Hingham Primary School

Online Safety and Internet Access Policy

Formally adopted by the Governing Body/ Trust of:-	**Hingham Primary School**
On:-	March 2026
Chair of Governors/Trustees:-	Susan Gothard
Review date:-	March 2027

Introduction

It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings.

This Policy document is drawn up to protect all parties: the students, the staff and the school. It aims to provide clear advice and guidance on how to minimise risks and how to deal with any unacceptable use.

NURTURE – LEARN - ACHIEVE

Adults need to **nurture** and model safe, independent use of the technology so that children are prepared for their next stage of learning. Children need to be kept safe, where possible, and be taught how to be resilient when problems arise in using the internet.

Children need to **learn** how to use the internet and be confident to use a range of technology to support their studies.

In order to **achieve** in the 21st century we must ensure our children can confidently adapt to changing and developing technology.

Roles and Responsibilities

Online safety and safe internet access is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school.

Governors

The School Governing body is responsible for overseeing and reviewing all school policies, including the Online Safety and Internet Access Policy.

Leadership team

The SLT ensures that the Policy is implemented across the school via the usual school monitoring procedures.

School Staff

All school staff are responsible for promoting and supporting safe behaviours and following school online safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials. Staff should ensure they are familiar with the school online safety policy, and ask for clarification where needed.

Class teachers should ensure that pupils are aware of the online safety rules, introducing them at the beginning of each new school year and reminding the children frequently (at least once a term). Use of Project Evolve in built into the curriculum.

Pupils

Pupils are expected to take an active part in planned lessons and activities to support their understanding and confidence in dealing with online safety issues, both at home and school.

They are asked to agree to a set of guidelines and rules covering their responsibilities when using technology at school.

Parents/ Carers

Parents and carers are given information about the school's Online Safety and Internet Access policy at their child's admission. Workshops are offered to inform parents and carers or the materials used with the children and to signpost further support.

We believe that **all adults** involved in bringing up children have a responsibility to teach, support and protect children when it comes to using the internet, particularly social media and gaming. Whilst it is vital that they are protected, we know that they cannot always be prevented from exposure to the potential harms.

Whole School Policy and Guidelines for Internet Access

The Internet is a valuable learning and administrative tool for adults and children alike. At Hingham Primary School, we encourage the use of the Internet to support and enhance children's learning and skills development. It is important that we acknowledge that the Internet is a tool to enhance learning and as such needs to be used appropriately to maximize its full potential. It is important to be aware of the critical part that the Internet and communications technology plays in lifelong learning and the requirements of future employment.

The statutory requirement for Computing in the National Curriculum 2014 states:

Computing also ensures that pupils become digitally literate – able to use, and express themselves and develop their ideas through, information and communication technology – at a level suitable for the future workplace and as active participants in a digital world.

The purpose of Internet access in school is to learn aspects of the computing curriculum, to support the broader curriculum, to support the professional work of staff and to enhance the school's management, information and business administration system.

As part of Keeping children Safe in Education (2025) there is a responsible to filter and monitor the systems in place. Our internet provider, SchoolsBroadband, functions both as a filtering tool and supports our monitoring by providing alerts and weekly reports. These are checked by the headteacher.

<u>Using the Internet for learning</u>

The Internet is an invaluable resource for learning for all our pupils, and we use it across the curriculum both for researching information and a source of digital learning materials. Using the Internet for learning is a part of the Computing Curriculum (Sept 2014). We teach all of our pupils how to find appropriate information on the Internet, and how to ensure as far as possible that they understand who has made this information available, and how accurate and truthful it is.

- ✓ Teachers plan Internet-based learning to teach the children how to ensure they are using appropriate and relevant materials.
- ✓ Children are taught how to use search engines and how to evaluate Internet-based information as part of the curriculum.
- ✓ They are taught how to recognise the difference between commercial and non-commercial web sites, and how to investigate the possible authors of web-based materials.
- ✓ They are taught how to carry out simple checks for bias and misinformation.
- ✓ They are taught that web-based resources have similar copyright status as printed and recorded materials such as books, films and music, and that this must be taken into consideration when using them.
- ✓ Children are able to independently use IT when appropriate to learning and this will involve being on devices that access the internet.

