**Coniston Primary School**
*working together we can succeed*

# e-Safety Policy

**Including Staff & Volunteer Acceptable Use Policy Agreement**
**Including Parent/Carer Acceptable Use Policy Agreement**
**Including Rules for Keeping Safe with ICT – Pupils**
**Including Home use of the Internet**

## Reviewed & Adopted June 2018

This e-safety policy has been developed, and will be reviewed and monitored, by our school e-safety working group which comprises of:

- Computing Subject Leader
- Headteacher
- A governor representative

Consultation with the whole school community has taken place through a staff meeting, Student Council meeting, governors meeting, parents evening and the school website / newsletter.

**Schedule for Development, Monitoring and Review**

| | |
|---|---|
| This e-safety policy was approved by the *Governing Body* | |
| The implementation of this policy will be monitored by the: | E-safety working group |
| Monitoring will take place at regular intervals: | Annually during Term 6 |
| The *Governing Body* will receive a report on the implementation of this policy including reported incidents: | Annually at last meeting of the year |
| This policy will be reviewed regularly and in the light of significant new developments or threats to e-safety. | Annually during Term 1 and/or when required |
| Should serious e-safety incidents take place, the following external persons / agencies should be informed: | Tina Wilson– Safeguarding (LADO)<br>Andreas Burt – Technical<br>Jo Briscombe – ICT Strategy Adviser |

The school will monitor the impact of the policy using:

- Logs of reported incidents
- SWGfL monitoring logs of internet activity and any network monitoring data from the LA technical team
- Surveys / questionnaires of students, parents / carers, and staff including non-teaching staff

**Scope of the Policy**

This policy applies to all members of the school community (including staff, students, volunteers, parents/carers, visitors and community users) who have access to and are users of school ICT systems, both in school and out of school where actions relate directly to school set activity or use of school online systems. The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of students / 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 such as cyber-bullying, which may take place out of school, but are linked to membership of the school. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, inform parents / carers of known incidents of inappropriate e-safety behaviour that take place out of school.

The following sections outline the roles and responsibilities, policy statements and education in relation to e-safety for individuals and groups within the school.

**Roles and Responsibilities**

These are clearly detailed in Appendix 1 for all members of the school community.

The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety is delegated to the E-Safety Leader.
The designated person for child protection is trained in e-safety issues and is aware of the potential for serious child protection 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 and cyber-bullying.

### Staff and Governors

There is a planned programme of e-safety training for all staff and governors to ensure they understand their responsibilities, as outlined in this, and the acceptable use policies.

- An audit of the e-safety training needs of all staff is carried out annually.
- All new staff  receive e-safety training as part of their induction programme
- The e-Safety Leader receives regular updates through attendance at SWGfL and LA training sessions and by reviewing regular e-safety updates from the local authority.
- This e-Safety policy and its updates shared and discussed in staff meetings.
- The e-Safety Leader  provides advice/guidance and  training as required to individuals as required and seeks LA advice on issues where required.

### Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating learners to take a responsible approach.  The education of pupils in e-safety is therefore an essential part of our 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.

- There is a planned e-safety programme (scheme of work) detailed below.
- Key e-safety messages are reinforced regularly through assemblies
- Pupils  are helped to understand the student acceptable use policy and act accordingly
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems are posted in all rooms where ICT is used and displayed on log-on screens.
- Staff act as good role models in their own use of ICT.

### Curriculum

E-safety is a focus in all relevant areas of the curriculum. The e-safety scheme of work is linked to the Becta Signposts to Safety key e-safety elements of culture, contact, commerce and content. It identifies for each year group progression statements, learning outcomes, processes, skills and techniques, vocabulary, suggested software and web links, sample activities and assessment activities.

