Honiton Primary School

Online safety policy

Approved by: Honiton Primary School Full governing body	**Date:**
Last reviewed on:	15.7.25
Next review due by:	July 2026

Summary of key amendments

Amendment	Section	Change
July 2025	Updated sections 3.1, 3.3, 3.7, 4.0, and 9.0 as follows: We also added a new section (11.2) outlining training for pupils on cyber-security, to meet the DfE's cyber security standards.	• In section 3.1: added 'The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.' • Section 3.1 added a checklist of • In section 3.1 added a link to the DfE's filtering and monitoring standards and a checklist of online safety standards to monitor • In section 3.3: added 'responding to safeguarding concerns identified by filtering and monitoring' to the list of DSL's responsibilities • In section 3.7: removed 'when relevant' from this paragraph • In section 4.0: added 'be discerning in evaluating digital content' to the list of topics that KS2 pupils will be taught, and added 3 new items to concepts all pupils will know when they leave primary school • In section 9.0: updated to include latest advice on creating strong passwords

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:
    - content: being exposed to illegal, inappropriate, or harmful content,
    - contact: being subjected to harmful online interaction with other users;
    - conduct: online behaviour that increases the likelihood of, or causes, harm
    - commerce: risks such as inappropriate advertising, phishing and or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for Head Teachers and school staff
- Relationships and sex education
- Searching, screening and confiscation
- DfE filtering and monitoring standards

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which 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.

3. Roles and responsibilities

3.1 The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the Head Teacher to account for its implementation.

The governing board will coordinate 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 Rebecca Buss.

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 governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.
- The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.
- The governing board will also make sure all staff receive regular online safety updates (via email, and staff meetings/staff training days), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.
- The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:
    - Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
    - Reviewing filtering and monitoring provisions at least annually;
    - Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
    - Having effective monitoring strategies in place that meet their safeguarding needs.

○

3.2 The Head Teacher

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

3.3 The designated safeguarding lead

Details of the school's DSL and the safeguarding officers are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL (Elaine Fyffe) and the Computing lead (Ross Hasler) take lead responsibility for online safety in school, in particular:

- Supporting the Head Teacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- The DSL should take lead responsibility for safeguarding and child protection including online safety and understanding the filtering and monitoring systems and processes in place.
- Working with the Head Teacher and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged on CPOMS under the 'online safety category' or 'internet filtering' category and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyberbullying are logged on CPOMS under the online safety category and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary (e.g. PCSO)
- Providing regular reports on online safety in school to the Head Teacher and/or governing board
- With the ICT manager and Governor review filtering and monitoring provision at least annually.
- Responding to safeguarding concerns identified by filtering and monitoring

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Liaising with our IT providers to conduct full security checks and monitor the school's ICT systems on a regular basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any incidents of cyberbullying are logged on CPOMS under the online safety category and dealt with appropriately in line with the school behaviour policy
- Ensuring that any incidents of cyberbullying are dealt with appropriately in line with the school behaviour policy
- With the DSL and Computing Governor, review filtering and monitoring provision at least annually.

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use. This should be communicated verbally in technology learning and online safety lessons in EYFS to year 4. In Year 5 and 6, where it is felt pupils will be able to show a higher level of understanding, an acceptable use agreement will be introduced, discussed and signed each year in September (appendix 1).
- Working with the DSL and computing lead to ensure that any online safety incidents are logged on CPOMS under the online safety category and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- All staff will receive appropriate online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the Head Teacher of any concerns or queries regarding this policy

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International

3.7 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 and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. 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
- Be discerning in evaluating digital content

*By the **end of primary school**, pupils will know:*

- *That people sometimes behave differently online, including by pretending to be someone they are not*
- *That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous*

- *The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them*
- *How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met*
- *How information and data is shared and used online*
- *How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.*
- *The benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing*
- *How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private*
- *Where and how to report concerns and get support with issues online*

The full progression of online safety learning intentions is included in appendix 4 and includes an online safety curriculum progression in response to the breadth of challenges and need for education in digital literacy and good citizenship young people today require.

There is a scheduled learning topic each academic year where the online safety learning intentions will be taught for each year group.

During these online safety half terms, in class learning will be supplemented with virtual / in-person assemblies messaging re-iterating the key themes of keeping safe online and respectful communication on social media and gaming channels.

5. Educating parents about online safety

The school will raise parents' awareness of online safety in letters or other communications home, and in information via:

- The e-safety parent letter, which is sent out every two months. This is emailed out to parents and posted in the newsletter section of the website.
- More targeted letters to parents in specific year groups / phases / key stages when required.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Head Teacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Head Teacher.

