

Highfield CE Primary School

E-Safety Policy 2026 - 2028



Approved by: The Governing Body **Date:** 15.7.2026

Last reviewed on: June 2026

Next review due by: June 2028

Legal Framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2025) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2024) 'Keeping children safe in education 2024' (KCSIE)
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- DfE (2025) 'Generative artificial intelligence in education'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2024) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people (updated March 2024)'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2020) 'Small Business Guide: Cyber Security'

Introduction

"All agencies providing services to children have a duty to understand e-safety issues, recognising their role in helping children to remain safe online while also supporting adults who care for children"

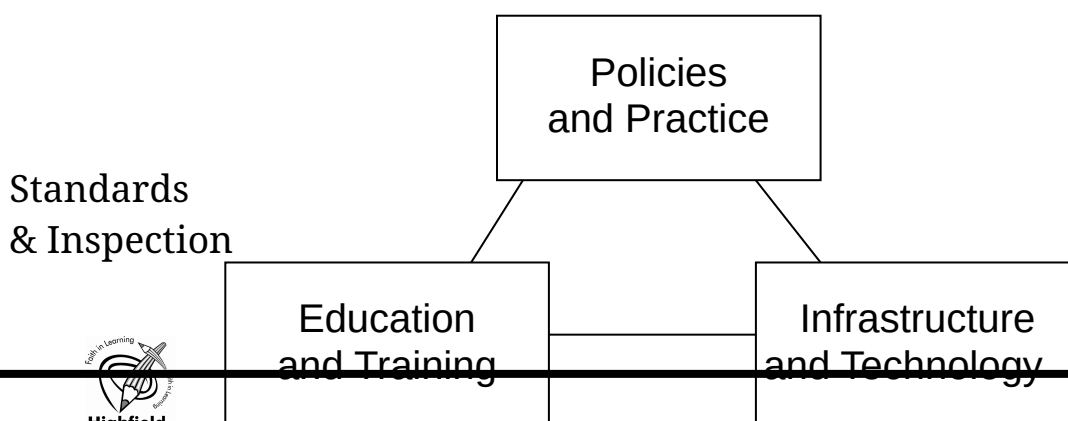
(from Safeguarding Children in a Digital World)

Effective Practice in e-Safety

E-Safety depends on effective practice in each of the following areas:

- Education for responsible ICT use by staff and pupils;
- A comprehensive, agreed and implemented e-Safety Policy;
- Secure, filtered broadband from the County Council (HPSN2);
- A school network that complies with the National Education Network standards and specifications.

PIES Model for Limiting E-Safety Risks



Becta 2008 - Safeguarding Children in a Digital World

E-Safety is the process of limiting risks to children and young people when using Information and Communication Technology (ICT). E-Safety is primarily a safeguarding issue not a technological issue which relates to the use of all ICT - fixed or mobile; current, emerging and future ICT.

ICT is used daily as a tool to improve teaching, learning, communication and working practices to the benefit of our children and young people and those that work to support them. The use of ICT is recognised as being of significant benefit to all members of our community, in personal, social, professional and educational contexts. However, alongside these benefits are potential risks that we have a statutory duty of care to manage, to ensure they do not become actual dangers to children and young people in our care or for employees.

At Highfield C.E. Primary we have a policy in place which considers the following issues:

- the acceptable use of ICT by all users;
- e-safety procedures, e.g. incidents of misuse of ICT by users, safeguarding incident when a user is at risk of or has come to actual harm through the use of ICT;
- e-safety training for staff and pupils;
- the technology available to users, its security features and settings, e.g. virus protection, filtering and monitoring;
- a named person with responsibility for e-safety which should ideally be a member of the senior leadership team and is not necessarily the ICT co-ordinator as e-safety is primarily about safeguarding and not the technology itself. This would be the DSL.

For Highfield C.E. Primary School the named person with overall responsibility for e-safety is Mrs Rosie Walford (Headteacher). This involves being responsible for:

- Taking the lead responsibility for online safety in the school.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT technicians.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.
- Understanding the filtering and monitoring processes in place at the school.
- Providing specialist knowledge in relation to filtering system management, e.g. the content and websites pupils should and should not be able to access.

- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.