- In lessons where internet use is pre-planned, students are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches. Staff pre check any searches.
- Where students are allowed to freely search the internet, e.g. using search engines, staff are vigilant in monitoring the content of the websites the young people visit and encourage students to use specific search terms to reduce the likelihood of coming across unsuitable material.
- Students are taught to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

### Parents / Carers

Parents and carers may have only a limited understanding of e-safety issues and may be unaware of risks and what to do about them. They have a critical role to play in supporting their children with managing e-safety risks at home, reinforcing key messages about e-safety and regulating their home experiences. The school supports parents to do this by:

- Providing clear acceptable use policy guidance and regular newsletter and web site updates
- Providing an awareness raising meeting for parents

### Technical Staff - Roles and Responsibilities

For **all** schools, the local authority provides technical guidance for e-safety issues, and the team are fully informed about the issues. Where the local authority provides technical support the "administrator" passwords for the school are not held by the school and the local authority are responsible for their security and any implications of their use.

The school ensures, when working with our technical support provider that the following guidelines are adhered to.

- School ICT systems are managed in ways that ensure that the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and relevant Local Authority E-safety guidance.
- There are regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling are securely located and physical access is restricted.
- All users have clearly defined access rights to school ICT systems.
- All users are provided with a username and password by the technical support provider.
- Users are responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by SWGfL.
- Requests from staff for sites to be removed from the filtered list must be approved by the head teacher and this is logged.
- In the event of the school technician needing to make requested changes to filtering, or for any user, this is logged and carried out by a process that is agreed by the Headteacher.
- Any filtering issues are reported immediately to the South Gloucestershire technical team.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Actual / potential e-safety incidents are documented and reported immediately to the E-safety Leader who will arrange for these to be dealt with immediately in accordance with the acceptable use policy.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy is in place for the provision of temporary access of “guests” (e.g. trainee teachers, visitors) onto the school system.
- The downloading of executable files by users is not permitted without the approval of the Headteacher, in consultation with the school’s ICT technical advice
- An agreed policy is in place that allows staff to install programmes on school workstations / portable devices only with the approval of the Headteacher, in consultation with the school’s ICT technical advice
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data can not be sent over the internet via e-mail or taken off the school site. SOFIE must be used for this.

**Use of digital and video images - Photographic, Video**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are reported incidents of employers carrying out internet searches for information about potential and existing employees. The school informs and educates users about these risks and implements policies to reduce the likelihood of the potential for harm:

- When using digital images, staff educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but follow guidance in the acceptable use policy concerning the sharing, distribution and publication of those images.
- Staff ensure that pupils also act in accordance with their acceptable use policy.
- Pupil’s work is only published on a public web site with the permission of the student and parents or carers.

**Guidance on the Use of Communications Technologies**

A wide range of communications technologies have the potential to enhance learning

- The official school email and text messaging service is used for communications between staff, and with parents/carers and pupils as it provides an effective audit trail.

- Any digital communication between staff and pupils or parents / carers must be professional in tone and content. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Users are made aware that electronic communications may be monitored and what to do if they receive an email that makes them feel uncomfortable, is offensive, threatening or bullying in nature through the acceptable use policies.
- Whole class or group email addresses will be used at KS1, while students / pupils at KS2 and above will be provided with individual school email addresses for educational use only.
- Pupils are taught about email safety issues through the scheme of work and implementation of the acceptable use policy.
- Personal information is not sent via e-mail as this is not secure. Personal information is also not posted on the school website and only official email addresses are listed for members of staff.

. The following table shows how the school currently considers these should be used.

