Cheselbourne Village School

'Inspiring a Lifetime Love of Learning'

e-Safety Policy

Adopted by the Governing Body on

March 2020

The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be: January 2021

ICT & E-Safety Co-Ordinator: Emma Collett

E-Safety Governor: Graham Waters

Designated Safeguard Lead and Deputy: Mary See, Jacquie Mowlam and Emma Collett

Should serious e-safety incidents take place, the following external persons / agencies should be informed:	DCC Stephen King – ICT Schools Support 01305 221153 Stephen.a.king@dorsetcc.gov.uk Dorset Police 01305 222222

E-SAFETY POLICY

Contents:

1. **Rationale**
2. **Monitoring of this Policy**
3. **Scope of this Policy**
4. **Roles and Responsibilities**
5. **Policy Statements**
6. **Communication Technologies**
7. **Mobile Technologies**
8. **Technical – Infrastructure / Equipment, Filtering and Monitoring**
9. **Use of Digital and Video Images**
10. **Youth Produced Sexual Imagery (Sexting/ nude selfies)**
11. **Data Protection**
12. **Prevent Duty**
13. **Remote Learning**
14. **Social Media – Protecting Professional Identity**
15. **Unsuitable / Inappropriate Activities**
16. **Responding to Incidents of Misuse**

The main template of this Policy was created by the South West Grid for Learning Trust and adapted by the school to fit our specific needs.

Rationale

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 and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. Our school E-Safety Policy should help to ensure safe and appropriate use. The development and implementation of such a strategy involves all the stakeholders in a child's education from the head teacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students / pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of/sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video/internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this E-Safety Policy is used in conjunction with other school policies (e.g. Equality, Accessibility, behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

1. Monitoring of this policy

The school will monitor the impact of this policy using:

- Logs of incident reports
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring of data for network activity
- Survey of pupils / parents / staff

The school will follow this schedule for monitoring:

The E-Safety Policy was approved by Governors:	March 2019
The implementation of this policy will be monitored by:	E-Safety and ICT Co-ordinator Head teacher
Monitoring will take place at regular intervals of:	Every 3 years (September)
The Governing Body will receive a report on the implementations of the E-Safety Policy (which will include anonymous details of online incidents) at regular intervals of:	Once a year (September)
The E-Safety Policy will be reviewed annually, or more regularly in light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	April 2020
Should serious online safety incidents take place, the following external persons / agencies should be informed:	LA Safeguarding Officer Dorset Police LADO

2. Scope of this policy

This policy applies to all members of the school community (including staff, pupils, governors, 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 Head teachers 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, but is linked to membership of the school.

Cheselbourne Village 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 e-safety behaviour that take place out of school.

3. Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school:

a) Governors:

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

- Regular meetings with the E-Safety Co-ordinator
- Regular monitoring of e-safety incident logs
- Regular monitoring of filtering / change control logs
- Reporting to relevant Governors meeting

b) Head teacher:

- The head teacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, through the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator.
- The Head teacher should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see flow chart on dealing with e-safety incidents – section 14 – "Responding to incidents of misuse" and relevant Dorset County Council disciplinary procedures).
- The Head teacher is responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Head teacher 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.

c) E-Safety Coordinator:

- 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
- 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 E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- Attends relevant meetings of Governors
- Reports regularly to Head teacher

d) Network Manager, Technical Staff and ICT Coordinator:

The Network Manager/Systems Manager/ICT Technician/ICT Co-ordinator is responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack
- That the school meets required e-safety technical requirements and any Dorset County Council 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 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 is regularly monitored in order that any misuse / attempted misuse can be reported to the Head teacher for investigation
- That monitoring software / systems are implemented and updated as agreed in school policies

e) 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 Policy (AUP)
- They report any suspected misuse or problem to the Head teacher or E-Safety Coordinator for investigation

- All digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- E-safety issues are embedded in all aspects of the curriculum and other activities
- Students / pupils understand and follow the e-safety and acceptable use policies
- Students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- In lessons where internet use is pre-planned 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

f) Designated Safeguarding Lead and Deputy

The designated person for safeguarding should be trained in e-safety issues and should 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

g) Pupils:

- Are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Policy
- 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 the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

h) Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to parents' sections of the website and on-line pupil records
- Their children's personal devices at home, as they are not allowed on site.