6. Cyber-bullying

6.1 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 policy.)

6.2 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.

All staff will (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).

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.

6.3 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 and the school's COVID-19 risk assessment.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Honiton Primary School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Honiton Primary School will treat any use of AI to bully pupils in line with our behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment (testing possible searches and instructions as well as evaluating responses for appropriateness and suitability) where new AI tools are being used by Honiton Primary.

7. Acceptable use of the internet in school

Pupils in Years 5 and 6, staff, governors and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Pupils in the EYFS and Years 1 - 4 will have the principles of acceptable use discussed with them in an age appropriate manner, and at relevant time points, depending on the technology use taking place.

Use of the school's internet 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.

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Pupils using mobile devices in school

All pupil mobile phones handed-in at the beginning of the day policy.

Pupils may bring mobile devices into school in order to remain in contact with parents on the journey to and from school. It is an expectation that mobile phones are turned off and handed in at the beginning of the day and only then collected at the end of the day. Teachers will store mobile phones in an out of reach location (e.g. a locked cupboard or lock box) for the school day. Pupils are not permitted to use them during:

- Lessons
- Break times
- Clubs before or after school, or any other activities organised by the school

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords can be made up of three random words, in combination with numbers and special characters if required, or generated by a password manager
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Having anti-virus and anti-spyware software installed if relevant
- Allowing installation of the latest operating system updates updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the **Computing lead**.

10. Pupils using loaned school devices outside of school

Should a device need to be loaned to a pupil to use outside of school, the parent will need to sign a loan agreement setting out in detail the purpose and terms of appropriate learning focused use of the loaned device. See appendix 5

11. How the school will respond to issues of misuse, online abuse or cyberbullying

11.1 In school

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our 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 / staff code of conduct. 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.

11.2 Out of school

If the school is made aware of an incident involving pupils outside of school hours and supervision the school will take the following steps:

- Advise the parent(s) bringing the incident to our attention the steps they can take (report the incident to the police, block offending users and supervise / monitor their child's phone / game / internet / social media use.
- The school will communicate to the parents / carers of other named pupils the details of the incident that has been reported and request that they speak to their child and investigate what has taken place.

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

12. Training

All new staff members will receive training 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 and staff meetings).

Safeguarding training is scheduled annually to be delivered for all staff at the beginning of the year by the DSL (EF) which includes reference to online safety.

School staff also receive training to help identify early signs of radicalisation and extremism which encompasses the risks posed from online radicalisation.

The DSL and Computing Lead 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.

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.

13. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed **annually** by the **Computing Lead**. At every review, the policy will be shared with the governing board.

The Computing Lead will monitor the teaching of the Online Safety learning intentions through evidence in SOLE books after the half term in which it has been taught.

The computing lead in line with the guidance of the DfE to review filtering and monitoring will hold a filtering and monitoring review when meeting with the computing governor termly.

14. Links with other policies

This online safety policy is linked to our:

- Safeguarding policy
- KCSIE
- Behaviour policy
- Computing Policy
- Staff disciplinary procedures
- GDPR policy
- Complaints procedure

- Mobile phone policy
- Code of conduct for school employees

Appendix 1: KS2 (Years 5 and 6) acceptable use agreement

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** ● Always use the school's ICT systems and the internet responsibly and for educational purposes only ● Only use them when a teacher is present, or with a teacher's permission ● Keep my username and passwords safe and not share these with others ● Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer ● Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others ● Always log off or shut down a computer when I'm finished working on it **I will not:** ● Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity ● 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 ● Log in to the school's network using someone else's details ● 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:** ● If I bring a mobile phone to school I understand that I will turn it off once I enter the school gates and hand it in to the teacher at the beginning of the day who will look after it for me. ● I understand that a mobile phone is not to be kept in my school bag, class tray or jacket but must be given in, each day, to my teacher who will look after it for me. ● If I have brought a mobile phone in, I will collect it at the end of the day and will only turn it on once I am leaving the school. **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**

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 (if applicable), I will not: ● Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) ● 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, or connect unauthorised hardware or devices to the school's network ● Share my password with others or log in to the school's network using someone else's details ● Take photographs of pupils without checking with teachers first ● Share confidential information about the school, its pupils or staff, or other members of the community ● Access, modify or share data I'm not authorised to access, modify or share ● Promote private businesses, unless that business is directly related to the school	
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 will monitor the websites I visit and my use of the school's ICT facilities and systems. 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 ICT manager 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.	
PRINT NAME: **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**:
Question	**Yes/No (add comments if necessary)**
Who is the person who has responsibility for online safety in school?	
What must you 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?	