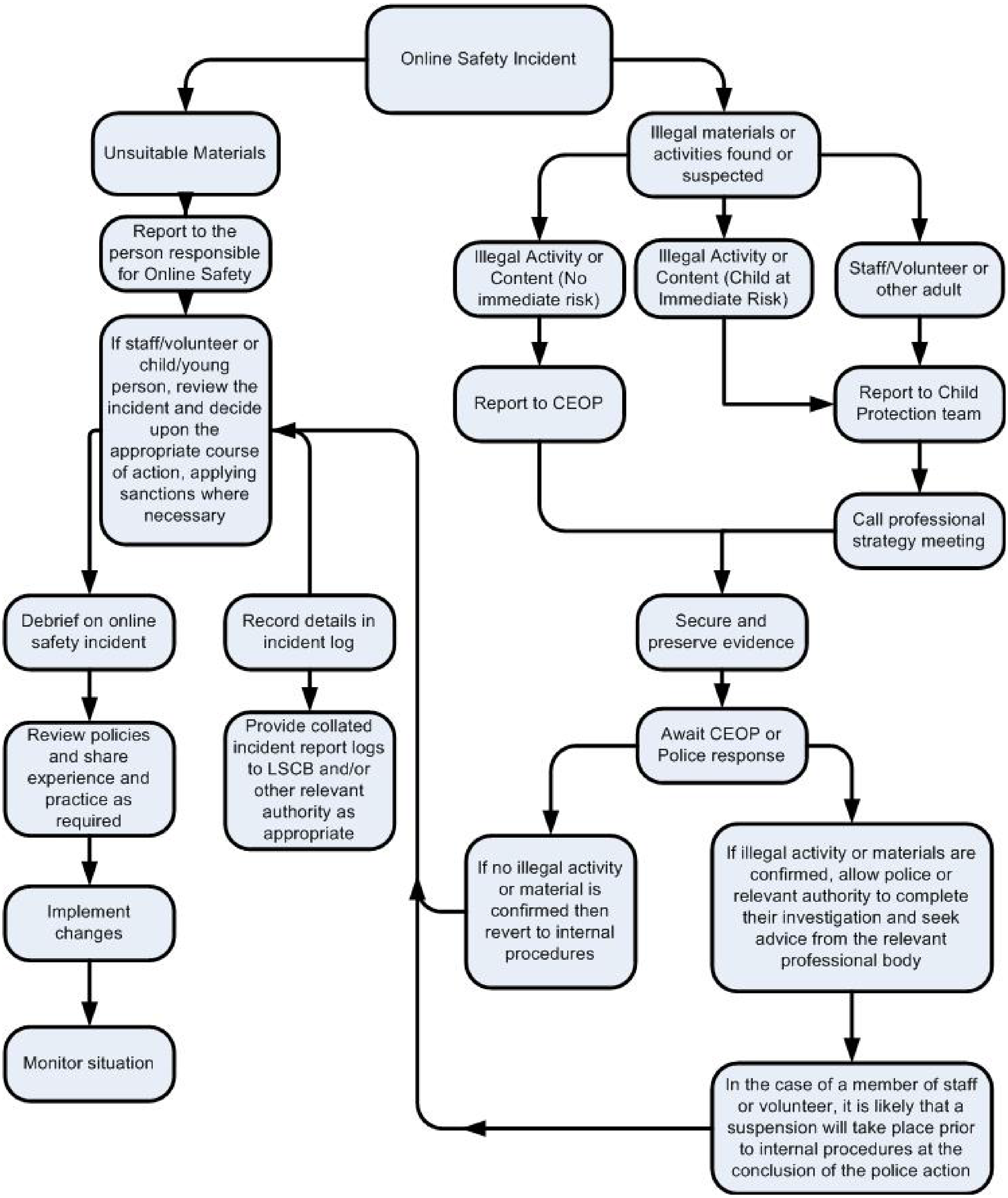
| | Staff & other adults | | | | Students / Pupils | | | |
|---|---|---|---|---|---|---|---|---|
| Communication Technologies | Allowed | Allowed at certain times | Allowed for selected staff | Not allowed | Allowed | Allowed at certain times | Allowed with staff permission | Not allowed |
| Mobile phones may be brought to school | ■ | | | | | | ■ | |
| Use of mobile phones in lessons | | ■ | | | | | | ■ |
| Use of mobile phones in social time | ■ | | | | | | | ■ |
| Taking photos on mobile phones or other camera devices | | | ■ | | | ■ | ■ | |
| Use of hand held devices e.g. PDAs, PSPs | | ■ | | | | | ■ | |
| Use of personal email addresses in school, or on school network | ■ | | | | | | | ■ |
| Use of school email for personal emails | | | | ■ | | | | ■ |
| Use of chat rooms / facilities | | | | ■ | | | | ■ |
| Use of instant messaging | | | | ■ | | | | ■ |
| Use of social networking sites | | | ■ | | | | | ■ |
| Use of blogs | | | ■ | | | | ■ | |

