Hoyle Court Primary School believes that every child is a learner and can achieve.

E-Safety Policy		
COMPILED BY: B Dickinson	DATE APPROVED: 24/10/2024	DATE TO BE REVIEWED: 24/10/2025

This policy is to be read alongside our Child Protection Policy, Safeguarding Policy, Staff code of conduct and Staff Disciplinary and Procedure policy.

Rationale

New technologies have become integral to the lives of children and young people in today's society, both within school and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. 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. 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 the subject of 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.

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

As a result, designing and implementing an E-safety Policy demands the involvement of a wide range of interest groups: the governors, headteacher, SLT, SENCO, DSL, classroom teachers, support staff, young people and parents, LA personnel, internet service providers (ISP), and regional broadband consortia, working closely with ISPs on network security measures.

E-safety is a child protection issue, and indeed it should not be managed primarily by the Computing team. It should be an extension of general safeguarding and led by the same people, so that, for instance, cyber bullying is considered alongside real-world bullying. As a result, there will be close involvement from the designated safeguarding governor in the monitoring of this policy.

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at school with respect to the use of ICT-based technologies.
- Monitor and respond to e-safety incidents.
- Aid the prevention of e-safety issues through education of staff, pupils and parents.
- Have clear structures to deal with online abuse, such as online bullying, which are cross referenced with other school policies.
- To evaluate and improve the whole school approach to e-safety.

Monitoring the impact of the policy

In order to maximise the effectiveness of this policy, the Computing Subject Lead will monitor the impact of the policy using logs of reported incidents recorded on CPOMS which will be reviewed by the Computing Subject Lead regularly.

- Staff and student's understanding of e-safety which will be gathered by the Computing Subject Lead through the use of pupil interviews or questionnaires. Progress will be monitored at the end of each academic year.
- Additional monitoring may be carried out by the Computing Subject Lead and Safeguarding governor using the checklist of e-safety evidence (see appendix 5).

Roles and responsibilities

Headteacher and Senior Leaders

The Headteacher and senior leaders are responsible for:

- Ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the Computing Subject Lead.
- Ensuring that the Computing Subject Lead and other relevant staff receive suitable continuous professional development (CPD) to enable their e-safety roles to be carried out and to train other colleagues, as appropriate.
- Ensuring that in the event of an e-safety allegation being made against a member of staff, the correct procedures are followed, and as detailed in the Child Protection policy.

Computing Subject Lead

The Computing Subject Lead is responsible for:

- The day to day management of e-safety issues and has a leading role in establishing and reviewing the school e-safety policy.
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Reviewing reports of e-safety incidents and ensuring any appropriate and necessary action is taken including contacting outside services where relevant.
- Providing SLT and the governors with a termly summary report detailing preventative actions taken and any relevant incidents and action points.

Teaching and Support Staff

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.
- They have read, understood and signed the Staff Acceptable Use Policy (appendix 2).
- They follow the correct procedures to deal with any e-safety incidents, using the E-safety incident procedure (see appendix 4).
- E-safety incidents are reported to the Computing Subject Lead for investigation using CPOMS.
- Digital communications with students/pupils (including online communications) are 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 school activities.
  E-safety lessons are taught through the Project Evolve scheme.
- Students/pupils understand and follow the school e-safety and Pupil Acceptable Use Policies. (see appendix 1). This includes monitoring pupils' access to ICT equipment and the internet and ensuring its responsible use.
- They are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.

Other members of staff, *e.g.* lunchtime supervisors, are also responsible for reporting any e-safety incident to the relevant member of staff and also sign to say they have read the Social Media and ICT Policy.

Named persons for child protection

The school's named persons for child protection are trained in e-safety issues and are 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.
- Cyber-bullying.

Technical staff

Bluebox IT are our current technical support company. Our contract provides one half day of support per week. The technician ensures:

- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- That monitoring software and anti-virus software is in place and up-to-date.

Children

The children in school are responsible for:

- Using school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems (see appendix 1).

Parents/carers

The school will take every opportunity to help carers/parents to understand issues related to e-safety. The school is registered with the Child Exploitation and Online Protection (CEOP) Centre's 'Think U Know' website, an internationally accredited organisation working to promote e-safety principles. In line with their recommendations, we will encourage parents to understand key issues, and how they can minimise the risk to their children, in the following ways:

- Parent/carer e-safety presentations.
- Regular newsletters to offer parents advice on the use of the internet and social media at home.
- CEOP published documentation displayed around school and on the school website.
- Parents are informed of our e-safety rules and are asked to discuss the pupil AUP (Acceptable Usage Policy) with their children.

Community users

Community users/visitors and volunteers will inform a member of staff of any websites they wish to access. No person can log on to the internet without a user account or the Internet password.