Appendix 4: progression of online safety learning

Online safety progression in learning 2024-25

Online safety progression: 2024/25						
Year	**Privacy and security**	**Online Relationships**	**Online Bullying**	**Self-image and identity**	**Health, Wellbeing and lifestyle**	**Managing Online Information**
1	I can explain how passwords are used to protect information, accounts and devices. I can recognise more detailed examples of information that is personal to someone (e.g where someone lives and goes to school, family names).	I can give examples of when I should ask permission to do something online and explain why this is important. I can explain why it is important to be considerate and kind to people online and to respect their choices.			-	I know / understand that we can encounter a range of things online including things we like and don't like as well as things which are real or make believe / a joke I know how to get help from a trusted adult if we see content that makes us feel sad, uncomfortable, worried or frightened
2		I can give examples of how someone might use technology to communicate with others they don't also know offline and explain why this might be risky. (e.g. email, online gaming, a pen-pal in another school / country). I can explain who I should ask before sharing things about myself or others online	I can explain what bullying is, how people may bully others and how bullying can make someone feel. I can talk about how anyone experiencing bullying can get help.		I can explain simple guidance for using technology in different environments and settings I can say how those rules / guides can help anyone accessing online technologies	

Online safety progression: 2024/25						
Year	**Privacy and security**	**Online Relationships**	**Online Bullying**	**Self-image and identity**	**Health, Wellbeing and lifestyle**	**Managing Online Information**
3	I can give reasons why someone should only share information with people they choose to and can trust. I can explain that if they are not sure or feel pressured then they should tell a trusted adult.	I can explain what it means to 'know someone' online and why this might be different from knowing someone offline. I can explain what is meant by 'trusting someone online', why this is different from 'liking someone online', and why it is important to be careful about who to trust online including what information and content they are trusted with. I can explain why someone may change their mind about trusting anyone with something if they feel nervous, uncomfortable or worried.			I can explain why spending too much time using technology can sometimes have a negative impact on anyone; I can give some examples of both positive and negative activities where it is easy to spend a lot of time engaged I can explain why some online activities have age restrictions, why it is important to follow them and know who I can talk to if others pressure me to watch or do something online that makes me feel uncomfortable (e.g. age restricted gaming or web sites).	
4			I can recognise when someone is upset, hurt or angry online. I can describe ways people can be bullied through a range of media (e.g. image, video, text, chat).	I can explain how my online identity can be different to my offline identity.	I can explain how using technology can be a distraction from other things, in both a positive and negative way. I can identify times or situations when someone may need to limit the amount of time they use technology e.g. I can suggest strategies to help with limiting this time.	I can analyse information to make a judgement about probable accuracy and I understand why it is important to make my own decisions regarding content and that my decisions are respected by others.

Online safety progression: 2024/25						
Year	**Privacy and security**	**Online Relationships**	**Online Bullying**	**Self-image and identity**	**Health, Wellbeing and lifestyle**	**Managing Online information**
5			I can recognise online bullying can be different to bullying in the physical world and can describe some of those differences. I can describe how to capture bullying content as evidence (e.g screen-grab, URL, profile) to share with others who can help me.		I can describe ways technology can affect health and well-being both positively (e.g. mindfulness apps) and negatively. I can describe some strategies, tips or advice to promote health and wellbeing with regards to technology.	I can explain what is meant by 'being sceptical'; I can give examples of when and why it is important to be 'sceptical'. I can demonstrate how to analyse and evaluate the validity of 'facts' and information and I can explain why using these strategies are important.
6		I can explain how sharing something online may have an impact either positively or negatively I can describe how to be kind and show respect for others online including the importance of respecting boundaries regarding what is shared about them online and how to support them if others do not. I can explain that taking or sharing inappropriate images of someone (e.g. embarrassing images), even if they say it is okay, may have an impact for the sharer and others; and who can help if someone is worried about this.		I can identify and critically evaluate online content relating to gender, race, religion, disability, culture and other groups, and explain why it is important to challenge and reject inappropriate representations online. I can describe issues online that could make anyone feel sad, worried, uncomfortable or frightened. I know and can give examples of how to get help, both on and offline.		I can recognise features of persuasive design and how they are used to keep users engaged (current and future use).