**Responding to incidents of misuse**

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

**Illegal Incidents**

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



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)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
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

### Unsuitable / inappropriate activities

The school believes that the activities referred to below are inappropriate for school and that users should not engage in these activities in school or outside school when using school equipment or systems.

| 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 | | | | | □ |
| | promotion or conduct of illegal acts, e.g. under child protection, obscenity, computer misuse and fraud legislation | | | | | □ |
| | adult material that potentially breaches the Obscene Publications Act in the UK | | | | | □ |
| | criminally racist material in UK | | | | | □ |
| | pornography | | | | □ | |
| | promotion of any kind of discrimination | | | | □ | |
| | promotion of racial or religious hatred | | | | □ | |
| | threatening behaviour, including promotion of physical violence or mental harm | | | | □ | |
| | any other information which may be offensive to colleagues, breaches the integrity of the ethos of the school or brings the school into disrepute | | | | □ | |
| Using school systems to run a private business | | | | | □ | |
| Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school | | | | | □ | |
| Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions | | | | | □ | |
| Revealing or publicising confidential or proprietary information (e.g. financial / personal, databases, computer / network access codes and passwords) | | | | | □ | |
| Creating or propagating computer viruses or other harmful files | | | | | □ | |
| Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet | | | | | □ | |
| On-line gaming (educational) | | | □ | | | |
| On-line gaming (non educational) | | | □ | | | |
| On-line gambling | | | | | □ | |
| On-line shopping / commerce | | | □ | | | |
| File sharing | | | | | □ | |
| Use of social networking sites apart from Merlin e.g. Bebo, Facebook for older users | | | | □ | | |
| Use of video broadcasting e.g. Youtube | | | | □ | | |

**Appendix 1: Roles and Responsibilities**

| Role | Responsibility |
|---|---|
| **Governors** | • Approve and review the effectiveness of the E-Safety Policy and acceptable use policies<br>• E-Safety Governor works with the E-Safety Leader to carry out regular monitoring of e-safety incident logs, filtering, changes to filtering and then reports to Governors |
| **Head teacher and Senior Leaders:** | • Ensure that all staff receive suitable CPD to carry out their e-safety roles and sufficient resource is allocated.<br>• Ensure that there is a system in place for monitoring e-safety<br>• Follow correct procedure in the event of a serious e-safety allegation being made against a member of staff<br>• Inform the local authority about any serious e-safety issues including filtering<br>• Ensure that the school infrastructure / network is safe and secure and that policies and procedures approved within this policy are implemented. |
| **E-Safety Leader:** | • Lead the e-safety working group and dealing with day to day e-safety issues<br>• Lead role in establishing / reviewing e-safety policies / documents,<br>• Ensure all staff are aware of the procedures outlined in policies<br>• Provide and/or brokering training and advice for staff,<br>• Attend updates and liaising with the LA e-safety staff and technical staff,<br>• Deal with and log e-safety incidents including changes to filtering,<br>• Meet with E-Safety Governor to annually to discuss incidents and review the log<br>• Report regularly to Senior Leadership Team |
| **Curriculum Leaders** | • Ensure e-safety is reflected in teaching programmes where relevant eg anti bullying, English, publishing and copyright and is reflected in relevant policies. |
| **Teaching and Support Staff** | • Participate in any training and awareness raising sessions<br>• Have read, understood and signed the Staff Acceptable Use Agreement (AUP)<br>• Act in accordance with the AUP and e-safety policy<br>• Report any suspected misuse or problem to the E-Safety Co-ordinator<br>• Monitor ICT activity in lessons, extra curricular and extended school activities |
| **Students / pupils** | • Participate in e-safety activities, follow the acceptable use policy and report any suspected misuse<br>• Understand that the E-Safety Policy covers actions out of school that are related to their membership of the school |
| **Parents and carers** | • Endorse (by signature) the Student / Pupil Acceptable Use Policy<br>• Ensure that their child / children follow acceptable use rules at home<br>• Discuss e-safety issues with their child / children and monitor their home use of ICT systems (including mobile phones and games devices) and the internet<br>• Access the school website in accordance with the relevant school Acceptable Use Policy.<br>• Keep up to date with issues through school updates and attendance at events |
| **Technical Support Provider** | • Ensure the school's ICT infrastructure is secure in accordance with Becta guidelines and is not open to misuse or malicious attack<br>• Ensure users may only access the school network through an enforced password protection policy, where passwords are regularly changed for those who access children's data<br>• Inform the head teacher of issues relating to the filtering applied by the Grid<br>• Keep up to date with e-safety technical information and update others as relevant<br>• Ensure use of the network is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator for investigation / action / sanction.<br>• Ensure monitoring software / systems are implemented and updated<br>• Ensure all security updates / patches are applied (including up to date anti-virus definitions, windows updates) and that reasonable attempts are made to prevent spyware and malware. |
| **Community Users** | • Sign and follow the AUP before being provided with access to school systems. |

