ONLINE SAFETY POLICY

APPROVED BY: Governing Body

NEXT REVIEW: September 2024

ONLINE SAFETY POLICY

Aims

This policy aims to:

- Set out expectations for online behaviour, attitudes and activities and use of digital technology (including when devices are offline) at Holmleigh Primary School.
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform.
- Facilitate the safe, responsible and respectful use of technology to support teaching and learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
  - for the protection and benefit of the children and young people in their care, and
  - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
  - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession

• Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Safeguarding and Child Protection Policy, Behaviour and Anti-Bullying Policy)

Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, **Keeping Children Safe in Education (**https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1181955/Keeping_children_safe_in_education_2023.pdf,) and its advice for schools on **preventing and tackling bullying and searching, screening and confiscation** https://www.gov.uk/government/publications/preventing-and-tackling-bullying. It also refers to the Department's guidance on **protecting children from radicalisation**. https://www.gov.uk/government/publications/the-prevent-duty-safeguarding-learners-vulnerable-to-radicalisation It reflects existing legislation, including but not limited to the **Education Act 1996** https://www.legislation.gov.uk/ukpga/1996/56/contents/data.pdf (as amended), the **Education and Inspections Act 2006** https://www.legislation.gov.uk/ukpga/2006/40/pdfs/ukpga_20060040_en.pdf **and the Equality Act 2010** . https://www.legislation.gov.uk/ukpga/2010/15/pdfs/ukpga_20100015_en.pdf. In addition, it reflects the **Education Act 2011**, https://www.legislation.gov.uk/ukpga/2011/21/pdfs/ukpga_20110021_en.pdf has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so. The

policy also takes into account the **National Curriculum computing programmes of study**. https://www.gov.uk/government/publications/national-curriculum-in-england-computing-programmes-of-study

Further Help and Support

Internal school channels should always be followed first for reporting and support, as documented in school policy documents, especially in response to incidents, which should be reported in line with the Safeguarding and Child Protection Policy. The DSL will handle referrals to Local Authority Multi-Agency Safeguarding Hubs (MASH) and the Headteacher will handle referrals to the LA Designated Officer (LADO).

Scope

This policy applies to all members of the Holmleigh Primary School community (including staff, governors, volunteers, contractors, students/pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school or centre role.

Roles and responsibilities

The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL). The governor who oversees online safety is Matthew Caudle

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)

The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The designated safeguarding lead

Details of the school's designated safeguarding lead and deputies (DSL) are set out in our Safeguarding and Child Protection policy. The DSL takes lead responsibility for online safety in school, in particular:

- Support the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.

- Work with the headteacher, Computing Lead and ICT Technician and other staff, as necessary, to address any online safety issues or incidents.
- Ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Update and deliver staff training on online safety
- Liaise with other agencies and/or external services if necessary
- Provide regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

All Holmleigh Primary Staff

- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up
- Know who the Designated Safeguarding Lead (DSL) is.
- Read Part 1, Annex A and Annex C of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex A for SLT and those working directly with children, it is good practice for all staff to read all three sections).
- Read and follow this policy in conjunction with the Holmleigh main Safeguarding and Child Protection Policy with key emphasis placed on section 27 (Further Information on Safeguarding Issues).
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with safeguarding procedures.
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself.
- Follow the Holmleigh Primary School Behaviour Code of Conduct Policy.
- Notify the DSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon.
- Identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils).
- Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites (ask the DSL what appropriate filtering and monitoring policies are in place).
- To carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.
- Prepare and check all online source and resources before using within the classroom.
- Encourage pupils/students to follow their acceptable use agreement, remind them about it and enforce school sanctions.
- Notify the DSL of new trends and issues before they become a problem.

- Take a zero-tolerance approach to bullying and low-level sexual harassment.
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL know.
- Receive regular updates from the DSL and have a healthy curiosity for online safety issues.
- They must model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.

PSHE/RHSE Lead

As listed in the 'all staff' section, plus:

- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / Relationships, Health and Sex Education curriculum. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives."
- Make reference to Section 27 of the Safeguarding and Child Protection Policy (Further Information on Safeguarding Issues- Online Safety).
- This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RHSE.

The Computing Lead

As listed in the 'all staff' section, plus:

- Look for opportunities to embed online safety in their subject or aspect, and model positive attitudes and approaches to staff and pupils alike
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing.
- Ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

ICT Technician

As listed in the 'all staff' section, plus:

- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- Make specific reference to section 27 in the Safeguarding and Child Protection Policy (Further Information on Safeguarding Issues- Filters and monitoring).
- Work closely with the Designated Safeguarding Lead / Data Protection Officer / LGfL nominated contact to ensure that school systems and networks reflect school policy.
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc .
- Support and advise on the implementation of appropriate filtering and monitoring systems.
- Maintain up-to-date documentation of the school's online security and technical procedures.
- To report online-safety related issues that come to their attention in line with school policy.
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls.
- Monitor the use of school technology and online platforms and that any misuse/attempted misuse is identified and reported in line with school policy
- Ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy

This list is not intended to be exhaustive.