Education

Pupils' education

The education of pupils in e-safety is 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 resistance to such risks. E-safety education will be provided in the following ways:

- A planned e-safety programme is delivered as part of our Computing curriculum.
- Key safety messages are reinforced as part of a planned programme of assemblies. They take place at the start of each academic year and to celebrate Safer Internet Day in February.
- Rules for use of ICT systems will be posted in all rooms and where there is access to the Internet.

- 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. Evaluation and cross referencing of sources is covered in the new computing curriculum.
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet. Copyright free audio and image sources are detailed in the new Computing curriculum.

Staff training

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:

- The e-safety training needs of staff will be carried out by the Computing Subject Lead.
- All new staff will be introduced to the school e-safety policy and Acceptable Use Policies as part of their induction programme.
- Staff development meetings will be delivered to ensure teaching staff have an up-to-date understanding of e-safety at Hoyle Court Primary School.
- The Computing Subject Lead is registered with the Think U Know website and will receive regular updates on good practice through the CEOP website and emails.

Internet provision

The school Internet is provided by Bluebox IT. All sites are filtered using a filtering system which also can be used to generate reports on user activity. Should staff or pupils gain access to any website(s) which they feel should be blocked; this should also be reported to the Computing Subject Lead in order for access to the website(s) to be restricted.

Use of digital photos and video

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, using, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images online.
- Staff are allowed to take digital/video images to support educational aims. Those images should only be taken on school equipment. The personal equipment of staff should not be used for such purposes.
- Photographs of children published on the website must not contain children's full names.
- Permission from parents or carers will be obtained before photographs of students/pupils are published on the school website (signed on enrolment to school).

Data Protection

- Staff must ensure that they take care to ensure the safe keeping of personal data (including photos and video), minimising the risk of its loss or misuse, in line with the school's data protection policy.
- Staff must ensure passwords remain private and lock their computer when leaving it unattended.
- Password protected, encrypted memory sticks are provided by school in order to ensure data stored externally is also secure.

Passwords

Members of staff will receive a personal username and password during induction. From
KS2, pupils will also use an individual username and password to access school systems. KS1 children will have an individual username and generic password. All users (adults and pupils) have a responsibility for the security of their username and password which is outlined in both staff and pupil AUPs. They must:

- Not allow other users to access the systems using their log on details
- Immediately report any suspicion or evidence that there has been a breach of security to the Computing Subject Lead

Appendix 1

Pupil Acceptable Use Policy

This document has been developed to help you understand the rules of using computers in school. You should always follow the rules set out in this policy because these rules will help keep you and your classmates safe. The term 'ICT equipment' includes but is not limited to iPod touches, iPads, netbooks and laptops.

I will follow these rules to keep me safe:

- ✓ I will not purposefully damage any school-owned ICT equipment.
- ✓ I will only use the Internet with my teacher's permission.
- ✓ I will only use the school's ICT equipment for school work as directed by the teacher.
- ✓ I will only log onto school systems as myself.
- ✓ I will keep passwords used to log onto school systems private.
- ✓ I will tell my teacher straight away if see something that I feel uncomfortable with or upsets me.
- ✓ I will not give out my personal details such as my name, phone number, home address or school.
- ✓ I will be responsible for my behaviour when using ICT in school or at home because I know that these rules are to keep me safe.
- ✓ I will make sure ICT communication with other pupils is polite and responsible.
- ✓ I will not deliberately look for, save or send anything that could be upsetting or unkind.
- ✓ I will not try and get to any websites that the school has blocked access to.
- ✓ I will not use any personal device (including cameras and mobile phones) in school.
- ✓ I understand that my use of school equipment, including activity when using the Internet, is monitored and that my parent/carer will be contacted if a member of school staff is concerned about my safety.

Agreement

I agree to follow the rules set out in this AUP. I know that if I break any of these rules my use of ICT equipment may be suspended and my parent/carer may be told.

Pupil name: ……

Signed: ……

Date: ……

Appendix 2

Staff Acceptable Use Policy

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this Acceptable Use Policy. For further information or clarification, please contact the Computing Subject Lead.

Under the Regulation of Investigatory Powers Act (2000) the school can exercise the right to monitor the use of the school's information systems and internet access where it is believed that unauthorised use may be taking place, to ensure compliance with regulatory practices, to ensure standards of service are maintained and to prevent or detect crime.

Internet Use

- ✓ I will not attempt to access inappropriate or illegal material in school.
- ✓ I will report to the Computing Subject Lead or Bluebox, access to any inappropriate websites that I feel should be blocked.
- ✓ I will only use the internet for personal use during out-of-school hours, including break and lunch times.