Other Roles and Responsibilities:

- Delegated responsibility for e-City; Internet and developing/implementing pupil email and internet codes of conduct, as well as keeping up to date with apps and trends that may affect children to Mrs Rachael Bond (Deputy Headteacher) and Mr Joe Rawlins (ICT Leader).
- Delegated responsibility for website content; internet infrastructure; filtering; data procedures to Harrap (School ICT Technical Support Team).
- Delegated responsibility for maintaining pupil image consents; managing signed staff and pupil codes of conduct and mobile phone agreements to Mrs C Donnachie (School Business Manager).

The term 'staff' is used as a broad term within this policy and includes every adult who works on the school site, as well as volunteers and governors.

Highfield C.E. Primary School's e-Safety Policy will cover the safe use of internet and electronic communications technologies such as mobile phones and wireless connectivity. The policy will highlight the need to educate children and young people about the benefits and risks of using new technologies both in and away from school. It will also provide safeguards and rules to guide staff, pupils and visitors in their online experiences.

E-Safety Risks & Issues

E-Safety risks and issues can be roughly classified into three areas: content, contact and commerce. The following are basic examples of the types of e-safety risks and issues that could fall under each category.

Content:

- Exposure to age-inappropriate material
- Exposure to inaccurate or misleading information
- Exposure to socially unacceptable material such as that inciting violence, hate or intolerance
- Exposure to illegal material, such as images of child abuse
- Downloading of copyrighted materials, e.g. music and films
- Plagiarism
- Interaction with AI-powered platforms that generate misleading or unsafe content, including false news, inappropriate text, or images not suitable for primary-aged pupils

Contact:

- Grooming using ICT, leading to sexual assault and/or child prostitution
- Bullying using ICT (email, mobile phones, chat rooms etc)

- Children and young people self-publishing information - sometimes inappropriate - about themselves and therefore putting themselves at risk
- Interacting with AI chatbots or anonymous users in online games that may expose children to risk or misinformation

Commerce:

- Exposure to inappropriate commercial advertising
- Exposure to online gambling services
- Commercial and financial scams
- Unregulated in-app purchases or loot boxes in online games that encourage spending real money

Infrastructure & Technology

It is recommended that all organisations providing services to children and young people use an accredited service supplier to deliver filtered internet access, configured to their own local circumstances and requirements.

Under the accreditation scheme, a product for filtering internet content must meet or exceed the following requirements:

- There must be telephone and web-based support for all aspects of the service.
- The product must block 100 per cent of illegal material identified by the Internet Watch Foundation (IWF) Child Abuse Images and Content (CAIC) URL List.
- The product must be capable of blocking 90% of inappropriate content in each of the following categories:
 - Pornographic, adult, tasteless or offensive material
 - Violence (including weapons and bombs)
 - Racist, extremist and hate material
 - Illegal drug taking and promotion
 - Criminal skills and software piracy
- It must be possible to request (or make) amendments to the blocked content.

Firewall protection is provided by Coconnect for computers connected to the school's network. It is the school's responsibility to ensure that anti-virus and anti-malware systems are installed and that the definition files are updated regularly on all school machines to maintain protection.

Monitoring Systems – to keep track of who downloaded what, when and on which device. This information can be made available from the Internet Service Provider.

Filtering and content control is provided by Coconnect – please see our Filtering and Monitoring Policy

Teaching and Learning

Why the Internet and digital communications are important

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. Pupils will be shown how to publish and present information to a wider audience.

Pupils will be taught how to evaluate Internet content

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Pupils will be taught the importance of cross-checking information before accepting its accuracy. Pupils will be taught how to report unpleasant Internet content.

Managing Internet Access

Information system security

School ICT systems security will be reviewed regularly. Virus protection will be updated regularly. Security strategies will be discussed with the Local Authority.