4. Policy Statement

a) Education – children

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 and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and PSHE 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 student 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.

b) 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 online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, web site
- 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 www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers (see appendix for further links / resources)

c) Education & 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:

- An annual 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. It is expected that some staff will identify e-safety as a training need within the performance management process.
- All new staff should receive e-safety training 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 meetings and INSET days.

d) Training – Governors

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

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

5. Communication Technologies

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				Students/Pupils			
Communication Technologies	Not allowed	Allowed at certain times	Allowed for selective staff	Allowed	Not allowed	Allowed at certain times	Allowed for selective pupils	Allowed
Mobile phones may be bought into school				X		X		
Use of mobile phones in lessons	X				X			
Use of mobile phones in social time		X			X			
Taking photos on mobiles / cameras		X				X		
Use of other mobile devices eg. tablets, gaming devices		X				X		
Use of personal email addresses in school, or on a 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.
- 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, 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.

- Individual email address will be provided by the school and managed by the class teachers for educational use.
- Students 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.

6. Mobile Technologies

Mobile technology devices may be school owned / provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet 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 of mobile / personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school policies, including but not limited to the Safeguarding policy, Behaviour policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about safe and appropriate use of mobile technologies should be an integral part of the school's E-Safety education program.

7. 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 ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling is securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- All users (at KS2) will be provided with a username and secure passwords. 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 (or other person) must also be available to the Head teacher kept in a secure place (e.g. school safe)
- The school secretary 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.
- The school can provide differentiated user-level filtering.
- School technical staff regularly monitors and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed (see section 14 for flow chart).
- 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. (Currently Eset provided by DCC)
- An agreed policy is in place for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school systems. Guests are provided with a temporary log in and password which enables them to access the school system.
- Staff members are blocked from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (e.g. 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.

8. 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 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 should not be used for such purposes.
- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website.

9. Youth Produced Sexual Imagery (Sexting/ nude selfies)

Youth produced sexual imagery (Sexting/ nude selfies) involves images or videos which are indecent or of a sexual nature, generated by children under the age of 18 or of children under the age of 18, shared via a mobile phone, handheld device or website. Incidences of youth produced sexual imagerry will be thoroughly investigated by the DSL Lead and Safeguarding Governor. Parents will be asked to come to school as a matter of urgency where the issue will be discussed before appropriate action is taken. This may involve involving a third party such as Police Community Support Officers or Social Welfare. Please refer to Sexting Incidences set out in the UK Council for Internet Child Safety guidance document Sexting in schools and colleges: responding to incidents and safeguarding young people. Cheselbourne Village School's Governing body should ensure that the child protection policy includes all that is set out on Section 90 page 22 / 23 of keeping children safe in education 2018.

Through Computing lessons, assemblies and PSHE, children will be taught *set out what we have in place to minimise the risk of peer on peer abuse (e.g. what policies*

are in place; addressing issues through the curriculum /PSHE; working with other agencies; risk assessments etc) Pantasaurs?

- *explain how allegations (in addition to those noted above) will be investigated and dealt with – e.g. initiation-type violence, incidents of sexual touching etc*

10. Data Protection GDPR

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.

Following a number of "high profile" losses of personal data by public organisations, schools are likely to be subject to greater scrutiny in their care and use of personal data.

The school will 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 protected (many memory sticks / cards and other mobile devices cannot be password protected).
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

11. Prevent Duty

The school acknowledges that E-safety has an important role to play in preventing radicalisation and terrorism. This is addressed through E-Safety lessons delivered to the children in school, and through monitoring of children's use of the internet, Acceptable Use Agreements, and filtering, as set out in this policy.

12. Social Media - Protecting Professional Identity

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk.

School staff should ensure that:

- No reference should be made in social media to students, 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.
- See also the school Social Media Policy.

13. Remote Learning

These guidelines are in response to the Covid-19 pandemic and also cover any future situation where the school could be closed and remote learning becomes necessary. There are a wealth of online services and systems that enable online video and audio communication. It's important to consider the features you need based on the group and objectives you have.

