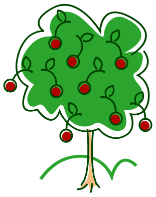
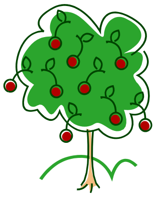


Cherry Orchard Online Safety Policy



At Cherry Orchard Primary School we are committed to creating a safe learning environment for pupils to learn. We readily use a range of technologies to enhance pupils' experiences during the school day and at home. We expect all members of our school community to follow our Online Safety policy.

The breadth of issues classified within online safety is considerable, but can be categorized into three areas of risk:

- Content – being exposed to illegal, inappropriate or harmful material.
- Contact – being subjected to harmful online interaction with other users
- Conduct – personal online behaviour that increases the likelihood of, or causes, harm.

Aims

We aim to help every pupil and adult to:

- Feel safe and confident when using new technologies.
- Know who to speak to when they feel unsafe.
- Know how to report any abusive behaviour.
- Know how to use the internet correctly, without misuse.
- Stay in control and keep personal information private.

Roles and Responsibilities

All the adults that are involved in the life of the school; whether governors, teaching staff, support staff, technicians and the community have roles and responsibilities that are associating with online safety as well as all pupils that come into contact with computers.

Governors

The Governors are responsible for the approval of the Online Policy and reviewing the effectiveness of it regularly. Regular meetings and information will be provided to the Governors so they are able to make the correct recommendations, they will also be able to carry out regular monitoring of online safety incident logs when required.

Head Teacher and Senior Leadership

The Head Teacher is responsible for ensuring the safety, including online safety of the members of the school community. Emma Emery is the named Online Safety Coordinator.

The Head Teacher and Senior Leadership Team are responsible for ensuring that all staff Safety receive correct and suitable Continuing Professional Development (CPD).

The Head Teacher and Senior Leadership Team will ensure that there is a system in place to monitor the usage of internet and other technologies and that the person who carries out the internal online safety monitoring receives support and is also monitored. This is to provide a safety net and also to support those colleagues who take on important monitoring roles.

The Head Teacher and another member of the Senior Leadership Team are to ensure they know the correct procedures that need to be followed when a serious allegation has been made by a child or one that is in regards to a member of a staff.

Teaching and Support Staff

Teaching and Support Staff are responsible for-

- Ensuring they stay up to date with current online safety matters and policies and practice.
- Reading, understanding and carrying out the Acceptable Use Policy and online safety and signing to say that they have read the policy.
- Reporting any misuse or problems to the Head Teacher Online Safety Coordinator or Lead DSL for further investigation.
- Ensuring any digital communications with pupils is strictly professional and only carried out using school systems.
- Ensuring online safety issues are embedded throughout the curriculum.
- Ensuring pupils follow the Online Safety policy.
- Awareness of online issues related to the use of mobile phones, cameras and hand held devices and monitoring their use and implementing current school policies with regards to these devices.

Designated Safeguarding Leaders

The Designated Safeguarding Leaders need to ensure that they are fully trained in online safety issues and are aware that there serious child protection issues could occur due to-

- Cyber- bullying
- Sharing of personal data
- Inappropriate online conduct with adults/ strangers
- Potential or actual incidents of grooming

Pupils/ Students

Pupils and students are responsible for-

- Knowing and acting accordingly to the school's Online Policy.
- Knowing the importance of reporting abuse, misuse or access to inappropriate materials and know how to report them.
- Knowing the policy on mobile phones, digital cameras and other hand held devices and to realise these can be used for cyber-bullying.
- Understanding that the E-Safety policy also covers their actions out of school, if related to their membership of the school.

At the start of each year, pupils will sign a class copy of these Internet safety rules. This will be displayed in class.

Key Stage 1 Rules

These rules help us to stay safe on the Internet

- We only use the internet when an adult is with us
- We can click on the buttons or links when we know what they do.

- We can search the Internet with an adult.
- We can write polite and friendly emails to people that we know

Key Stage 2 Rules

These rules help us to stay safe on the Internet

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with or if anyone asks for personal information.
- We immediately close any webpage we are not sure about.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not use Internet chat rooms.
- We understand that if we break the rules that sanctions will be taken.

Parents/ Carers

Parents and carers have the responsibility to ensure that their children use the internet and mobile phones correctly and do not misuse these technologies. They must be aware of the school's Online Safety Policy.

Other Users

Volunteers, including governors, who help in the school and who use information and communication technology systems and devices in helping the school are expected to:

- Participate in training of online safety provided by the school.
- Use information and communication technology in accordance with this policy and the training provided.
- Report any suspected misuse or problem to the person designated by the school for this purpose.

Curriculum

- All children will receive planned online safety lessons throughout Computing/ P.S.H.E / workshops and online safety assemblies and lessons. These lessons will be regularly revisited and revised to suit the new technologies in and out of school. Key messages will be delivered through a variety of assemblies to ensure all children are aware of the matter. They will also be made aware to question the validity of the information they find online.
- Parents will be able to find out more about online on the school's website and newsletters.
- Online issues will be reported to governors in termly HT reports.

Technical safety

At Cherry Orchard, all staff and pupils have access to the Internet. We use *Filtered Broadband* provided by RM to protect children from inappropriate websites and images. If any inappropriate data is viewed, staff are to report it to the network manager in the first instance or subsequently the DHT, who will then contact the provider.

Computer usage of staff and pupils is also monitored by the school using Securis software. This software helps protect students by monitoring, capturing and alerting on potentially harmful content or behaviour, thus allowing for intervention to stop inappropriate and potentially harmful computer use, whether it involves just looking or active participation. This is monitored by the Headteacher and a DSL who monitors the Headteacher. Any items of concern are logged and dealt with by the Headteacher or DSL. All users are reminded that any information that they view on a school machine can be logged on Securis.