## Appendix 2: Staff (and Volunteer) Acceptable Use Policy Agreement

**Policy Context**

The internet and other technologies are powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users have an entitlement to good, safe access to ICT and the internet. This Acceptable Use Policy is intended to ensure that:

- Staff and volunteers are responsible users and stay safe while using technologies
- School ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Staff are protected from potential risk from the use of ICT in their everyday work and work to ensure that young people in their care are safe users.

### Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems, other users and pupils.

**Keeping Safe**

- I know that the school will monitor my use of the school ICT systems and communications.
- I will only use my own user names and passwords which I will choose carefully so they can not be guessed easily. I will not use any other person's username and password.
- I will ensure that my data is regularly backed up.
- I will not engage in any on-line activity that may compromise my professional responsibilities or compromise the reputation of the school or its members.
- I understand that data protection requires that any personal data that I have access to must be kept private and confidential, except when I am required by law or by school policy to disclose it to an appropriate authority.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school personal data policy. I will not send personal information by e-mail as it is not secure.
- Where personal data is transferred outside the secure school network, it must be encrypted.
- I will not try to bypass the filtering and security systems in place.
- I will only use my personal ICT in school for permissible activities and I will follow the rules set out in this agreement.

**Promoting Safe Use by Learners**

- I will model safe use of technologies and the internet in school.
- I will educate young people on how to use technologies safely according to the school teaching programme.
- I will take immediate action in line with school policy if an issue arises in school that might compromise learner, user or school safety or if a child reports any concerns.
- I will monitor learner behaviour online when using technology and deal with any issues that arise.

**Research and Recreation**

- I will not upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.
- I will not (unless I have permission) make large downloads or uploads that might take up internet capacity.
- I know that all school ICT is primarily intended for educational use and I will only use the systems for personal or recreational use if this is allowed by the school (see main policy)

**Communicating and Sharing**

- I will communicate online in a professional manner and tone, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will only communicate with pupils and parents / carers using official school systems.
- I will be aware that any communication could be forwarded to an employer or governors.
- I will only use chat and social networking sites for school purposes that are approved by the school.
- I will not use personal email addresses on the school ICT systems unless I have permission to do so.
- I will not access, copy, remove or otherwise alter any other user's files, without their permission.
- I will ensure that I have permission to use the original work of others in my own work and will credit them if I use it. Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I will only take images or video of pupils/staff where it relates to agreed learning and teaching activities and will ensure I have parent/staff permission before I take them. If these are to be published online or in the media I will ensure that parental / staff permission allows this.
- Where these images are published (e.g. on the school website / Twitter) I will ensure it is not possible to identify the people who are featured by name or other personal information.
- I will not use my personal equipment to record images / video unless I have permission to do so.
- I will not keep images and videos of students stored on my personal equipment unless I have permission to do so. If this is the case I will ensure that these images can not be accessed or copied by anyone else or used for any purpose other than that I have permission for.

**Buying and Selling**

- I will not use school equipment for online purchasing unless I have permission to do so.

