Updated: Autumn 2025
Next Review: Autumn 2026

Howe Dell Primary School and Day Care

e-Safety Policy

1. Introduction

Howe Dell Primary School and Day Care recognises that internet, mobile and digital technologies provide positive opportunities for children and young people to learn, socialise and play but they also need to understand the challenges and risks. The digital world is an amazing place, but with few rules. It is vast and fast moving, and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that **all** pupils, staff and governors will be supported to use internet, mobile and digital technologies safely. This is part of our safeguarding responsibility. Staff are aware that some pupils may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

We are also committed to ensuring that all those who work with children and young people, including their parents/carers, are informed about the ever-changing risks so that they can take an active part in helping children and young people navigate the online world safely and confidently.

At Howe Dell**,** we understand the responsibility to educate our pupils on e-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

2. Responsibilities

The Head teacher and governors have ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored. The named online safety lead in this school is Rick Xu (DPO).

All breaches of this policy must be reported to Rick Xu.
All breaches of this policy that may have put a child at risk must also be reported to the DSL, Tracy Prickett. Both can be contacted via the admin email address admin@howedell.herts.sch.uk with FAO Rick Xu / Tracy Prickett in the subject line.

Organisations that are renting space from the school and are a totally separate organisation should have and follow their own online safety policy and acceptable use agreements. If, however, they have any access to the school network, cloud-based services and/or equipment then they must adhere to the school's online safety procedures and acceptable use agreements. If an organisation doesn't have a policy, then school can support them to get one in place.

3. Scope of policy

The policy applies to:

- pupils
- parents/carers
- teaching and support staff
- school governors
- peripatetic teachers/coaches, supply teachers, student teachers
- visitors
- volunteers
- voluntary, statutory or community organisations using the school's facilities

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc.); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, and other mobile devices).

The school provides online safety information for parents/carers, for example, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting their child/ren to behave appropriately and keep themselves safe online.

This policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community. It is linked to the following other school policies and documents: safeguarding, Keeping Children Safe in Education, Early Years Framework, GDPR, health and safety, home–school agreement, google classroom user agreement, behaviour, computing, anti-bullying and PSHCE/RSE policies.

4. Policy and procedure

The school and Day Care seek to ensure that internet, mobile and digital technologies are used effectively and safely, for their intended educational purpose, in ways that will not infringe legal requirements or create unnecessary risk.

The school and Day Care expect everyone to use internet, mobile and digital technologies responsibly and strictly according to the conditions set out in this policy. This policy also includes expectations on appropriate online behaviour and use of technology outside of school for pupils, parents/carers, staff and governors and all other visitors to the school.

Use of email

Staff and governors should use a school email account or Governor Hub for all official school communication to ensure everyone is protected through the traceability of communication. Under no circumstances should staff contact pupils, parents or conduct any school business using a personal email address. Pupils should use school approved accounts on the school system for educational purposes. Where required parent/carer permission will be obtained for the pupil account to exist. For advice on emailing, sharing personal or confidential information or the need to gain parent permission refer to the policy for GDPR. Emails created or received as part of any school role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

Users must not send emails which are offensive, embarrassing or upsetting to anyone (i.e. cyberbullying).

Visiting online sites and downloading

- Staff must preview sites, software and apps before their use in school or before recommending them to pupils. Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with the Data Protection Officer with details of the site/service and seek approval from a senior leader. The terms and conditions of the service should be read and adhered to, and parental/carer permission sought where required. If internet research is set for homework, specific sites will be suggested that have been checked by the teacher. All users must observe copyright of materials from electronic sources

- Staff must only use pre-approved systems if creating blogs, wikis or other online content

  Users must not:

- Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative)

- Indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative)

- Adult material that breaches the Obscene Publications Act in the UK

- Promoting discrimination of any kind in relation to the protected characteristics: age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race or ethnicity, religion or belief, sex, sexual orientation

- Promoting hatred against any individual or group from the protected characteristics above

- Promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy

- Any material that may bring the school or any individual within it into disrepute e.g. promotion of violence, gambling, libel and disrespect

Users must not:

- Reveal or publicise confidential or proprietary information

- Intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses

- Transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given to the school
- Use the school's hardware and Wi-Fi facilities for running a private business

- Intimidate, threaten or cause harm to others

- Access or interfere in any way with other users' accounts

- Use software or hardware that has been prohibited by the school

Only a school/day care device or closed, monitorable system set up by the school for use on a personable device may be used to conduct school business outside of school. Such a system would ensure the user was not saving files locally to their own device and breaching data security. This would ensure any school documents accessed on a personal device are never actually on the computer being used, they remain on the school server. When the user logs-out of the monitorable system, there are no copies left on their own device.