Data Protection

- ✓ I will ensure that any personal data is stored in line with the GDPR. (Policy available on request).
- ✓ I will respect system security and I will not disclose any password or security information to anyone other than on request from an authorised system manager (including but not limited to the Computing Subject Lead, Business Manager and external technical support provider).
- ✓ I will only use encrypted USB sticks provided by school and will ensure that pupil data is stored securely and is used appropriately.
- ✓ I will take reasonable precautions to ensure that any devices (laptops, tablets, cameras) are stored in a secure manner when taken off site *e.g.* not left in a car overnight.
- ✓ I will ensure any sensitive personal data is not transferred to a personal device unless completely necessary – and, when doing so, that it is encrypted.
- ✓ I will not use any personal device (including cameras and mobile phones) to capture images, videos or audio of pupils.
- ✓ I will not install any software (including mobile apps) or hardware without permission from the Computing Subject Lead

E-Safety

- ✓ I will report any incidents of concern regarding children's safety whilst using ICT equipment in or out of school to the Computing Subject Lead.
- ✓ I will promote e-safeguarding with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

Social Media

Employees are advised that they set the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy. Employees should keep their passwords confidential, change them often and be careful about what is posted online. Employees also should not identify themselves as employees of the school on social networking sites.

- ✓ I will not talk about my professional role when using personal social media such as Facebook and Twitter.
- ✓ I will not have any contact with pupils' family members through personal social media if that contact is likely to constitute a conflict of interest or call into question their objectivity.
- ✓ I will ensure that my activity on social networking sites does not conflict with or affect my professional duties.
- ✓ I will not post or upload any images and videos of pupils, staff or parents on any online website without consent from the individual(s) in the images or videos.

Email

- ✓ I will use my school email address for all correspondence with staff, parents or other agencies.
- ✓ I understand that use of the school email system may be monitored and checked.
- ✓ I understand that I must report any known breaches of this policy, including any inappropriate images or other material which may be discovered on the school's ICT systems, to the Computing Subject Lead.
- ✓ I understand that any breach of this policy or of other school policies relating to the use of ICT equipment may result in disciplinary action in line with the school's established disciplinary procedures.

Signed _____ Date _____

Print name _____

Appendix 3


Childnet International
BE SMART ONLINE
S
SAFE
Keep your personal information safe. When chatting or posting online don't give away things like your full name, password or home address. Remember personal information can be seen in images and videos you share too. Keep them safe to keep yourself safe.
M
MEET
Meeting up with someone you only know online, even a friend of a friend, can be dangerous as this person is still a stranger. If someone you only know online ever asks you to meet up, for personal information or for photos/videos of you then tell an adult straight away and report them together on www.thinkuknow.co.uk
THINK U KNOW
A
ACCEPTING
Think carefully before you click on or open something online (e.g. links, adverts, friend requests, photos) as you never know where they may lead to or they may contain viruses. Do not accept something if you are unsure of who the person is or what they've sent you.
R
RELIABLE
You cannot trust everything you see online as some things can be out of date, inaccurate or not entirely true. To find reliable information compare at least three different websites, check in books and talk to someone about what you have found.
T
TELL
Tell a trusted adult if something or someone ever makes you feel upset, worried or confused. This could be if you or someone you know is being bullied online. There are lots of people who will be able to help you like your teachers, parents, carers or contact Childline – 0800 11 11 or www.childline.org.uk
BE SMART WITH A HEART
Remember to always be smart with a heart by being kind and respectful to others online. Make the internet a better place by helping your friends if they are worried or upset by anything that happens online.
WWW.CHILDNET.COM

Appendix 4

innovation centres

Bradford District Council
www.bradford.gov.uk

This short guide explains to adults in school the procedure when illegal or inappropriate material is discovered on a device. If you suspect or discover any other (e) safeguarding incident such as individuals contacting children online, cyber bullying, inappropriate actions, breach of copyright or loss of data then consult your (e) safeguarding officer as soon as possible.

Actions upon discovering inappropriate or illegal material.

1. Remove the device from the sight of children.

If it's a web site do not close any browser windows. Do not shut the device down.

2. Preserve the evidence.

If the image contains child abuse do not copy it.
Take screenshots of the page in question unless the image involves child abuse. On a PC press the print screen button and paste into a word document. Save this document to a location identified by your E Safeguarding officer. Make sure the document is not stored on a device / location accessible to children.
On an iPod or iPad hold down the home key and power key at the same time to take a screenshot. Go to your photo roll and email the screenshot to a secure email (never a personal account).

3. Inform the E safeguarding officer.

4. Write the incident in the e safeguarding log as soon as possible.

Innovationcentres.org.uk

Appendix 5

In line with the Ofsted publication 'Inspecting e-safety' April 2013, these questions are to be used by a member of staff to evaluate the impact of the e-safety policy.

Qs for children	If you felt uncomfortable about anything you saw, or if anybody asked you for your personal details such as your address on the internet would you know who to tell?
	Can you tell me one of the rules your school has for keeping safe online?
Qs for staff	Can you tell me one of the staff AUP rules?
	How would you report a concern regarding e-safety?