Volunteers

- Read, understand, sign and adhere to the Acceptable Use Agreement (AUA).
- Report any concerns, no matter how small, to the DSL.
- Maintain an awareness of current online safety issues and guidance in reference to the Safeguarding and Child Protection Policy.
- Model safe, responsible and professional behaviours in their own use of technology.

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on Acceptable Use Agreement (AUA) of the school's ICT systems and internet (appendix 1)
- Parents can seek further guidance on keeping children safe online from the following organisations and websites:
- What are the issues?, UK Safer Internet Centre:https://www.saferinternet.org.uk/advicecentre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it.
If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2)

Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.
In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private.
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- The safe use of social media and the internet will also be covered in other subjects where relevant. The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Educating parents about online safety

The school will raise parents' awareness of internet safety in workshops, letters or other communications home, and in information via our website. This policy will also be shared with parents. Online safety will also be covered during parents' evenings. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL. Concerns or queries about this policy can be raised with any member of staff or the headteacher.

Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school Behaviour and Anti-bullying policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected. In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules
- If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police
- Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.
- Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Acceptable use of the internet and e-mail in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems, the internet and e-mail (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. Use of the school's internet and e-mail must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

Pupils using mobile devices in school

Year 5 and Year 6 pupils are permitted to bring their own mobile phones to school for the purpose of communication with parents before and after school. Mobile phones will need to be switched off by pupils before entering the playground. They need to be handed in to a designated member of staff at the beginning of the school day. The phones will be kept in the class safe during the day for safekeeping. Pupils are responsible for collecting their mobile phone after school. Pupils may not bring mobile devices into school other than for the purpose stated above. Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school's Behaviour Policy.

Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2. Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT technician. Work devices must be used solely for work activities.

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the Behaviour Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and

seriousness of the specific incident. The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings). The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually. Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training. Volunteers will receive appropriate training and updates, if applicable. More information about safeguarding training is set out in our Child Protection and Safeguarding Policy.

Monitoring Arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 4. This policy will be reviewed in Autumn 2025 by the Designated Safeguarding Lead. At every review, the policy will be shared with the governing board.

Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour and Anti-bullying policy
- Staff Behaviour Conduct Policy
- Acceptable use of mobile phones policy
- Data protection policy and privacy notices
- Complaints procedure

Acceptable Use Agreement (pupils, parents/carers)

What is Acceptable Use Agreement (AUA)?

We ask all children, young people and adults involved in the life of Holmleigh Primary School to sign an Acceptable Use Agreement (AUA), which is a document that outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school). Your child will also be asked to sign an AUA as part of the Computing curriculum.

Why do we need an AUA?

These rules have been written to help keep everyone safe and happy when they are online or using technology. Sometimes things go wrong and people can get upset, but these rules should help us avoid it when possible, and be fair to everybody. School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. This means anything on a school device or using school networks/platforms/internet may be viewed by one of the staff members who are here to keep your children safe. We tell your children that they should not behave any differently when they are out of school or using their own device or home network. What we tell pupils about behaviour and respect applies to all members of the school community:

"Treat yourself and others with respect at all times; treat people in the same way when you are online or on a device as you would face to face."

You can read Holmleigh's full Online Safety Policy here for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding and Child Protection Policy, Behaviour Policy, etc.). If you have any questions about this AUA or our approach to online safety, please speak to a member of the senior leadership team.

Appendix 1: acceptable use agreement (pupils and parents/carers)

<table>
<tr><th colspan="2">Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers</th></tr>
<tr><td colspan="2">Name of pupil:</td></tr>
<tr><td colspan="2">When using the school's ICT systems and accessing the internet in school, I will not:
Use them for a non-educational purpose
Use them without a teacher being present, or without a teacher's permission
Access any inappropriate websites
Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
Use chat rooms
Open any attachments in emails, or follow any links in emails, without first checking with a teacher
Use any inappropriate language when communicating online, including in emails
Share my password with others or log in to the school's network using someone else's details
Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer
Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision
If I bring a personal mobile phone or other personal electronic device into school: I will leave it at the school office for safekeeping
I will not use it during lessons, clubs or other activities organised by the school
I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online
I agree that the school will monitor the websites I visit.
I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.
I will always use the school's ICT systems and internet responsibly.</td></tr>
<tr><td>Signed (pupil):</td><td>Date:</td></tr>
<tr><td colspan="2">Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.</td></tr>
<tr><td>Signed (parent/carer):</td><td>Date:</td></tr>
</table>

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

Acceptable use of the school's ICT systems and internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
• When using the school's ICT systems and accessing the internet in school, or outside school on a work device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software • Share my password with others or log in to the school's network using someone else's details	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school may monitor the websites I visit. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and Computing Lead know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 3: online safety training needs – self-audit for staff.

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here	

Appendix 4: online safety incident report log

Online Safety Incident Report Log				
Date:	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**