Online Safety Policy

Reviewed: September 2025
To be reviewed: September 2026

Policy Statement

For clarity, the Online Safety Policy uses the following terms unless otherwise stated:

Users - refers to staff, governing body, school volunteers, students and any other person working in or on behalf of the school, including contractors.

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Wider school community – students, all staff, governing body, parents.

At Highwoods Community Primary School we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, also known as e-safety, is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an e-safety incident, whichever is sooner.

The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

This policy is available for anybody to read on the Highwoods Community Primary School website. Upon review, all members of staff will sign as read and understood both the Online Safety policy and the Staff Acceptable Use Policy. A copy of this policy and the Students Acceptable Use Policy will be sent home as part of the school induction pack and returned to school when a child officially begins their education at Highwoods Community Primary School and again at the beginning of Key Stage 2 (see Appendix B).

Policy Governance (Roles & Responsibilities)

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

Appoint one governor (Hannah Cooper) to have overall responsibility for the governance of e-safety at the school who will:

- Keep up to date with emerging risks and threats through technology use.
- Receive regular updates from the Headteacher in regards to training, identified risks and any incidents.

Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for e-safety within our school.

The Headteacher will ensure that:

- Online Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. children, all staff, senior leadership team and governing body, parents.
- The designated Online Safety Officer(s) has had appropriate CPD in order to undertake the day- to- day duties.
- All online safety incidents are dealt with promptly and appropriately in line with safeguarding procedures.
- It is reported to governors when there are any breaches of our filtering systems.

Online Safety Officers

The day-to-day duty of Online Safety Officer(s) is devolved to Martha McLewin/Paul Disley.
The Online Safety Officer(s) will:

- Keep up to date with the latest risks to children whilst using technology; familiarise him/herself with the latest research and available resources for school and home use.
- Review this policy regularly.
- Advise the Headteacher, governing body on all online safety matters.
- Engage with parents and the school community on online safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for the reporting of online safety incidents; ensure staff know what to report and ensure the appropriate audit trail (CPOMS).
- The designated safeguarding officer for filtering and monitoring will ensure any technical online safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.
- Make him/herself aware of any reporting function with technical online safety measures, i.e. internet filtering reporting function; liaise with the Headteacher and responsible governor (Hannah Cooper) to decide on what reports may be appropriate for viewing.

IT Technical Support Staff

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
    - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
    - Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
    - Any online safety technical solutions such as Internet filtering are operating correctly.

- Filtering levels are applied appropriately and according to the age of the user; that 'categories of use' are discussed and agreed with the person with responsibility for filtering and monitoring within school (Headteacher).
- Passwords are applied correctly to all users regardless of age.
- The IT System Administrator password is to be changed on a monthly (30 day) basis.

All Staff

Staff are to ensure that:

- Any online safety incident is reported to the Safeguarding lead and deputy safeguarding lead and is recorded as an Online Safety Incident.

All Students

The boundaries of use of computer equipment and services in this school are given in the student Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy (see Appendix B).

e-Safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff on how to keep themselves safe and report concerns. This can include assemblies, speaker which run alongside our curriculum offer.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will endeavour to support parents to have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parent consultation evenings, meet the teacher, training opportunities, school newsletters and the website, the school will keep parents up to date with new and emerging online safety risks, and will involve parents in strategies to ensure that students are empowered.

Parents must also understand the school needs to have boundaries and safeguarding measures in place to ensure that their child can be properly safeguarded at home. It is the expectation that parents monitor and educate their children outside of the school hours to ensure that the child and school is not negatively impacted upon. Parents are expected to support the school in managing, reporting and dealing with incidents that breach statutory guidance and school polices. As such, parents will sign the student Acceptable Use Policy before any access can be granted to school ICT equipment or services.

The school expects parents and carers to conduct themselves in a manner that supports the school on social media platforms. The school expects parents and carers to know that if the family has a grievance or issue with the school, the complaints policy is available to detail the correct procedures to follow.

The Headteacher reserves the right to consider limitations on access to school site and staff for a parent or carer who threatens, harasses or causes distress to staff or the school community through their use of social media or online platforms. It is enough for a staff member or person within the school community to feel threatened for the Headteacher to act.

This policy works in conjunction with the Behaviour policy, the Child Protection policy, Safeguarding policy and the Child on Child abuse policy. School adheres to DfE guidance and legislation.