All breaches of prohibited behaviours detailed above will be investigated, where appropriate, in liaison with the police.

The school and Day Care recognises that in certain planned curricular activities, access to controversial and/or offensive online content may be beneficial for educational use. In

such circumstances, there is an expectation that access is pre-planned, risk assessed and recorded, and permission given by the headteacher.

Storage of images

Photographs and videos provide valuable evidence of pupils' achievement and progress in a variety of contexts and can be used to celebrate the work of the school. In line with GDPR they are used only with the written consent of parents/carers which is secured in the first instance on a child's entry to the school and Day Care. Records are kept on file and consent can be changed by parents/carers at any time. (See GDPR policy for greater clarification).

Photographs and images of pupils are only stored on the school and Day Care's agreed secure networks which include some cloud based services. Rights of access to stored images are restricted to approved staff as determined by the headteacher. Staff and pupils may have temporary access to photographs taken during a class session, but these will be transferred/deleted promptly.

Parents/carers should note that there may be some children who are at risk and must not have their image put online and others who do not want their image online. For these reasons parents/carers must follow the school's Acceptable Use Agreement and refrain from posting online photographs of any member of the school community, other than their own child/ren.

Staff and other professionals working with pupils, must only use school equipment to record images of pupils whether on or off site. See also GDPR. Permission to use images of all staff who work at the school is sought on induction and a written record is located in the personnel file.

Publishing pupil images and work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school/day care web site
- in the school prospectus and Day Care registration form and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- on the school's or Day Care's learning platform or Virtual Learning Environment, Tapestry
- in display material that may be used in the school and Day Care's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school and Day Care
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

Parents or carers may withdraw permission, in writing, at any time.

Pupils' names will not be published alongside their image and vice versa. Email and postal addresses of pupils will not be published. Pupils' full names will not be published.

Use of personal mobile devices (including phones)

The school and Day Care allows staff, including temporary and peripatetic staff, and visitors to use personal mobile phones and devices only in designated areas and never in the presence of pupils. Under no circumstance does the school allow a member of staff to contact a pupil or parent/carer using their personal device.

Parents/carers may only use personal mobile phones and devices in designated areas unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises or on off-site school events and activities of anyone other than their own child, unless there is a pre-specified permission from the headteacher. When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight.

Only pupils in agreed year groups are allowed to bring personal mobile phones to school, but must, upon arrival in school, hand in their phone for safe storage by their teacher. These devices are not to be used during school operating hours unless for medical purposes.

Under no circumstance should pupils use their personal mobile devices/phones to take images of:

- any other pupil unless they and their parents have given agreement in advance
- any member of staff

Wearable devices (such as an apple watch, AI glasses) with access to the internet, or those that are connected to a mobile phone, are not permitted to be worn by pupils and staff and must not be brought onto the school premises.

The school is not responsible for the loss, damage or theft of any personal mobile device that is brought into school.

Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

New technological devices

New personal technological devices may offer opportunities for teaching and learning. However, the school and Day Care must consider educational benefit and carry out risk assessment before use in school is allowed. Parents/carers, pupils and staff should not assume that new technological devices will be allowed in school and should check with the headteacher before they are brought into school.

Reporting incidents, abuse and inappropriate material

There may be occasions in school when either a pupil or an adult receives an offensive, abusive or inappropriate message or accidentally accesses upsetting or abusive material. When such a situation occurs the pupil or adult must report the incident immediately to the first available member of staff, the DSL or the headteacher, Tracy Prickett. Where such an incident may lead to significant harm, safeguarding procedures should be followed. The school takes the reporting of such incidents seriously and where judged necessary, the DSL will refer details to social care or the police.