Internet Code of Conduct

- Pupils should be supervised at all times when using the Internet. Independent pupil use of telecommunications and electronic information resources is not permitted at Highfield C.E. Primary. Access to school network must be with a unique class user name and password, which must not be made available to any other staff member or pupil.
- All Internet activity should be appropriate to staff's professional activity or the student's education. Netsweeper reports are produced by Coconnect and we receive weekly student and Staff reports of any inappropriate searches and we receive 1-minute alerts for students who are making inappropriate searches. This is added to CPOMS as it is a safeguarding issue.
- Staff may use their Internet facilities for non-business research or browsing during meal time breaks, or outside of work hours, provided that all other Internet usage policies are adhered to.
- Internet activity that threatens the integrity or security of the school's ICT systems, or activity that attacks, corrupts, or threatens the security of other organisations' systems, is prohibited.
- Copyrights, software licensing rules, laws of the land, property rights, privacy and the rights of others must be respected and adhered to at all times.
- The Internet must not be used to access, display, store, transmit, distribute, edit or record inappropriate sites such as those containing pornographic, violent, racist, discriminatory, criminal skills related, illegal drugs related or offensive material. Users will recognise materials that are inappropriate and, if deliberately accessing them, should expect to have their access removed.
- The Internet must not be used to download entertainment software or games, or play games against other Internet users.
- Uploading materials or files to City Council systems must only be performed on machines that have virus protection to the latest corporate standards and with appropriate authorisation from the relevant departments. This is done via the appropriate encrypted system, i.e. Anycomms.
- Downloading of files to school systems using ftp, email and http must be carried out with an appropriate level of care and thought. Problems arising from the installation of

files, utilities and software updates obtained by such methods are the school's responsibility unless directed to do so by representatives of the City Council or their agents. Virus infection and subsequent removal caused by such methods on machines without protection to the latest corporate standards will be the school's responsibility.

- The Internet must not be used to engage in any activity for personal gain or personal business transactions.
- The Internet must not be used to conduct or host any on-going non-education related activities, including discussion groups, chat lines, newsgroups or any other form of on-line club.
- The Internet must not be used for personal or commercial advertisements, solicitations or promotions.
- The use of a computer system without permission or for a purpose not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990.
- To ensure compliance with the acceptable use policy for Web browsing and email the school reserves the right to monitor and record activity in these areas. All users should therefore have no expectation of privacy in respect of their web browsing and email activities when using the school's computer facilities.

Email Code of Conduct

- Access to email should only be via the authorised user name and password, which must not be made available to any other staff member or pupil.
- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Normally, access to another staff user's email account will not be granted to anyone. However, there are occasions when such access may be legitimately needed, e.g. To aid investigation of suspected irregularities; upon summary dismissal of an employee; during suspension or prolonged absence of an employee; where the retrieval of information is necessary to allow continuation of work in hand by the user whose ID/password combination is to be circumvented.
- Attachments from unknown sources should not be opened, but deleted immediately. All attachments should be scanned for viruses.
- Schools are responsible for all email sent and for contacts made that may result in email being received.
- Pupils must not send or publish their personal details in an email to an unknown recipient
- Posting anonymous messages and creating or forwarding chain letters is forbidden.
- As email can be forwarded or inadvertently sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.
- Messages that contain abusive or objectionable language, that libel others, or that infringe the privacy rights of others are forbidden.
- Changes must not be made to other people's messages that are then sent on to others without making it clear where the changes have been made.
- Users must not pretend that they are someone else when sending email, or use someone else's account to send a message.
- Users must not publish, electronically or otherwise, any school email address as a point of contact for non-education related activities.
- Personal or otherwise sensitive data must not be transferred via email.

Social Networks, Chat Rooms, Instant and Text Messaging Code of Conduct

The school will control access to social networking sites, and consider how to educate pupils in their safe use. Newsgroups will be blocked unless a specific use is approved. Ideally, pupils would use only moderated social networking sites. Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils, and the age restrictions for signing up to these networks.

- Pupils should only be given access to secure, age-appropriate chat rooms and social networks, which are moderated by a teacher, or other recognisable, identifiable and approved e.g. Showbie as this is monitored by staff.
- The use of such websites should be permitted only within an educational or professional context.
- Teachers should familiarise themselves with any chat room that may be used in school, to ensure that it offers a genuine educational experience.
- Pupils should be supervised at all times when using such websites.

- Pupils should be taught to understand the importance of personal safety on the Internet, i.e. taught never to give out personal contact information or to arrange to meet someone they have met online.
- Access to internet related services such as instant messaging, chat services and social networks is commonplace outside of the school environment. Many young people own, or have access to mobile phones which now commonly provide online access. For this reason, schools will need to ensure that pupils are taught safe and responsible behaviours whenever using ICT.
- All staff should be aware of the Highfield C.E. Primary guidelines for the use of social networking sites. The guidelines are in place to protect staff, volunteers and governors from allegations of professional misconduct in their use of networking sites at all times in connection with school matters **(see Appendix A)**.

