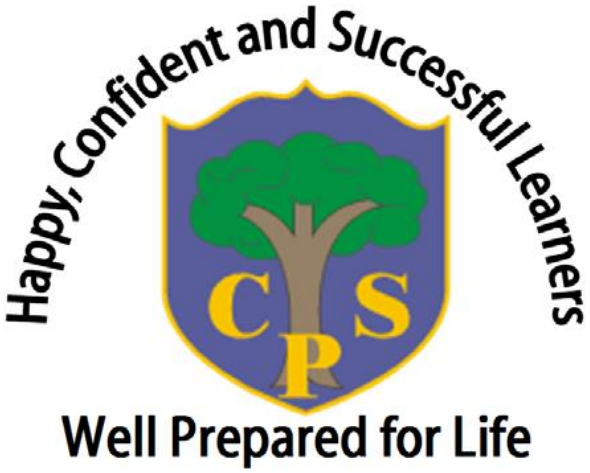

The Coppice Primary School
ICT Acceptable Usage Policy

Written by	
Approved by Trustees	February 2016
Date for Review	February 2019

Purpose
This policy relates mainly to the school's Internet facility. The purpose of the policy is to protect pupils from undesirable materials on the Internet, to protect them from undesirable contacts over the Internet, and to prevent unacceptable use of the Internet by children or adults.
The policy also addresses issues of copyright for materials published on the Internet.

Definitions

Undesirable materials:
Pornographic images or obscene text on Internet web sites
Language that is abusive, profane, inflammatory, coercive, defamatory, blasphemous or otherwise offensive, on Web sites or e-mail messages
Racist, exploitative or illegal materials or messages on Web Sites or e-mail

Undesirable contacts:
E-mail messages from unknown or unverified parties, who seek to establish a child's identity and/or to communicate with them, such as for advertising or potentially criminal purposes.

Unacceptable use:
Deliberate searching for and accessing of undesirable materials
Creating and transmitting e-mail messages that contain unacceptable language or content
Creating and publishing on the Internet materials that contain unacceptable language or content.

Adults:
School teaching staff
Non-teaching school staff
Visitors and guests of the staff
Parents

Unintentional Exposure of children to undesirable materials
It is the school's policy that every reasonable step should be taken to prevent exposure of children to undesirable materials on the Internet. It is recognised that this can happen not only through deliberate searching for such materials, but also unintentionally when a justifiable Internet search yields unexpected results. To prevent such occurrences, the School has adopted the following position:

The use of an Internet Service Provider which offers protection by:
- the filtering of sites by language content with prohibition of sites with unacceptable vocabulary
- the imposition of a banned list of undesirable sites

In-school protection by:
- adult supervision of pupils' internet activity, with direct supervision of all computer use
- regular use of monitoring software to review computer and specifically internet usage (Policy Central)
- pupil awareness of safe use and the e-safety agreement – a relevant summary of the requirements of this document.
- regular review of this policy

In the event of children being unintentionally exposed to undesirable materials the following steps will be taken:
1. Pupils should switch off their monitor and notify a teacher immediately.
2. The teacher will ensure no pupils can see the monitor and will write down the website, date and nature of the material. The website can then be logged off.
3. The teacher will inform the Computing Coordinator who will ensure the website is filtered out.
4. The teacher will record the incident in a central log, by which the school may be able to reliably report the frequency and nature of any incidents.
5. Parents or Governors will be notified at the discretion of the Head according to the degree of seriousness of the incident.

Pupils will be taught as part of the curriculum to use the internet safely and thoughtfully.

Intentional Access of Undesirable Materials by Children
Children must never intentionally seek offensive material on the internet. Any transgression should be reported and recorded as above. Any incident will be treated as a disciplinary matter and the parents of the child or children will normally be informed.

If deliberate access to undesirable materials is found to be repeated, flagrant or habitual, the matter will be treated as a serious disciplinary issue. The child's parents will be informed and the Governing Body will be advised.

Deliberate Access to Undesirable Materials by Adults
Deliberate access to undesirable materials by adults is unacceptable and will be treated as a disciplinary issue. If abuse is found to be repeated, flagrant or habitual the matter will be treated as a very serious disciplinary issue. The Governors will be advised and the LA will be consulted. The school's Discipline Policy will be applied accordingly.
All adults will agree and follow the adult e-safety agreement as well as have a full copy of this policy.

