



THE HASELWORTH WAY P012

GOSPORT



HASELWORTH PRIMARY SCHOOL ACCEPTABLE USE OF ICT FOR PUPILS POLICY

Policy approved:	September 2020	FGB
Signed:	<i>N. Jones</i>	Headteacher
Signed:	<i>Dr C Roast</i>	Chair of Governors
Date of next review:	Summer 2022	Bi -Annually
Monitored and evaluated by:	Computing Leader	Termly



Introduction

As an increasingly digital world develops, at Haselworth Primary School we encourage the pupils' use of the rich information and communication resources available through the internet, together with the development of appropriate skills to analyse and evaluate these resources. While technology is unlikely to be the same by the time our pupils leave secondary school, this will enable fundamental skills to be developed to support successful citizenship.

The school recognises and embraces the powerful tool of technology, and as such we strive to ensure our pupils have good, appropriate and safe access. However, the school also recognises its responsibilities in ensuring safe use of the internet and other communication systems for all pupils and so this policy outlines our strategy to protect pupils.

This policy applies to pupils of the school who have access to and are users of school ICT systems, both in and out of the school. For all other members of the school (staff, governors, visitors and volunteers) please refer to the separate policy "acceptable use of ICT for staff".

Pupil Protection

It is our intention to protect our pupils from inappropriate or undesirable material. The following criteria define inappropriate or undesirable materials:

- Obscene, offensive, illegal, inaccurate or discriminatory
- Pupils should not feel or become uncomfortable, threatened or worried by material or information on websites, email or other online forums.
- Similarly, pupils must not harass, insult, attack others, violate copyright, or trespass in others' folders
- Illegal, inappropriate, inaccurate, harmful or discriminatory material
- Pupils should not feel or become uncomfortable, threatened or worried by material or information on websites, email or other online forums, exposed to commercial advertising, or adults posing as children or young adults
- Personal online behaviour that increases the likelihood of, or causes harm, for example making, sending and receiving explicit images, online bullying
- Pupils should not violate copyright or trespass in others' folders

In addition, the school will never make publically available photos or videos with the names of individual children. Where photographs or videos are used in published materials, including the school website or other areas, the school will ensure:

- Parental permission is given
- Photographs or videos of groups of children will be described as "children investigating a science problem", for example.

Parental permission will be sought to share photos and comments on private online platforms such as Seesaw.



Internet Access/Filters

- Access to the internet is possible via the computer network, using computers (including tablets) and Interactive whiteboards (IWBs).
- There is a bank of laptops for use throughout the school. In addition, there are PCs in various offices, in the library and linked to IWBs in each classroom.
- A bank of iPads is also available, which must be collected and returned by staff only.
- All computers linked to the internet incorporate automatic anti-virus protection.
- Pupils must not bring in software from home to upload onto the system.
- The broadband internet connection is provided by Hampshire County Council and incorporates a filtering system or “firewall” appropriate to the age of our pupils, which screens undesirable sites at a proxy server.
- Children should not use their own equipment, such as mobile phones, to access the internet as the filtering in place may not be deemed adequate for the school environment and content accessed cannot be monitored by the school systems. Mobile phones will be stored securely in the office during the school day.

Guidelines for in school use of the Internet with pupils

The Computing subject leader has overall responsibility for ensuring that skills are planned into the curriculum in line with National Curriculum expectations and made specific in long term planning. Internet access is integrated into learning activities at the planning stage across the school.

Where applicable, suitable websites to support learning are identified by all staff and are identified on planning and can be bookmarked for later use.

Children are also able to use specified search engines such as “Google” to find appropriate websites – to ensure appropriate content is returned in these searches, children are taught to include terms such as ‘for kids’ or use child-safe search engines.

Our website will provide links to safe websites which are appropriate for the age phase being taught, as well as current topics. For online tools children will be provided with login information.

The use of social networking sites are not permitted in the school. Children are advised against the risks of social media and the importance of age restrictions.

Supervision/responsibility

It is critical that responsible usage of the internet to all pupils is taught in specific detail at least termly in Computing and other lessons (including P4C and in assemblies). Children will be reminded of their responsibility each time they use a device. Therefore, children are only allowed to access the internet once they have been given consent from a member of staff. This applies to lesson times, break times and before/after school.



However, due to the nature of information available via the Internet, it is not possible to guarantee that particular types of material will never appear on a computer screen. Neither the school nor Hampshire County Council can accept liability for the material accessed or any consequences thereof.