Published content and the School Website Code of Conduct

Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office. The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

- The school website will be accessed via the home page:
www.highfieldceprimaryschool.co.uk
- The production and publication of any unofficial websites is strictly forbidden and, if undertaken will be actively pursued by the City Council for removal on behalf of the school.
- Only designated staff member(s) within the school may authorise the uploading of material to the school website and all material for the website must be monitored and approved by the person(s) responsible. In Highfield C.E. Primary School this named designated person is Mrs Walford (Headteacher). The user name and password must not be given to any other members of staff or pupils. If other people know this information, the school should immediately contact CSL ICT Strategy telephone 023 8083 2111 or email: csl.ict@southampton.gov.uk to have the password changed.
- Images of pupils and staff should be classed as personal data under the terms of the UK GDPR and Data Protection Act of 2018. Therefore, using such images for school publicity purposes, i.e. school web site will require the consent of either the individual concerned or in the case of pupils, their legal guardians.
- Full names, addresses, telephone numbers and email addresses of pupils must not be published on the school website. Home addresses and telephone numbers of school staff, parents and governors should not be published on the school website, where possible the school details should be given as the main point of contact.
- Southampton City Council and Hampshire County Council reserve the right to ask for any material to be removed from school websites if it is considered to be unsuitable or if it poses a threat to the safety of a school or pupil. Individual support and guidance on developing school websites is available from CSL ICT Strategy telephone 023 8083 2111 or email csl.ict@southampton.gov.uk.

Publishing Pupils' Images and Work Code of Conduct

- Photographs that include pupils will be selected carefully so that their image cannot be misused.
- Written or electronic (via online form) permission from parents or carers will be obtained before photographs of pupils that may include their full names, are published on the school Web site.
- Work can only be published with the permission of the pupil and parents/carers.

- Pupil image file names will not refer to the pupil by name.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories

Managing Videoconferencing & Webcam Use

- Videoconferencing should use the educational broadband network to ensure quality of service and security.
- Pupils must ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing and webcam use will be appropriately supervised for the pupils' age groups.
- For remote learning and video conferencing, Google Meet should be used under supervision

Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook
- Abuse between young people in intimate relationships online i.e. teenage relationship abuse
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

The school will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

Child-on-child sexual abuse and harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks

- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The school will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking “sides”, often leading to repeat harassment.

The school will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse will be reported to the DSL, who will investigate the matter.

Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, e.g. the pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time online.
- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, covered as part of annual Prevent training. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay.

Online hoaxes and harmful online challenges

For the purposes of this policy, an “**online hoax**” is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, “**harmful online challenges**” refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing pupils.
- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils.
- Proportional to the actual or perceived risk.
- Helpful to the pupils who are, or are perceived to be, at risk.
- Appropriate for the relevant pupils' age and developmental stage.
- Supportive.
- In line with the Child Protection and Safeguarding Policy.

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or individual pupils at risk where appropriate.

The DSL will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

Online safety training for staff

The DSL will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

Managing Emerging Technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by any means is forbidden. Please refer to **Acceptable use of Mobile Phones at Highfield C.E. Primary School**
- The use by pupils of cameras in mobile phones is not permitted during or after school time. No pictures should be taken of staff or other children at out of school events organised by the school or the Parents' Association, such as discos and fetes. The school will investigate any reported cases of photos of staff or other pupils at such events being uploaded to social networking sites.
- Staff will be issued with a school phone where contact with pupils is required or where mobile phones are used to capture photographs of pupils. At no time should staff use their personal mobile phone to talk, text, send a picture to a pupil or the parent of a pupil.

Artificial Intelligence (AI) – Safe and Responsible Use

Artificial Intelligence (AI) technologies are increasingly present in society and education. While these tools can offer benefits for teaching and learning, they also present risks if used without appropriate oversight. Our school is committed to ensuring that any use of AI prioritises pupil safety, wellbeing, and ethical practice.