Receipt and transmission of e-mails by Children
It is recognised that e-mail messages received or transmitted by children can contain language or content that is unacceptable. It is also recognised that some people may try to use e-mail to identify and contact children for unacceptable reasons.

To avoid these problems the School has adopted the following practice:
Pupils do not have access to e-mail except in teacher-controlled situations
Pupils do not read external e-mail messages unless an adult is present or the message has been previewed by a teacher

Steps are taken to verify the identity of any school or child seeking to establish regular e-mail with this school
Pupils never send an e-mail message without permission
To avoid children revealing their identification within e-mail messages the child's address is never revealed.

If staff believe that children have been targeted with e-mail messages by parties with criminal intent the message will be retained, the incident recorded and the Governors and the child's parents informed. Advice will also be given regarding further steps.

Publishing of materials on the Internet
It is recognised that staff and children may at some time produce and publish materials on an Internet Web site associated with the school or the LA.
No materials will be published on the Internet which contains any unacceptable images, language or content. Infringement of this rule will be taken as a serious disciplinary issue.
No materials will be published on the internet which reveals the identity of any child.
Parents will be asked for approval to published pupil's photographs on the internet.
Staff publishing materials on sites that do not link to school (e.g. Facebook) need to be certain that what they do is appropriate to their professional standing, and they certainly should not be publishing anything that brings the school or themselves into disrepute.
Anything that children publish on websites away from school that causes distress to others in school will be dealt with by applying our Behaviour Policy and Ant-Bullying Policy.

Use of the Internet by staff and adult users
It is expected that staff will also adhere to a code of responsible use of the internet and computers belonging to the school. Staff are expected to read and keep to the Policy on acceptable internet use for staff and adult users. Chat rooms and social networking sites should not be used in school unless as part of specific curriculum content supervised by a teacher.

Use of the School Internet by Visitors and Guests
Members of school staff will take responsibility for the actions of any adult guests or visitors who they allow or encourage to use the school Internet facilities. The essential "dos and don"ts" of this policy should be explained to such visitors and guests prior to their use of the internet.
Unacceptable use will lead to the immediate withdrawal of permission to use the school Internet facility.

Copyright Issues
It is recognised that all materials on the internet are copyright, unless copyright is specifically waived. It is the school's policy that the copyright of Internet materials will be respected.
Where materials are published on the internet as part of the teacher's professional duties, copyright will remain with the County Council. Materials published on school web sites will contain due copyright acknowledgements for any third-party materials contained within them.

Mobile Internet Use
The school currently has a policy of no mobile phones allowed in school, apart from in Year 6 where it is expected that they will be handed in at the beginning of the day and returned at the end. If phones are discovered they may be confiscated. There are certain circumstances when mobiles may be allowed. Permission may be granted for instance on school trips and sporting activities. Pupils are advised to use their phones in this case appropriately and reminded they should still keep to the e-safety agreement.

Personal phones
We recognise that the area of mobile technology is rapidly advancing and it is our school's policy to review its stance on such technology on a regular basis. Currently our policy is this:

- *Members of staff are permitted to bring their personal mobile devices into school. They are required to use their own professional judgement as to when it is appropriate to use them. Broadly speaking this is:*
    - ✓ *Personal hand held devices will be used in lesson time only in an emergency or extreme circumstances*
    - ✓ *Members of staff are free to use these devices outside teaching time.*
    - ✓ *A school mobile phone is available for all professional use (for example when engaging in off-site activities) and members of staff should not use their personal device for school purposes except in an emergency.*
- *Apart from the exceptions mentioned above, pupils are not currently permitted to bring their personal hand held devices into school.*

Monitoring
The school has software designed to record and monitor inappropriate computer use across the network (Policy Central). The records are checked twice a week and details are recorded and passed onto the Computing Coordinator to sort and action. Pupils will be warned of minor offences and a record kept. Parents will be contacted if the offence is more serious and the pupil may receive a ban from the computers. Staff use will also be monitored.

Data Protection Statement

The procedures and practice created by this policy have been reviewed in the light of our GDPR Data Protection Policy.

All data will be handled in accordance with the school's GDPR Data Protection Policy.

Name of policy	Content	Reason for policy	Who does it relate to?	Where is it stored?
ICT Acceptable Usage Policy	Guidelines for Acceptable ICT Usage	To provide clarity	Pupils & Staff	Secure Network drive

As such, our assessment is that this policy:

Has Few / No Data Compliance Requirements	Has A Moderate Level of Data Compliance Requirements	Has a High Level Of Data Compliance Requirements
√		