<u>Teaching safe use of the Internet and ICT</u>

We think it is crucial to teach pupils how to use the Internet safely, both at school and at home. To this end, we discuss internet safety in assemblies and in class, we acknowledge Safer Internet Day and we regularly revisit the issues around Internet safety. We have developed a progressive online safety curriculum through the Computing and PSHRE curriculum. We use the CEOP materials ("Think u know") to support our teaching and learning. For the younger children materials from Kidsmart.org.uk are used.

The main aspects include the following:

- Staying safe involves being careful and not giving out your name, address, mobile phone no., school name or password to people online. Children should avoid sharing images beyond "real-world" friends and not give out their location through status updates and messaging.

- Treat people online as you would in reality. You wouldn't invite someone you didn't know into your house or chat with strangers on the street– so don't do it online.

- Remember someone online may be lying and not be who they say they are. If you feel uncomfortable when chatting or messaging end the conversation.

- Tell your parent or carer if someone or something makes you feel uncomfortable or worried.

- Report to CEOP using the "report abuse" icon.

These points make up the S.M.A.R.T. acronym (https://www.childnet.com/young-people/primary)

S.M.A.R.T.

S – SAFE - Keep safe by being careful not to give out personal information when you are chatting or posting online. Keep personal information safe.
M – MEETING – Meeting someone you have only been in touch with online can be dangerous. Remember online friends are still strangers even if you have been talking to them for a long time.
A – ACCEPTING – Accepting messages, emails or opening files/pictures/texts from people you don't know or trust can lead to problems and they may contain viruses or be nasty messages.
R – RELIABLE – Someone online might lie about who they are and information on the internet may not always be true. Always check information from a range of sources and only chat to people who are your "real world" friends.
T – TELL – Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online. You can report abuse online to the police through www.thinkuknow.co.uk.

Suitable material

We encourage pupils to see the Internet as a rich and challenging resource, but we also recognise that it can be difficult to navigate and find useful and appropriate material. Where possible, and particularly with younger children, we provide pupils with suggestions for suitable sites across the curriculum, and staff always check the suitability of websites before suggesting them to children, or using them in teaching.

Non-Education materials

We believe it is better to support children in finding their way around the Internet with guidance and positive role modelling rather than restrict Internet use to strict curriculum based research.
As well as Internet material directly related to the curriculum, we encourage children to visit appropriate entertainment and child-oriented activity sites that have interesting and relevant activities, games and information, in free time at out-of-school-hours provision, and at home.
There is a selection of links to such resources available on the school website.

Unsuitable material

Despite the best efforts of the SchoolsBroadband and school staff, occasionally pupils may come across something on the Internet that they find offensive, unpleasant or distressing. Pupils are taught to always report such experiences directly to an adult at the time they occur, so that action can be taken.
The action will include:
1. Making a note of the website and any other websites linked to it.
2. Informing the ICT Administrator (JC Comtech Ltd) to remove access to the site.
3. Logging the incident – JC Comtech Helpdesk and add to CPOMS alerting the DSLs.
4. Discussion with the pupil about the incident, and how to avoid similar experiences in future
5. Discuss with a parent or carer to ensure the child receives support

Using E-Mail at school

E-Mail is a valuable and stimulating method of communication that plays an important role in many aspects of our lives today. We believe it is important that our pupils understand the role of e-mail, and how to use it appropriately and effectively.

- We may teach the use of e-mail as part of our computing curriculum, and use appropriate pupil email accounts where necessary.
- Pupils are not allowed to access personal e-mail using school Internet facilities.

Chat, discussion and social networking sites

These forms of electronic communication are used more and more by pupils out of school, and can also contribute to learning across a range of curriculum areas. Online chat rooms, discussion forums and social networking sites present a range of personal safety and privacy issues for young people. There is currently wide-ranging debate around social media and its impact on children and young people.

We use the resources, guidelines and materials offered by CEOP and Kidsmart, as outlined above in the Safe use of the Internet section to teach children how to use chat rooms safely.

All commercial Instant Messaging and Social Networking sites are filtered for the children's login. Pupils may take part in discussion forums or post messages on bulletin boards that teachers have evaluated as part of specific lesson activities. Individual pupil full names or identifying information will never be used.

Internet-enabled devices

More and more young people have access to sophisticated internet-enabled devices such as Smart mobile phones, Smart watches, Smart speakers, tablets and music players.