**Problems**

- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the e-safety co-ordinator or head teacher.
- **If I believe a young person may be at risk I will follow the child protection procedures.**
- **If I believe a young person may be being bullied I will follow the anti-bullying procedures.**
- I will not install or store programmes on a computer unless I have permission.
- I will not try to alter computer settings, unless this is allowed in school policies.
- I will not cause damage to ICT equipment in school and will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.

I understand that these rules are in place to enable me to use ICT safely and that if I do not follow them I may be subject to disciplinary action. I agree to use ICT by these rules when:

- I use school ICT systems at school or at home when I have permission to do so
- I use my own ICT (including mobile phone when allowed) in school
- I use my own ICT out of school (including mobile phone) to use school sites or for activities relating to my employment by the school

Staff / Volunteer Name

Signed

Date

## Appendix 3: Parent / Carer Acceptable Use Policy Agreement

Technologies open up new learning opportunities and can promote creativity, effective learning and communication. They can promote more effective communications between parents / carers and the school in order to support young people with their learning. This Acceptable Use Policy is intended to ensure:

- You are aware of what the school is doing to help your child become a responsible user of technology and stay safe at school
- You are aware of the importance of e-safety and able to support your child with keeping safe and behaving well online at home.

The school will aim to ensure your child has good, safe access to ICT for learning and, in return, expects your child to use the equipment responsibly.

### Keeping Safe

- Your child will be asked to sign the attached Acceptable Use Agreement which sets out clear expectations of behaviour when working online. We hope you will take to your child about this.
- Your child will be provided with teaching about e-safety and keeping safe using technology.
- They should only use their own log in for systems and to keep their details private. Your child is responsible for what their log in is used for.
- The school takes every reasonable precaution, including monitoring and filtering systems, to ensure that your child is safe when they use technology at school. The school cannot be held responsible for the nature and content of materials accessed using technology as security systems cannot protect against everything.
- Your child's use of ICT in school will be monitored and we will contact you if we have e-safety concerns.
- We only allow children to use age appropriate web sites in schools as using sites for older users can increase risks. We accept that you may allow them to use sites that they are not old enough for at home. If this is the case then we would hope that you will be monitoring their use and will deal with any issues that arise.

### Communicating and Sharing

- Children and members of staff may use digital cameras to record learning activities. These images may be used in lessons or to celebrate success through being published in newsletters, on the school website or occasionally in the public media.
- The school will comply with the general data protection regulations and ask your permission, through this policy, before taking images. We will also ensure that when images are published the young people cannot be identified by the use of their names.
- If you take images at school events which include children, other than your own, you will need to follow these guidelines. Your child should also only take images with permission.

### Behaviour

- Your child is expected to behave well online as they are expected to during all other school activities.
- Bullying is not tolerated in any form and this includes online.

### Problems

- We can only take responsibility for e-safety issues that happen in school, or at home when children are using sites recommended by the school.
- Any issues you are made aware of with use of technology in school should be reported immediately to a child's teacher so that appropriate steps can be taken.
- If your child does not behave appropriately online then the school will take steps to deal with this as with any other issue with behaviour.

**Permission Form**

We request that you sign the permission form below to show your support of the school in helping to keep your child safe. By signing this form you are agreeing that:

- You have read and discussed the rules with your child
- You understand the rules that your child should following when using ICT in school and this also applies to their use of their mobile phone
- Your child can use school ICT systems for systems
- You give permission for taking and using images of your child for learning purposes
- You are responsible for your child's safety online when at home

Parent / Carers Name Date

Pupil Name

## Appendix 4: Rules for Keeping Safe with ICT

### Keeping Safe

- I will not use ICT in school (including my own) without permission from my teacher.
- I will choose my user names and passwords carefully to protect my identity and I will not share them. I will not ask computers to remember my password.
- I must keep my personal details and those of others private.
- I will not visit unsafe sites or register for things I am not old enough for.
- I will log off sites when I have finished.