Technology

Highwoods Community Primary School uses a range of devices including PCs, laptops and iPads. In order to safeguard the student and in order to prevent loss of personal data, we employ the following assistive technology:

Internet Filtering – we use Essex County Council (as of 1st April 2020 London Grid for Learning – LGfL) proxy filtering that prevents unauthorized access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The Online Safety Officer with responsibility for monitoring and filtering and IT Support are responsible for ensuring that the filtering is appropriate. Any breaches of the code of conduct around acceptable use must be formally recorded on CPOMS. Any breaches are to be reported in the first instance to ICT support, then as appropriate to Essex Broadband Team (as of 1st April 2020 London Grid for Learning – LGfL).

Email Filtering – we use McAfee (as of 1st April 2020 Sophos) anti-virus software and anti-malware software that prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message. Our email system, which is hosted by Office 365, operates its own filtering/anti-spam measures. There is a two- year retention policy for staff emails.

Encryption – No data is to leave the school on an un-encrypted device. Any breach (i.e. loss/theft of device such as laptop or USB flashdrives/memory sticks) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office.
(Note: Encryption does not mean password protected.)

Passwords – all staff will be unable to access any device without a unique username and password.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated at least daily for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns. All USB peripherals such as Flashdrives/Memory Sticks are to be scanned for viruses before use.

Safe Use

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted to staff upon signing the e-safety and the staff Acceptable Use Policy and to students upon signing and returning their acceptance of the Acceptable Use Policy.

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted using the school email accounts. Similarly use of personal email addresses for work purposes is not permitted. All staff are given their own e-mail address, solely for the purpose of 'business' communication. This will take the format of a.teacher@highwoodsprimary.com.

Photos and videos –All parents/ guardians must sign to give permission for their child's image to be used for the following on the admissions form completed when children join our school: photos or videos for promotional purposes, the school's social media, the school website and newspapers. Non-return of this form will not be assumed as acceptance. This will also ascertain if parents give permission for newspaper publication.

Social Networking – Highwoods Community Primary School communicates through its Twitter page, which is updated by teachers and the headteacher. This is for celebrated achievements within the school and sharing experiences with parents. It is not a forum to resolve school matters and issues.

Staff Members who are linked with other staff members or parents of pupils at the school on social media platforms are reminded to conduct themselves professionally (see Code of Conduct) and adhere to confidentiality regarding school matters. We strongly recommend that all personal social media forums used by staff members are 'private'.

In addition, the following is to be strictly adhered to:

- Permission slips (via the school photographic policy) must be consulted before any image or video of any child is uploaded.
- Where services are "comment enabled", comments are to be set to "moderated".
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a license which allows for such use (i.e. creative commons).

Notice and take down policy – should it come to the school's attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Incidents - Any online safety incident is to be brought to the immediate attention of safeguarding lead/deputy safeguarding lead. Where appropriate, this will be logged on CPOMS by the staff member dealing with the incident.

Training and Curriculum -
Online Safety for students is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology

and risks as part of the student's learning. This will take place over the whole academic year following the Purple Mash computing curriculum.

The Online Safety Officer is responsible for recommending a programme of training and awareness for the school year to the Headteacher and responsible Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headteacher for further CPD.

Appendix A

Staff and Governor
Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This agreement is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this agreement and adhere at all times to its contents. Any concerns or clarification should be discussed with school online safety officers, Paul Disley and Martha McLewin.

- I will only use the school's email account/school's ICT equipment for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose/display any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number, personal e-mail address and social networking identities to pupils, parents or carers.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware or software without permission of the IT technician.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images and videos of pupils and/ or staff will only be taken, stored and used for professional purposes in-line with school policy and with written consent of the parent, carer or staff member. Images/videos will not be distributed outside the school network (press, school website, social media, including WhatsApp) without the permission of the parent or carer.
- I understand that all my use of the school's network and internet and other related technologies are monitored and logged and can be made available, on request, by the Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute. I will ensure 'privacy' settings on my personal social media.
- I will support and promote the school's Online Safety and GDPR policies and help pupils to be safe and responsible in their use of ICT and related technologies.
- I understand this forms part of the terms and conditions set out in my contract of employment.
- I understand that images/videos of pupils who have left the school must be deleted from all devices, school media and online platforms.
- I understand that I should not post photos or videos of children onto my personal social media accounts (eg Twitter/Facebook). Parents have given permission for @HCPSColchester to post images and videos. All photos and images should be posted from this account and not personal ones.
- Images and videos of children should not be shared on any personal WhatsApp groups.

This Acceptable Use Agreement is a summary of our Online Safety Policy which is available on our website or on request.

