Immediate Risk)
→ Report to Child Protection team

Staff/Volunteer or other adult
→ Report to Child Protection team
→ Call professional strategy meeting

Secure and preserve evidence
→ Await CEOP or Police response

If no illegal activity or material is confirmed then revert to internal procedures

If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
→ In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Other Incidents

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

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

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).

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

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

Students / Pupils — Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Head Teacher / Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X		X	X		
Unauthorised use of non-educational sites during lessons			x	X		X	x		
Unauthorised use of mobile phone / digital camera / other mobile device			x			X	x	X	
Unauthorised use of social media / messaging apps / personal email			X			X	x	x	
Unauthorised downloading or uploading of files			x			X	X		
Allowing others to access school / academy network by sharing username and passwords			x	X		X	X		
Attempting to access or accessing the school / academy network, using another student's / pupil's account			X	x		X	X		

Incidents									
Attempting to access or accessing the school / academy 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		
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			X	X		X	X		
Continued 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		
Using proxy sites or other means to subvert the school's / academy's filtering system			X	X		X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident			X	X		X	X		
Deliberately accessing or trying to access offensive or pornographic material			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		

Staff   Actions / Sanctions

Incidents:	Refer to line managerr	Refer to Head Teacher Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X				
Inappropriate personal use of the internet / social media / personal email		x	x					
Unauthorised downloading or uploading of 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 eg holding or transferring data in an insecure manner		x	X	X				
Deliberate actions to breach data protection or network security rules		x	x	X				
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	x	X				
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		x	x	x				
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		x	x	X				
Actions which could compromise the staff member's professional standing		x	x	X				

Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy		x	x	X				
Using proxy sites or other means to subvert the school's / academy'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				
Continued infringements of the above, following previous warnings or sanctions		x	x	X				