It is important to note the shared responsibility of all stakeholders to ensure safe usage. Further information on using ICT safely, potential misuses and reporting procedures can be found in the Child Protection and Safeguarding policy.

Misuse of the Internet

Misuse of the Internet will not be tolerated. In the first instance, the class teacher should deal with any misuse of the internet with the child. However, the incident must always be reported to the Computing Leader and will be logged in the child's behaviour log.

Should there be any concerns over the types of material accessed (e.g. types of materials identified earlier in this policy), the matter should immediately be reported to the Headteacher. The sanctions imposed will reflect the severity of the incident. These could range from the Headteacher contacting parents, to a temporary suspension of ICT rights, to permanent exclusion for very serious offences.

Pupils must report accidental access to inappropriate material immediately to their teacher.

Promoting Fundamental British Values, and Preventing Radicalisation and Violent Extremism

Haselworth Primary School values the fundamental rights of freedom of speech, expression of beliefs and ideology and understanding of others which are the core values of our democratic society. However, all rights come with responsibilities and free speech or beliefs designed to manipulate the vulnerable or which advocate harm or hatred towards others will not be tolerated.

Haselworth Primary School seeks to protect its children and staff from all messages and forms of violent extremism and ideologies including those linked to, ***but not restricted to***, the following: Far Right/Neo Nazi, White Supremacist ideology, extremist Islamic ideology, Irish Nationalist and Loyalist paramilitary groups and extremist Animal Rights groups.

Haselworth Primary School is clear that exploitation and radicalisation will be viewed as a safeguarding concern and will be referred to the appropriate safeguarding agencies. For further information, refer to the Department for Education (DfE) Prevent guidance, our statement of British Values and Safeguarding and Child Protection policies.



Home Learning

Staff at Haselworth Primary School will consider the safety of the children at their school when they set home learning tasks online. When planning online lessons/activities Haselworth staff will follow all relevant guidance received from the DfE and the Local Authority and will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

Haselworth Primary School will ensure children who are being asked to work online have very clear reporting routes in place so they can raise any concerns whilst online. For example, talking to the adult in class or raising an issue on Seesaw.

As well as reporting routes back to Haselworth, the school will also signpost children to age appropriate practical support from the likes of:

- **Childline** - for support
- **UK Safer Internet Centre** - to report and remove harmful online content
- **CEOP** - for advice on making a report about online abuse.

Haselworth Primary School will be in regular contact with parents and carers to reinforce the importance of children being safe online. It will be especially important for parents and carers to be aware of what their children are being asked to do online.

Advice to parents and carers on keeping pupils safe online during home learning.

During home learning, it is important to help your child stay safe online when they are using existing devices and services or when they are using new services, apps or devices, such as webcams and tablets, to access the set work. Therefore, to support this it is vital that you:

1. Check security and privacy settings

- Adjust privacy and safety settings increases security and controls the personal data you/your child shares. Look for the 'privacy and security' or 'settings' on the app or website.
- Review the security settings on your/your child's smart devices. If your/your child's device is using a default or easily guessable password, change it.
- Set up two-factor authentication. This is a free security feature to stop unwanted people getting into your/your child's accounts. You/your child will receive a text or code when you/they log in to check you/they are who you/they say you are.
- Update your/your child's devices because using the latest version of software and apps can immediately improve your/your child's security.

2. Block unsuitable content

- It is important to understand the website or app your child is using and how they (website or app) do things - find out in their terms and conditions.
- If you/your child sees harmful activity, report it to the site. Platforms often offer advice on how to do this but you/your child can also seek support at:
 - Samaritans



- Mind
- BEAT
- To prevent unwanted content from appearing, set filters on your home broadband and mobile networks. The UK Safer Internet Centre has advice on how.

3. **Protect against Fraud**

- Criminals will use every opportunity they can to scam innocent people. Beware of fraud and scams online eg: phishing emails and text messages. There is guidance on how to recognise these emails.
- You/your child can forward any suspicious emails to report@phishing.gov.uk, a new service run by the National Cyber Security Centre (NCSC) Suspicious Email Reporting Service. The NCSC's automated programme will immediately test the validity of the site and if found to be phishing scams, they will be removed immediately.
- Do not give out your/do not let your child give out, personal information to websites or in response to emails/text messages you/they do not recognise or trust.
- If you think you/your child has been scammed, defrauded or experienced cyber crime **Action Fraud** is the UK's national reporting centre for fraud and cyber crime.