### Communicating and Sharing

- I know that I need to behave well online as in real life and be polite and friendly.
- I will not open messages if the subject field is not polite or if I do not know who it is from. I know that others may have different opinions and that I should respect them.
- I am careful about what I send as messages can be sent on to my parents or head teacher.
- I know that I must have permission to communicate online and will make sure my teacher / parents know who I communicate with.
- I will talk to an adult if an online friend wants to meet me and never arrange to meet anyone without permission.
- I will not use anyone else's work or files without permission.
- Where work is protected by copyright, I will not try to download copies.
- I will not take or share pictures of anyone without their permission.
- I know that anything I put up on the internet can be seen by anyone.
- I will only use my mobile phone at school for things that the school allows.

### Research and Fun

- I will use clear search words so that I find the right information.
- I know that some content may not be filtered out and what to do if I find something worrying.
- I will double check information I find online.

### Buying and Selling

- I know that I should not buy anything on line without permission.

### Problems

- I will not try to change computer settings or install programmes.
- I will not damage equipment and will tell a teacher if equipment is broken or not working.
- I will tell a teacher or adult I trust if I find anything on a computer or message that is unpleasant or makes me feel uncomfortable.
- I will tell a teacher or adult I trust if I know of anyone that is behaving badly on line or anyone may be being bullied.

I agree to use ICT by these rules when:

- I use school ICT or my own in school (including my mobile phone when allowed)
- I use my own ICT (including mobile phone) out of school to use school sites or for school activities

My Name is

My Class teacher is

Signed                Date

## Appendix 5: Home Use of the Internet

We hope you will reinforce the e-safety messages when your child uses the internet at home. Some ways that you could do this are listed here to support parents who may not be aware of all the issues.

### Equipment

- Make sure your child accesses the internet in a communal room and with appropriate supervision (including supervising all internet use by younger users).
- Make sure that family computers are password protected and have anti-virus software which is regularly updated.
- Make sure content is appropriately filtered for younger users.
- Make sure your child knows that a protection system does not stop all unsafe content and they need to tell you if they access something inappropriate or get an upsetting message.

### Keeping Safe

- Set appropriate rules for using ICT at home. The school rules could be a starting point.
- Tell the school of any concerns that they could help to address through teaching.
- Ensure that your child knows not to leave computers logged on with their user name or logged on to sites with personal details entered as others could use them.
- Discuss user names and talk about how to choose them carefully to protect their identity.
- Talk about the information children should keep private in order to stop them being contacted including full name, address, telephone no, school, places they go regularly.
- Ask your child about the sites they are visiting.
- Talk about the need use the safety and privacy features of sites to only give access to people they know and being careful who they add as friends.

### Communicating

- Talk to your child about the fact that any information published on the web can be read by anyone and that they should only post things they would be happy for anyone to read.
- Check information that younger users are publishing to ensure that they are not putting themselves at risk.
- Check that they are old enough for the sites they are using. If you allow them to use a site they are not old enough for ensure that you have access to what they are doing so that you can monitor it.
- Talk about the need to be polite online and that they should not use bad language or comments which might upset others.
- Discuss the fact that e-mails / messages can be intercepted and forwarded on to anyone (including parents, head teacher or future employer!).
- Make sure they know they should not open messages if the subject field is offensive or if they do not recognise who it is from and that the safest thing to do is to delete it without opening it.

### Buying and Selling Online

- Make sure they know that downloading copyrighted games and music without paying for it is illegal
- Discuss how to recognise commercial uses of the internet e.g. I Tunes, mobile phone downloads.
- Remind them they should not respond to offers they have not requested as these could be scams, result in costs or be trying to find out their personal information.
- Remind them that they should not purchase or download anything that costs money without asking permission and that they should not use someone else’s identity to buy things online.

### Problems

- Make sure they know that if they get any problems with using computers or get an offensive or worrying message / e-mail they should not reply but should save it and tell you.
- Reassure your child that if they talk to you about a problem online you will not ban them from using it as this will discourage them from telling you.

**Signed …………………………………….**

**(M Lloyd, Chair of Governing Body)**

**Adopted: June 2018**

**Date for review: May 2019**