User Signature
I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature ……Date ……

Full Name ……(printed)

Role in school
……

Appendix B

Highwoods Community Primary School

Acceptable Use Policy – Pupils

Our Charter for Safe Online Behaviour

I promise – to only use the school computers/tablets for schoolwork that the teacher has asked me to do.

I promise – not to look for or show other people things that may be upsetting or inappropriate.

I promise – to show respect for the work that other people have done.

I promise - that if I accidentally damage something, I will tell my teacher.

I promise- that I will not take ipads or laptops home.

I will not – use other peoples' usernames or passwords at school or home.

I will not – share personal information online with anyone.

I will not – download anything from the internet unless my teacher has asked me to.

I will- remember the Highwood's High- Five when I am at home using social media or gaming.

I understand – that some people on the internet are not who they say they are, and some people can be unkind or dangerous. I will tell my teacher if I am ever concerned in school, or an adult if I am at home.

I understand – if I break the rules in this charter there will be consequences of my actions and my parents will be told.

Signed (Parent):

Signed (pupil):

Date:

Name of child:

Appendix C

Highwoods Primary School: Artificial Intelligence (AI) Guidance

1. Introduction

Highwoods Primary School acknowledges the increasing prevalence of Artificial Intelligence (AI) and its potential to support and enhance educational practices. This guidance outlines our commitment to the responsible, ethical, and effective use of AI, ensuring alignment with our school values of **accessibility, inspiration, aspiration, and resilience**, while adhering to all relevant legal and statutory responsibilities.

2. Aims

This guidance aims to:

- Establish a framework for the responsible and ethical integration of AI to enhance teaching and learning.
- Provide clear guidelines for staff on the appropriate use of AI tools.
- Ensure the protection of sensitive data and compliance with relevant data protection legislation.
- Promote the use of AI to support staff workload and the creation of high-quality resources.
- Cultivate a culture of innovation and continuous improvement in our use of technology.
- Support the nominated person responsible for monitoring and filtering to effectively safeguard pupils and staff.

3. Legal and Statutory Responsibilities

Highwoods Primary School is committed to complying with all applicable data protection laws, including the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. We recognize our duty to safeguard pupil data and ensure its secure and confidential handling.

- **Data Protection:** Staff must not input any sensitive pupil data into AI tools. This includes, but is not limited to, names, dates of birth, addresses, assessment data, or any other personally identifiable information.
- **Copyright and Intellectual Property:** Staff must ensure that the use of any AI-generated content complies with copyright law and respects intellectual property rights.

- **Safeguarding:** AI must not be used in any way that could compromise the safety and wellbeing of pupils, staff of parents/carers. The uploading of pupil photographs, or photographs that refer to staff or families, to AI platforms is strictly prohibited.

4. AI Usage Guidelines

4.1 Staff Use:

- Staff are encouraged to explore the potential of AI to reduce workload and enhance resource creation, promoting **accessibility** to efficient tools.
- Examples of appropriate AI use include:
    - Generating initial drafts of lesson plans and schemes of work.
    - Creating differentiated learning materials.
    - Summarizing complex texts for adaptation.
    - Developing creative writing prompts and lesson activities.
    - Assisting with administrative tasks, such as creating templates or formatting documents.
    - Drafting policies and other forms of school content linked to statutory guidance and recommendations
    - Research and fact find on aspects for school systems, operations and policies
- Staff should exercise professional judgment when using AI-generated content, adapting and refining it to meet the specific needs of their pupils. This ensures the delivery of **inspirational** learning experiences that foster **aspiration**. *
- Staff should critically evaluate the accuracy and suitability of AI-generated content.
- Staff should consider the efficiency of using AI tools in relation to the specific task and their overall workload.
- Staff are encouraged to engage in professional development opportunities to enhance their understanding and effective use of AI.

4.2 Pupil Use:

- Pupil use of AI tools will be carefully considered, age-appropriate, and supervised, with a focus on developing critical thinking, digital literacy, and responsible use- examples in school include the use of AI in TT Rockstars and number bots.
- Pupils will be taught about internet safety and being safe online as part of the National Curriculum.

5. Data Security and Confidentiality

- All staff are responsible for maintaining the confidentiality and security of pupil data.
- Sharing sensitive pupil information with AI tools or external platforms is strictly prohibited.

- The school will regularly review and update its data security measures to ensure ongoing compliance with best practices.

6. Review and Monitoring

This guidance will be reviewed annually by Trustees or as needed to reflect changes in legislation, best practice, and technological advancements. The school will monitor the use of AI tools to ensure compliance with this guidance and address any emerging issues- this monitoring will incorporate the wider IT support that the school employs through PEP solutions.