Principles

- The school will review AI tools on an individual basis, assessing their educational value, potential risks, and alignment with safeguarding and data-protection requirements.
- AI will not replace professional judgement. Staff remain responsible for all decisions relating to teaching, assessment, and pupil support.
- Children's safety, privacy, and digital wellbeing are central to all decisions about AI use.

Use of AI by Staff

- Staff may use AI tools for school-related tasks such as lesson planning, drafting reports, or composing emails when logged in under a staff account.
- Staff must follow the ICT Code of Conduct and Acceptable Use Policy (AUP), including guidance on confidentiality, data protection, and ethical use.
- Any AI-generated content used for teaching or communication must be checked carefully for accuracy, bias, and appropriateness.

Use of AI by Pupils

- AI platforms will be blocked on children's iPads and class accounts unless specifically approved for a supervised learning activity.
- When AI is used as part of a planned lesson, teachers will guide pupils to understand both the benefits and the risks, including misinformation, bias, inappropriate content, and over-reliance on automated tools.
- In older year groups, pupils may be supported to agree with their teacher what appropriate use of AI looks like for a particular task, ensuring it does not undermine learning objectives.

Curriculum and Education

- Pupils are taught about safe, ethical, and responsible use of digital technologies, including AI, through the Computing and PSHE/Wellbeing curricula.
- Teaching includes age-appropriate discussions about how AI works, how to question information, and how to recognise potential risks.

Safeguarding and Monitoring

- AI tools can produce biased, misleading, or inappropriate content. For this reason, any AI use involving pupils will be supervised and risk-assessed.
- The school will monitor emerging technologies and update guidance regularly to ensure continued compliance with safeguarding, online safety, and data-protection requirements.
- Parents will be informed of any significant changes to how AI is used within the school.

Partnership with Families and the Local Authority

- The school will work with parents, carers, and the Local Authority to ensure a shared understanding of safe and responsible AI use.
- Any concerns about AI-related risks will be addressed promptly and transparently.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions

Authorising Internet Access

- All staff must read and sign the **Staff Acceptable Use of Schools ICT Systems and the Internet** (see **Appendix A**) before using any school ICT resource, this includes volunteers and governors.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- Parents and pupils will be asked to sign and return a Parental Consent for Internet Access Form (**Appendix C**).

Communications Policy

Introducing the e-safety policy to pupils

- All pupils must read and sign the e-Safety Contract (see Appendix D) before using any school ICT resource.
- E-safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- E-safety training will be embedded within the ICT scheme of work or the Personal Social and Health Education (PSHE) curriculum.

Staff and the E-safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.
- Staff will always use a child friendly safe search engine when accessing the web with pupils.

Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.
- The school will ask all parents to sign the consent form in the Parent Handbook
- The school will maintain a list of e-safety resources for parents/carers

Community use of the Internet

The school will liaise with local organisations to establish a common approach to e-safety.

Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor SCC/HCC can accept liability for any material accessed, or any consequences of Internet access. The school will audit ICT use to establish

if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

Handling E-safety complaints

Complaints of Internet misuse will be dealt with by a senior member of staff. Any complaint about staff misuse must be referred to the Headteacher, who may then consult LADO or HR. Complaints of a child protection nature must be dealt with in accordance with Highfield C.E. Primary School child protection procedures. Pupils and parents will be informed of the complaints procedure (see schools complaints policy). Pupils and parents will be informed of consequences for pupils misusing the Internet.

Writing and reviewing the E-safety policy

Highfield C.E. Primary's E-safety policy is part of the School Development Plan and will operate in conjunction with other policies including for ICT, Behaviour, Anti-Bullying, Curriculum, Safeguarding Children and Security plus the Home-School Agreement. The school has appointed an e-Safety Coordinator (Rosie Walford – Headteacher with delegated responsibilities to other key staff). This may be the Designated Child Protection Coordinator as the roles overlap. It is not a technical role.

Our e-Safety Policy has been written by the school, using CSL e-safety guidance and government guidance. It has been agreed by senior management and approved by governors.

Highfield C.E. Primary School would like to acknowledge Kent CC e-Safety policy.

Appendix A- Acceptable Use of School's ICT Systems and the Internet

Highfield C.E. Primary School

Acceptable Use of School's ICT Systems and the Internet

Every member of staff must give prior careful thought to anything that they post on any social networking site where others can read it or see it (comments and photographs).