It is important that whilst the school recognises the potential advantages these devices can offer, there are clear and enforceable rules for their use in school, particularly when they give access to the Internet, and allow pictures and information to be remotely posted.

Pupils will be taught the legal and moral implications of posting photos and personal information from devices to public websites etc. and how the data protection and privacy laws apply.

Pupils are not allowed to have personal mobile phones, smart watches or other similar devices in school.
Parents may request that such devices are held by the teacher for pupils who may need them on their journey to and from school.

Cyberbullying and harassment
This is closely linked with our Anti-bullying policy.

Online bullying and harassment via messaging, texting, e-mail and chat rooms (including in-game) are potential problems that can have a serious effect on pupils. Our school has a range of strategies and policies to prevent online bullying, outlined in various sections of this policy.
These include:

- ✓ No access to social media and sites on which you can comment for children's log-ins.
- ✓ Pupils are taught how to use the Internet safely and responsibly, and are given access to guidance and support resources from a variety of sources.

We encourage pupils to discuss any concerns or worries they have about online bullying and harassment with staff, and have a range of materials available to support pupils and their families.

- ✓ Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy.
- ✓ Complaints related to child protection are dealt with in accordance with school child protection procedures.

Contact details and privacy

As specified elsewhere in this policy, pupil's personal details, identifying information, images or other sensitive details will never be used for any public Internet-based activity unless written permission has been obtained from a parent or legal guardian. Pupils are taught that sharing this information with others can be dangerous – see Teaching the Safe Use of the Internet.

School website – pictures and pupil input

As part of the Computing and wider curriculum, pupils may be involved in evaluating and designing web pages and web-based resources.

Any work that is published on a public website and attributed to members of our school community will reflect our school, and will therefore be carefully checked for mistakes, inaccuracies and inappropriate content.

Pupils may design and create personal web pages. These pages will generally only be made available to other school users, or as part of a password protected network or learning platform. Where pupil websites are published on the wider Internet, perhaps as part of a project with another school, organisation etc, then identifying information will be removed, and images restricted.

Where families have requested that their child does not have an image presence online (for example; through choice, as a Looked After Child or as a Post-Looked After Child), images will not be displayed. Parents and carers will have completed a *Photographs and Video Consent Form*. If at any time a parent/carer wishes to retract their consent they should complete a *Photographs and Videos Consent withdrawal* form available in the GDPR section of the website.

Deliberate misuse of the Internet facilities

All pupils have discussed the rules for using the Internet safely and appropriately.

Where a pupil is found to be using the Internet inappropriately, for example to download unsuitable games, or search for unsuitable images, then sanctions will be applied according to the nature of the misuse, and any previous misuse.

Sanctions will include:
Unsuitable material (e.g. online games, celebrity pictures, music downloads, sport websites etc)

- Initial warning from class teacher
- Banning from school hours Internet facilities
- Report to Headteacher
- Letter to parent/carer

Offensive material (e.g. pornographic images, racist, sexist or hate website or images etc)

- Incident logged and reported to Head teacher
- Initial letter to parent/carer
- Removal of Internet privileges/username etc
- Meeting with Parent/Carer to sign Internet use agreement
- Subsequent incidents will be treated very seriously by the Headteacher, and may result in suspension, exclusion and/or police involvement.
- Referral under the PREVENT agenda

In all circumstances support and education will be the priority to ensure the child knows how to keep themselves safe in the future.

How will complaints regarding Online Safety be handled?

It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings. Due to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions.
Sanctions available include:

- All incidents will be recorded
- Interview and support by class teacher and Headteacher;
- Counselling may be sought where necessary
- informing parents or carers;
- removal of Internet or computer access for a period,
- referral to LA / Police.

Class teachers act as first point of contact for any complaint. Any complaint about staff misuse is referred to the Head teacher.

Data Protection Policy

Our school is aware of the data protection law as it affects our use of the Internet, both in administration and teaching and learning.

We adhere to the LA Guidelines on Data protection and use DPE (Data Protection Education) for advice and guidance.

Staff and pupils are informed of the legal and disciplinary implications of using the Internet at school for illegal purposes.

Where appropriate, the police and other relevant authorities will be involved in cases of deliberate misuse or abuse of the Internet by members of the school community using the connection provided by the school.

Please also see Staff Code of Conduct, Internet Access policy and Anti-bullying policy

Last reviewed - 11.03.26