4. **Check the facts**

Not all information online is reliable. Before your child likes, comments or shares something online they need to use the SHARE checklist to make sure they're not contributing to the spread of harmful content:

- **Source** - make sure information comes from a trusted source
- **Headline** - always read beyond the headline
- **Analyse** - check the facts
- **Retouched** - does the image or video look as though it has been doctored?
- **Error** - look out for bad grammar and spelling

The SHARE checklist can help you understand and spot disinformation and **NewsGuard** has a free tool to help the public identify fake news.

5. **Take breaks**

Make sure that your child takes regular breaks from their screens. There are a range of tools available to help you manage their screen time:

[Apple's Screen Time](#)

[Google's Family link](#)

[Xbox One](#)

[Playstation 4](#)

[Nintendo Switch](#)

Videoconferencing



When children are unable to attend school for a period of time, such as during a pandemic, the school may use video conferencing to keep in touch with pupils and/or enable pupils to keep in touch with each other. Such events require parental consent, and will follow relevant guidance for safeguarding. Children will be instructed on use, such as understanding that they may be muted to facilitate communication through turn-taking and listening, and that invitations are for them only. Two members of staff will be present at any one time throughout the session.

Advice for parents and carers for keeping children safe online during COVID-19

During the recent pandemic many of our children were studying at home, and home study may return at some point. It is important for your child/children to stay both connected and safe online during such times.

Have a conversation with your child about staying safe online

Most children have a positive experience online, accessing educational resources and entertainment and connecting with friends and family. Spending time online can be beneficial for children, particularly at the moment, but we recognise that many parents may worry about online safety.

Make use of parental controls

If you have downloaded new apps or bought new devices like web cams or tablets, remember to adjust the privacy and security settings to suit you.

There is technology to help you manage the content your children can access. The Government has encouraged Internet Service Providers to help parents easily filter content. Switch on family friendly filters to help prevent age inappropriate content being accessed on devices in your home. Parental controls put you in control of what your child can see. **Internet Matters** has step by step guides on how to set these up.

If you are concerned or upset about something your child has seen online, seek support from the online platform using the report function on the app or website - you can often find these in the 'help' section or 'settings' or seek support from other organisations and helplines.

The UK Safer Internet Centre offers a service, **Report Harmful Content**, which you can use if you are not satisfied with the result of a report.

Reduce the risk.

The **UK Council for Internet Safety** has guidance on minimising children's exposure to risks online. The **UK Safer Internet Centre** with **Childnet International** has specific guidance on under 5s.



Talk to your child

Childnet has guidance for parents and carers to begin a conversation about online safety and **Ditch the Label** teacher resources that can be helpful for parents to discuss cyberbullying and the government also has helpful advice. Encourage your child to speak to you or a trusted adult if they come across content that makes them uncomfortable.

If you have concerns about specific serious harms, this [guidance outlines how to protect your child](#) from the various forms of online abuse. See also Haselworth's Child Protection and Safeguarding policy.

Stay safe and healthy

If you are concerned about how long your child is using their device/deviceless, the government has published [guidance for parents and carers](#) on supporting children and young people's mental health and wellbeing during COVID-19.

The UK's Chief Medical Officer has also provided [advice on screen time](#).

Here are a few of the tips to help your children strike a balance:

- **Sleep matters** Getting enough good quality sleep is very important. Leave phones outside the bedroom when it is bedtime.
- **Sharing sensibly** Talk about sharing photos and information online and how photos and words are sometimes manipulated. Parents and carers should never assume that children are happy for their photos to be shared. For everyone – when in doubt, don't upload!
- **Talking helps** Talk with children about using screens and what they are watching. A change in behaviour can be a sign they are distressed – make sure they know they can always speak to you or another responsible adult if they feel uncomfortable with screen or social media use.
- **Keep moving!** Everyone should take a break after a couple of hours sitting or lying down using a screen. It's good to get up and move about a bit. #sitlessmovemore
- **Family time together** Screen-free meal times are a good idea – you can enjoy face-to-face conversation, with adults giving their full attention to children.
- **Use helpful phone features** Some devices and platforms have special features – try using these features to keep track of how much time you (and with their permission, your children) spend looking at screens or on social media.