Every member of staff is expected to adhere to the guidelines below in order to ensure that their position is not compromised.

If any member of staff is concerned about what they have read or seen on any social networking site they should report it to HT or DHT.

Human resources may also be alerted.

Please remember to keep yourself safe.

- Comments must not be made about children in the school
- Avoid writing things like 'had a bad day at school' or 'don't want to go to work' as this could cause others to speculate.
- Avoid writing things about colleagues, even in code.
- Be aware of who you have as friends/followers. Teaching staff must refuse any requests from parents or pupils to be a 'friend'. Where a member of staff is also a parent, they should be very careful about what they post and how it may be interpreted by their friends who are also parents of children in the school.
- Ensure no indecent photos of you are posted on these sites. Consider that photos of you are most likely to be posted by the person that took them and not you!
- Ensure your settings are set up properly to restrict access and require that posts in which you are tagged need your prior approval before posting
- Mention this guidance to spouses and partners, so that their postings do not compromise your position either.

This guidance must be shared with every new staff member as part of their induction. This guidance will be reviewed annually alongside the safeguarding policy.

To ensure that members of staff, including volunteers and governors, are fully

aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct.

Members of staff should consult the school's e-safety policy for further information and clarification.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that school information systems may not be used for private purposes without specific permission from the Headteacher.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the e-Safety Coordinator, the Designated Child Protection Coordinator or Headteacher.
- I will ensure that electronic communications with pupils including email, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.
- I have read, understood and accept the acceptable use of School's ICT Systems and the Internet.

Signed: _____ Printed: _____ Date: _____

Accepted for school: _____ Printed: _____

Position : _____ Date: _____

Appendix B- Acceptable use of Mobile Phones

Highfield C.E. Primary School

Parent and Pupil Emergency Mobile Phone Agreement

Your child's name_____Class_____

Your name_____

Please explain why your child needs to have a mobile phone on them when they arrive/
leave school.

Mobile phone protocols

- Parents will need to briefly explain why their child needs to have their mobile phone on them.
- The phone is to be used for emergency use only on the journey to or from school.
- The phone must not be used by the child on school premises.
- Phones must be handed in at the office as soon as the child arrives at school.
- The phone must be clearly labelled with the child's name and class.
- The child is responsible for collecting the phone. Any phones not collected will be locked away once the office is closed.
- Parents take full responsibility for the phone and their child's use of the phone during the journey to and from school.
- The school will take no responsibility for the loss of any phone.
- Parents will be contacted if a child does not follow the agreement

Our policy is still that no mobile phones should be taken by children on residential/ day trips organised by the school in school time.

We understand and agree with all the protocols above and that failure to keep any part of the agreement may result in a complete mobile phone ban.

I have discussed the mobile phone agreement with my child and will support the school in implementing it.

Signed by parent _____ Date _____

I agree to follow the mobile phone agreement and have discussed how I will use my mobile phone with my parent.

Signed by pupil _____ Date _____

This agreement is in force until the end of July each year or sooner at the discretion of the school.

Appendix C – Parent Consent for Internet Form

Parental Consent Form

Parent's Consent for Internet Access

Please could you tick the appropriate boxes below to give your consent.

I have read and understood the school e-Safety policy as published on the school website.

I give permission for my child to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task. I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

I give permission for my child to have a school-based email address.

I give permission for my child to engage in age appropriate online learning.

I am happy for my child to be live streamed to an invited audience only, i.e. to invite parents to watch live Christmas performances etc.

Please complete your child's name, sign, date and return this form to the school.

Child's Name _____

Parent's name _____

Signed _____

Date _____

Process for withdrawal or amendment of consent

Should you wish to withdraw or amend consent at any time, please do so via email to info@highfieldschool.co.uk

Appendix D – E-Safety Contract

Highfield C.E. Primary School E-Safety Contract

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.

These e-Safety rules help to protect pupils and the school by describing acceptable and unacceptable computer use.

- 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.
- We immediately close any webpage we not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.

- We do not open e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.
- We do not use AI-powered platforms such as ChatGPT.

Pupil: _____

Class: _____

Pupil's Agreement

I have read and I understand the Highfield CE Primary E-Safety Rules.

I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times.

I know that network and Internet access may be monitored and that irresponsible use may result in the loss of network or Internet access.

Signed: _____

Date: _____