Live Video

Staff may consider using Live Streaming services but would exercise caution here given requirements for accounts, personal data and privacy questions. Equally messaging services may be considered, but equal. Do consider the terms of service together with privacy policies and in particular if there are any minimum age requirements of the chosen service. Consider if the system includes online chat feature, and if this can be moderated. Consider Privacy settings before posting – (e.g. YouTube has a variety of settings (Public, Unlisted, Private, Comments Allowed/Not Allowed) that will determine who can see and comment on the video). If messaging services are used by staff, e.g. WhatsApp, be mindful of professional standards.

Technology

Not all students will have access to technologies that will enable them to participate in online classes. School staff should reasonably find solutions to enable them to continue learning, such as loan of devices, posted assignments, or phone calls with staff. Consider activities carefully when planning – online access within school will have internet content filtering systems in place that are unlikely to be replicated in the home environment. Be careful that staff and children don't incur surprising costs, eg mobile data access charges - (video utilises significant amounts of data). Also consider the security of devices, in particular cameras and microphones. We would strongly recommend that staff avoid using personal devices and should only use school provided equipment. If staff have to use their own devices as they do not have an alternative they should only use their school email account and block their phone number.

Location/Environment

If live video and audio is being used, staff should carefully consider the location that everyone uses. You may choose to use a conferencing service that the teacher can disable users microphone and video cameras.

Behaviour

Be clear about the expectations of both student and staff behaviour (e.g. a 'classroom standard' of behaviour is expected from all participants). During video conferencing it is worth considering some ground rules such as; creating safe spaces and explaining these as the introduction to each session. If this is the first time that classes are delivered online, it may take some time in becoming familiar with the new environment.

Recording

Always make a note of the conference timing and who participated, including those that arrived/departed early or late. Be clear about whether it is acceptable for students to record events and expectations/restrictions about onward sharing. If the service you use records the conference, make sure that everyone is aware of this. It's important that the school keeps these recordings inline with the school's GDPR guidelines.

Personal Data
The conference service may require the sharing of personal data, eg usernames to invite in. It is always best practice to use school-provided email addresses as Data protection laws still apply.

Safeguarding
Online or offline, effective Safeguarding requires a whole-school approach. Planning for online or distance learning activities should include the school's safeguarding team as part of the planning process. Ensure online tuition follows best practice (e.g. 2 members of staff involved) and is in-line with the School's Safeguarding Policy. Regularly remind students of who they can contact within the school for help or support. Staff will regularly inform parents about enhanced online safety measures by setting online safety challenges, sending out information/posters to inform about how to keep safe accessing online resources whilst at home and reminding them of reporting options. Most importantly, staff should always report any safeguarding incidents or potential concerns to the Safeguarding Lead or Deputy. If an incident occurs during on site learning (where it is provided for specific children) at the school or another school if schools have been hubbed, report concerns to CVS safeguarding leads as well as the safeguarding leads at the hub school site. Safeguarding Lead and Deputy will follow the schools safeguard reporting procedures.

14. Unsuitable / inappropriate activities

Some internet activity, e.g. accessing child abuse images or distributing racist material, is illegal and would obviously be banned from school and all other technical systems. Other activities, e.g. cyber-bullying, would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those 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