Useful links

Organisation	Link
BBC	The BBC's Own It app helps children stop and think before they press the 'send' button.
Childnet	A tool kit to support parents and carers of any age child to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support.
CTIRU	You can report terrorist content they find online through the public referral tool . More information about what to report and what happens when you make a report.
Every Mind Matters	Advice and simple tips on how to maintain your mental wellbeing if you need to stay at home during the coronavirus outbreak
Internet Matters	StaySafeStayHome online resources and advice to support families.
Let's Talk About It	Support for parents and carers to keep children safe from online radicalisation .
LGfL	Support for parents and carers to keep their children safe online , including 6 top tips to keep primary aged children safe online.
Net-aware	Support for parents and carers from NSPCC, providing a guide to social networks, apps and games .
Parent Info	Provides support and guidance for parents from leading experts and organisations.
Rise Above	Public Health England's Rise Above social marketing programme aims to help build resilience and support good mental health of young people aged 10-16.
Thinkuknow	Provides advice from the National Crime Agency (NCA) to stay safe online. To help families manage during this time, the NCA has launched #OnlineSafetyAtHome , a set of fun, engaging activities based on Thinkuknow cartoons, films, games, and advice articles.
UK Council for Internet Safety	Education for a Connected World . A framework to equip children and young people for digital life.



Acceptable Usage Policy - KS1 Children

These rules have been written to make sure that you stay safe when using the computers. This includes cameras, laptops and microphones too. By using the technology in school, you have agreed to follow these rules.

Your teacher will talk about these rules before you sign them and a copy will be sent home to your parents.

If you have any questions, please ask your teacher.

The Golden Rule: Think before you click

- 😊 I will be careful when going on the internet.
- 😊 I will tell a teacher if I see something that upsets me.
- 😊 I know people online might not be who they say they are.
- 😊 I will be kind and polite when talking to people or writing online.
- 😊 I will think before I print or delete.
- 😊 I will be careful when using or carrying equipment.
- 😊 I will keep my password secret, but I can tell my family.
- 😊 Remember to log off properly before closing the lid of the laptops.
- 😞 I won't tell anyone any personal details like my phone number or last name.
- 😞 I won't logon using someone else's username.

Signed: (Pupil) _____ Class _____

Date _____



Acceptable Usage Policy - KS2 Children

This document is to provide some guidelines to ensure that you stay safe and act responsibly when using the computers.

When we talk about Computing, we are talking about computers, laptops, tablets and other electrical equipment, including cameras and other devices. By using the technology in school, you have agreed to follow these rules. These rules will be discussed with you as a class before you sign them and link to our school rules. A copy of this will also be sent home to your parents.

If you have any questions, please ask your teacher.

- At all times, I will think before I click (especially when deleting or printing)
- When using the internet, I will think about the websites I am accessing, and make sure they are appropriate and used to help my learning
- If I find a website or image that is inappropriate, I will shut the lid of my laptop or switch off the tablet and tell my teacher straight away
- When using information or pictures from websites, I will try and say which website it came from and if possible link back to the site
- When communicating online (in blogs, email, Virtual Learning Environments (VLEs), video conferencing [eg Zoom], etc.) I will think about the words that I use and will not use words or images that may offend other people.
- When communicating online, I will only use my first name and not share personal details such as my email address or phone number
- I understand that people online might not be who they say they are
- I will not look at other people's files or documents without their permission
- I will not logon using another person's account without their permission
- I will think before deleting files
- I will think before I print
- I know that the teachers can, and will, check the files and websites I have used
- I will take care when using the computers and transporting equipment around
- I will make sure the laptops have shutdown (so the power light is not lit up), before shutting the lid.
- I will keep my usernames and passwords secure, but I understand I can share them with appropriate people, such as my parents or teachers
- I will not install any software or hardware (including memory sticks) without permission from a teacher
- I understand that if I am acting inappropriately then my parents may be informed
- If I bring a mobile to school, I will hand it in at the start of the day. I will not bring any other device, such as a tablet, into school.

Signed: (Pupil) _____ Class _____

Date _____



Be Internet Legends.



Think Before You Share

I will thoughtfully consider what I share and with whom, and keep extra-sensitive information to myself (such as my home address, current location, or other people's business).



Check it's For Real

I will watch out for phishing and scams, and report questionable activity every time.



Protect Your Stuff

I will take responsibility for protecting important information by crafting strong and unique passwords with characters, numbers, and symbols.



Respect Each Other

I will spread positivity and use the skills I have learned to block and report negative behaviours.



When in Doubt, Discuss

I will use my voice when I notice inappropriate behavior and seek out a trusted adult to discuss situations that make me uncomfortable. Because that's what it takes to be a safe and fearless explorer of the online world.