The school uses Kaspersky anti-virus protection on all machines. The technical support team are responsible to remove any viruses that do infect computers.

Use of Digital Video and Images

The developments of digital images and videos have significant benefits within the curriculum and enhance learning. Image and videos can either be taken by staff and pupils for educational purposes or downloaded from the internet to support learning in the classroom. However, staff and pupils need to be aware of the risks associated with sharing images, especially via the internet. Staff and pupils need to be aware that once an image/ video is posted on the internet that it will remain there forever. This could cause harm or embarrassment in the future.

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Staff are allowed to take digital / video images to support educational purposes, 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 that when capturing images/ videos that all pupils concerned are appropriately dressed and not participating in activities that could bring either the pupils or the school into disrepute.
- Pupils' full names will not be used anywhere on the website or in blogs and particularly not associated with photographs on there.
- Parents are asked when their child begins school whether they wish for their child's pictures to be published on the school website, newsletter or Twitter. A record of this is sent to the class teacher (stored in the class register).
- Cherry Orchard Primary School will always comply with the Data Protection Act 1998 in regards to digital images and videos.

Reporting Online Safety issues

All children will be made aware of the importance to report any incident to either an adult at school that they can trust or the 'Online safety' button that is present on the school website, regarding any incidents that may occur outside of school.

If an online incident has occurred due to carelessness, this will be investigated and the correct sanctions will be implemented. All users within the school are aware that there is a monitoring system that is in place and is sensitive enough to pick up slight infringements regarding; cyber-bullying, searching for inappropriate content etc.

The following table indicates how different offences will be dealt with in regards to both pupils and staff. In all cases the Head Teacher when notified will decide what action to take and whether the incident needs further action, e.g. reporting to police, Local Authority.

Below is a table which outlines how communication devices are to be used by both staff and children at school. Some applications are permitted at certain times, but are strictly for education purposes. If there are any queries/ uncertainty please seek the guidance of the Head Teacher, DHT or DSL.

Acceptable Use

	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				/				/
Taking photos on use of hand held devices eg Samsung, Ipads	/						/	
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 e.g. Skype		/						/
Use of social networking sites				/				/
Use of blogs		/					/	

List of potential Incidents and Sanctions for Pupils

Incidents:	**Refer to class teacher**	**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 (possible time constraints)**	**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).		/			/	/	
Unauthorised use of non-educational sites during lessons		/			/	/	

Unauthorised use of mobile phone / digital camera / other handheld device	/	/			/	/	/
Unauthorised use of social networking / instant messaging / personal email		/			/	/	/
Unauthorised downloading or uploading of files		/		/	/	/	/
Allowing others to access school network by sharing username and passwords	/	/		/	/	/	/
Attempting to access or accessing the school network, using another student's / pupil's account	/	/		/	/	/	/
Attempting to access or accessing the school network, using the account of a member of staff	/	/		/	/	/	/
Corrupting or destroying the data of other users	/	/		/	/	/	/
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	/	/		/	/	/	/
Continued infringements of the above, following previous warnings or sanctions		/		/	/	/	/
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		/	/		/	/	/
Using proxy sites or other means to subvert the school's filtering system		/		/		/	/
Accidentally accessing offensive or pornographic material and failing to report the incident		/		/			
Deliberately accessing or trying to access offensive or pornographic material		/	/	/	/	/	/

List of potential Incident and Sanctions for Staff

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 (verbal / Written /final)	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable /		/	/					/

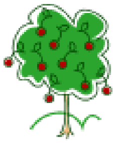
inappropriate activities).								
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	/	/	/		/	/	/	/
Unauthorised downloading or uploading of files	/	/				/		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person’s account	/	/				/		
Careless use of personal data eg holding or transferring data in an insecure manner	/	/	/			/		/
Deliberate actions to breach data protection or network security rules		/	/			/		/
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		/				/		/
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		/	/	/				/
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		/	/			/	/	/
Actions which could compromise the staff member’s professional standing		/				/		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		/	/					/
Using proxy sites or other means to subvert the school’s filtering system		/	/			/		

Accidentally accessing offensive or pornographic material and failing to report the incident	/	/				/		
Deliberately accessing or trying to access offensive or pornographic material		/	/				/	/
Breaching copyright or licensing regulations		/				/		
Continued infringements of the above, following previous warnings or sanctions		/	/					/

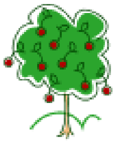
This policy is reviewed annually. Read in conjunction with mobile phone and behaviour policies.

A Taylor, E Emery, A Jaswal

December 2016



Staff Acceptable Use Policy



- I will only use the school’s digital technology resources and systems for Professional purposes or for uses deemed ‘reasonable’ by the Head and Governing Body.
- I will not allow unauthorised individuals to access email / Internet / intranet /network, or other school / LA systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school’s network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved school email, or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school’s information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I understand that failure to comply with this agreement could lead to disciplinary actions.

User Signature

I agree to abide by all the points above.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school’s most recent online safety policies.

Signature: ______________________________ Date: _________________________

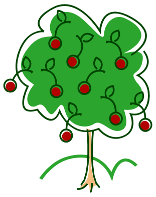
Full Name ____ (printed)

Authorised Signature (Head Teacher (primary) / Head/Deputy/ senior teacher

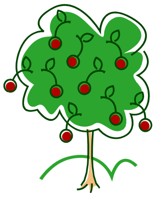
I approve this user to be set-up.

Signature: ______________________________ Date: _________________________

Full Name :____(printed)



Online Safety Incident Log



No:	Reported by:	Reported to:
	When:	When:

Description of incident:

Signed: ____

Result of enquiry/Action taken:

Signed: ____