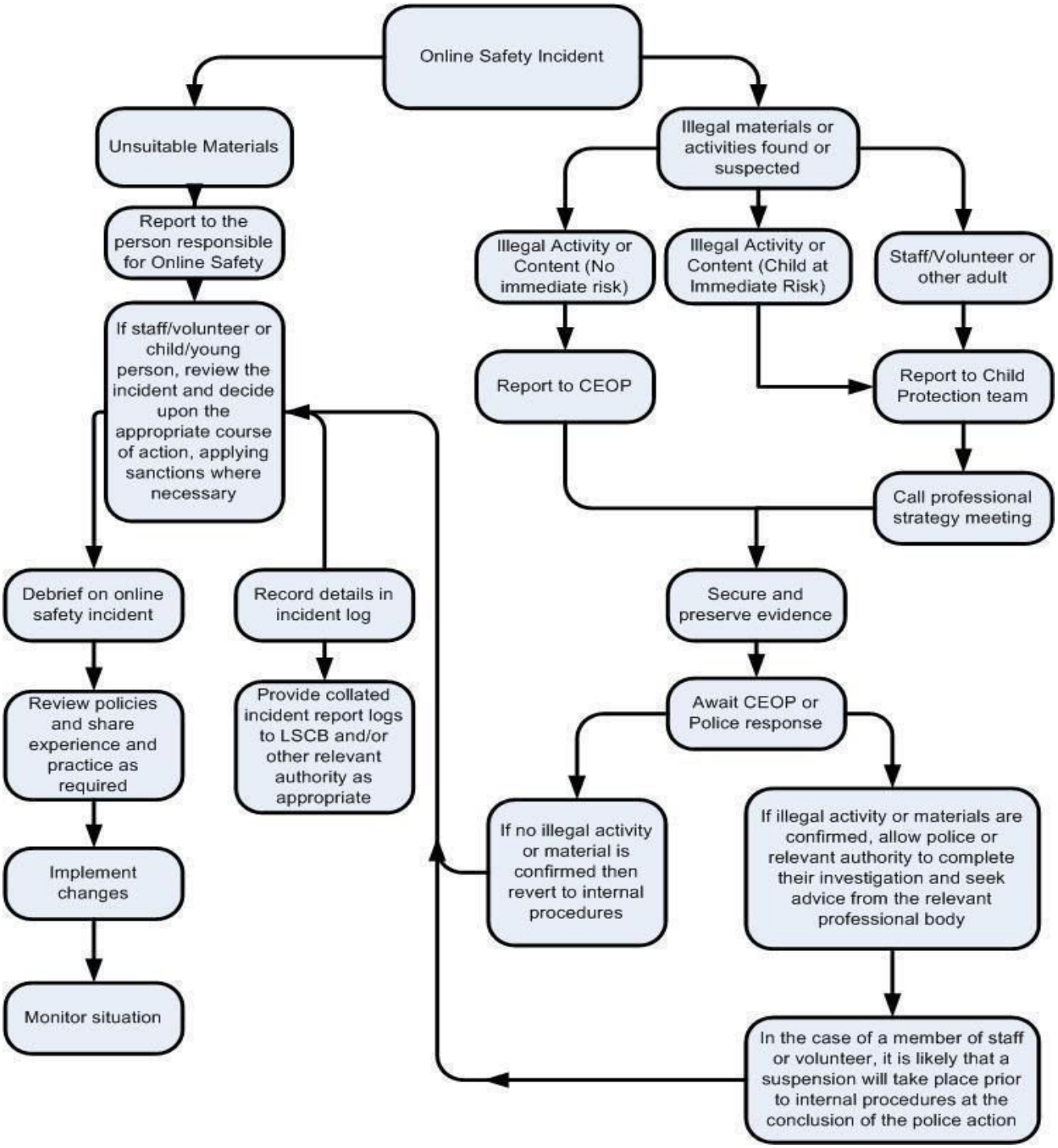
		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child sexual abuse 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	
On-line gaming (educational)				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		

15. 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.

a) 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) for responding to online safety incidents and report immediately to the police.



b) 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:

- There will be 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).
- 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.

c) 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.

Students / Pupils Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to IT Co-ordinator	Refer to Headteacher	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					
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		X	
Unauthorised use of social media / messaging apps / personal email	X	X	X			X	X	X	
Unauthorised downloading or uploading of files	X	X	X			X	X	X	
Allowing others to access school / academy network by sharing username and passwords	X	X	X			X	X	X	
Attempting to access or accessing the school / academy network, using another pupil's account	X	X	X		X	X	X	X	
Attempting to access or accessing the school / academy network, using the account of a member of staff	X	X	X		X	X	X	X	X
Corrupting or destroying the data of other users	X	X	X			X	X	X	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X		X	X	X	X
Continued infringements of the above, following previous warnings or sanctions	X	X	X			X	X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X			X	X	X	X
Using proxy sites or other means to subvert the school's / academy's filtering system	X	X	X		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	X	X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X			X		X	

Staff Actions / Sanctions

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action 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			X	X
Inappropriate personal use of the internet / social media / personal email	X	X				X		
Unauthorised downloading or uploading of files	X	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		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	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		X	X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X				X	X	X
Actions which could compromise the staff member's professional standing	X	X				X		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X				X		
Using proxy sites or other means to subvert the school's / 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	X	X	X	X	X
Breaching copyright or licensing regulations	X	X				X		
Continued infringements of the above, following previous warnings or sanctions	X	X				X	X	X