Appendix 5: Device loan agreements for pupils

Device loan agreement for pupils

1. This agreement is between:

1) **Honiton Primary School, Clapper Lane, Honiton, Devon, EX14 1QF** (the school)

2) and [•_____] (“the parent” and “I”)

And governs the use and care of devices assigned to the parent’s child (the “pupil”). This agreement covers the period from the date the device is issued through to the return date of the device to the school.

All issued equipment shall remain the sole property of the school and is governed by the school’s policies.

1. The school is lending the pupil **a •chromebook / iPad / tablet / laptop** (“the equipment”) for the purpose of **accessing and doing their remote learning schoolwork from home**

2. This agreement sets the conditions for taking a **Honiton Primary School •chromebook / iPad / tablet / laptop** (“the equipment”)] home.

I confirm that I have read the terms and conditions set out in the agreement and my signature at the end of this agreement confirms that I and the pupil will adhere to the terms of loan.

2. Damage/loss

By signing this agreement I agree to take full responsibility for the loan equipment issued to the pupil and I have read or heard this agreement read aloud and understand the conditions of the agreement.

I understand that I and the pupil are responsible for the equipment at all times whether on the school’s property or not.

If the equipment is **damaged, lost or stolen**, I will immediately inform **Mrs Teasdale in the school office (01404 548 700 / admin@honiton-pri.devon.sch.uk**) and I acknowledge that I am responsible for the reasonable costs requested by the school to repair or replace the equipment. If the equipment is stolen, I will also immediately inform the police.

I agree to keep the equipment in good condition and to return it to the school on their demand from the school in the same condition.

I will not leave the equipment unsupervised in unsecured areas.

I will make sure my child takes the following measures to protect the device:

- Keep the device in a secure place when not in use
- Don’t leave the device in a car or on show at home
- Don’t eat or drink around the device
- Don’t lend the device to siblings or friends
- Don’t leave the equipment unsupervised in unsecured areas

3. Unacceptable use

I am aware that the school may monitor the pupil’s activity on this device.

I agree that my child will not carry out any activity that constitutes ‘unacceptable use’.

This includes, but is not limited to the following:

- **Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination**
- **Any illegal conduct, or statements which are deemed to be advocating illegal activity**
- **Activity which defames or disparages the school, or risks bringing the school into disrepute**
- **Causing intentional damage to ICT facilities or materials**

- **Using inappropriate or offensive language**
- **Using it to access social media accounts**

I accept that the school will sanction the pupil, in line with our **behaviour policy,** if the pupil engages in any of the above **at any time.**

4. Personal use

I agree that the pupil will only use this device for educational purposes and not for personal use and will not loan the equipment to any other person.

I agree that the laptop will only be used by the pupil for whom it is intended with the exception of parental/carer support only in the circumstance of supporting the pupil to access remote learning.

5. Data protection

I agree to take the following measures to keep the data on the device protected.

- **Keep the equipment password-protected**
- **Make sure my child locks the equipment if it's left inactive for a period of time**
- **Do not share the equipment among family or friends**

If I need help doing any of the above, I will contact **Mr Hasler** on the email **admin@honiton-pri.devon.sch..uk**.

6. Return date

I will return the device in its original condition to **the school office within 3 days of either: being requested to do so OR the full reopening of schools after the Government announced reopening.**

I will ensure the return of the equipment to the school if the pupil no longer attends the school.

7. Consent

By signing this form, I confirm that I have read and agree to the terms and conditions set out above.

PUPIL'S FULL NAME	
PARENT'S FULL NAME	
PARENT'S SIGNATURE	

If a signed physical copy is not possible the below shall be signed electronically by means of typing and shall be included by receipt of email from the parent/carer:

By signing this form, I confirm that I have read and agree to the terms and conditions set out above.

Please sign by typing your name and your child's name.

PUPIL'S FULL NAME	
PARENT'S FULL NAME	

Appendix 6: EYFS and Years 1 - 4 acceptable use principles for discussion

Teachers to discuss the acceptable use principles with pupils in a manner which is relevant for that age group and the activities they are undertaking.

I will:

- Always use the ipads, chromebooks and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- 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
- Log in to the school's network using someone else's details
- 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:

- If I bring a mobile phone to school I understand that I will turn it off once I enter the school gates and hand it in to the teacher at the beginning of the day who will look after it for me.
- I understand that a mobile phone is not to be kept in my school bag, class tray or jacket but must be given in, each day, to my teacher who will look after it for me.
- If I have brought a mobile phone in, I will collect it at the end of the day and will only turn it on once I am leaving the school.

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.