5. Curriculum

Online safety is embedded within our curriculum. The school provides a comprehensive age appropriate curriculum for online safety which enables pupils to become informed, safe and responsible. This includes teaching to prevent radicalisation, for which staff provide a narrative to counter extremism. The PSHE curriculum, Relationships and Health Curriculum are central in supporting the delivery of online safety education.

The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

It is necessary for pupils to develop skills of critical awareness, digital resilience and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly. Pupils are taught to recognise the creative, collaborative, cultural, economic and educational opportunities provided by the internet, mobile and digital technologies. Curriculum work will also include areas such as:

- Understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity

- Learning how to develop a positive online reputation and enhance future opportunities e.g. in relationships and employment

- Developing critical thinking skills and the confidence to challenge and question what they see and read in relation to online content e.g. recognising fake news and extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online pressure, learning how easy it is to lie online (i.e. users may not be who they say they are and may have ulterior motives Understanding the dangers of giving out personal details online and the importance of maintaining maximum privacy online

- Thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others

- Understanding the permanency of all online postings and conversations

- Understanding relevant legislation, including copyright, and the importance of respecting other people's information, reputation and images.

- Understanding the importance of online respect and what constitutes cyberbullying, how to avoid it, the impact it has and how to access help.

- How the law can help protect against online risks and abuse

6. Staff and Governor Training

Staff and governors are trained to fulfil their roles in online safety. The school audits the training needs of all school staff and provides regular training to improve their knowledge and expertise in the safe and appropriate use of internet, mobile and digital technologies. This training is recorded as part of safeguarding records.

New staff are provided with a copy of the e-safety policy and must sign the school's Acceptable Use Agreement as part of their induction and before having contact with pupils.

Any organisation working with children and based on the school premises are also provided with a copy of the online safety policy and required to sign the Acceptable Use Agreement.

Peripatetic staff, student teachers and regular visitors are provided with a copy of the online safety policy and are required to sign the Acceptable Use Agreement

Visitors, volunteers and parent/carer helpers will be provided with relevant information prior to their access to school premises.

7. Working in Partnership with Parents/Carers

The school and Day Care work closely with families to help ensure that children can use internet, mobile and digital technologies safely and responsibly both at home and school. The support of parents/carers is essential to implement the online safety policy effectively and help keep children safe.

It is important that parents/carers understand the crucial role they play in this process. The school and Day Care seek to regularly consult and discuss online safety with parents/carers and seeks to promote a wide understanding of the benefits of new technologies and associated risks. The school provides regular updated online safety information through the school website, newsletters and by other means.

Parents/carers are asked on an annual basis to read, discuss and co-sign with each child the Online Safety Expectations: Acceptable Use Agreement. The Acceptable Use Agreement explains the school's expectations and pupil and parent/carer responsibilities.

8. Records, Monitoring and Review

The school recognises the need to record online safety incidents and to monitor and review policies and procedures regularly in order to ensure they are effective and that the risks to pupils and staff are minimised.

The Senso monitoring system provides the headteacher with weekly updates and significant breeches. The headteacher undertakes fortnightly monitoring of all incidents logged.

All breaches of this policy must be reported and all reported incidents will be logged. All staff have the individual responsibility to ensure that incidents have been correctly recorded, acted upon and reported to the headteacher and using the agreed recording system. This school records incidents on CPOMS.

The school supports pupils and staff who have been affected by a policy breach. Where there is inappropriate or illegal use of internet, mobile and digital technologies, this will be dealt with under the school's behaviour and disciplinary policies as appropriate. Breaches may also lead to criminal or civil proceedings.

Governors receive termly summary data on recorded online safety incidents for monitoring purposes. In addition, governors ensure they have sufficient, quality information to enable them to make a judgement about the fitness for purpose of this policy on an annual basis.

Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct (revised September 2024)

ICT (including data) and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Computing Subject leader.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed acceptable by the Head or Governing Board
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role and adhere to the professional standards
- I will not give out my own personal details, such as mobile phone number, personal email address, personal Twitter account, or any other social media link, to pupils
- I will only use the approved, secure email system(s) for any school business
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Board. Personal or sensitive data taken off site must be encrypted, e.g. on a password secured laptop or memory stick/hard drive
- I will not install any hardware or software without permission of the Computing Subject Leader.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member
- I will only use school devices to take images of children/staff
- Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher
- I will support the school approach to online safety and not upload or add any images, video, sounds or text linked to or associated with the school or its community'
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher
- I will respect copyright and intellectual property rights
- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional reputation, or that of others, into disrepute
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies
- I understand this forms part of the terms and conditions set out in my contract of employment
- I am happy to have my photograph taken for school purposes and understand it may be used for professional purposes

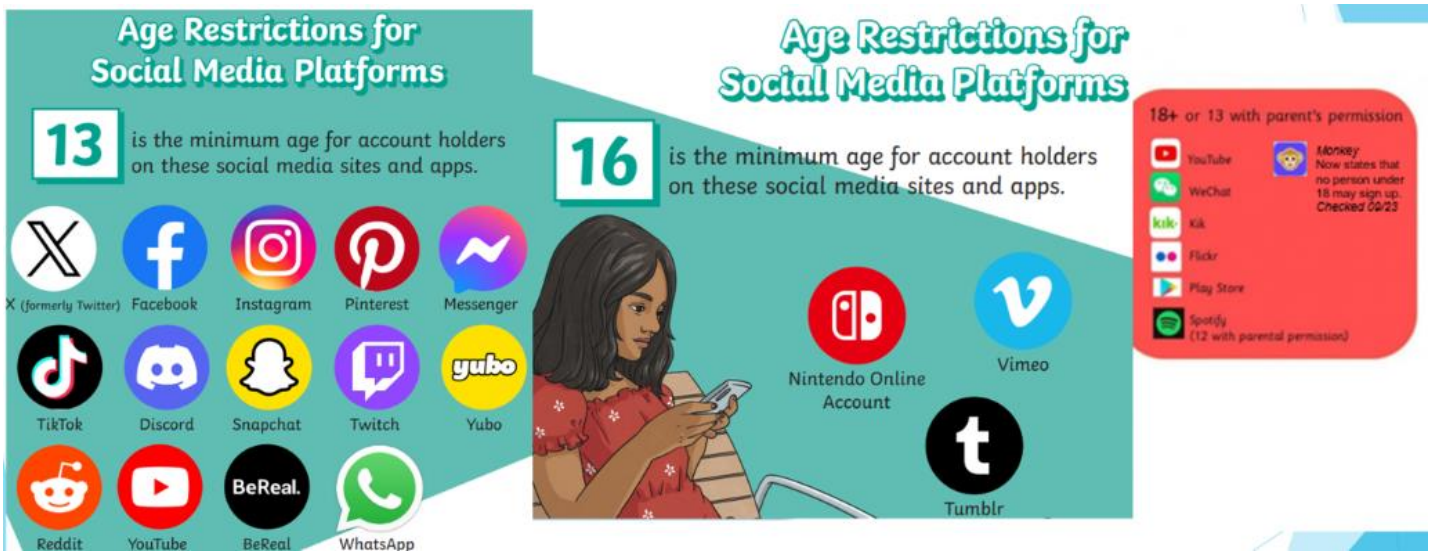
User Signature
I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school
Signature …….…… Date ……

Full Name ……..... (printed)

Job title ……

Dear Parent/Carer,
ICT and Computing (including the internet, Google Classroom, emails, blogging and mobile technologies) is an important part of learning at Howe Dell. We expect all children to be safe and responsible when using any ICT at home and at school.
As part of Howe Dell's commitment to safeguarding, we monitor activity on school accounts and devices. Content and use will be checked by the Executive Head regularly to ensure all users comply with the acceptable use agreements. Unacceptable activity is filtered and flagged.

Please read and discuss these e-Safety rules overleaf with your child and return the slip at the bottom of this page. If you have any concerns, or would like any further details, please contact the school office.



For your information, please also find below information regarding social media age restrictions.

Yours sincerely,

Tracy Prickett
Executive Headteacher

Parent/ carer agreement

Parent(s)/Carer(s) name(s)……

I/we have discussed this agreement with, which highlights the associated risks when accessing the internet, mobile and digital technologies, with our child/ren.
I/we agree to support them in following the terms of this agreement.
We understand that our child's use of ICT can be checked in school and that we will be contacted if a member of school staff is concerned about our child's e-Safety.

Pupil name …… Class …….

I understand this agreement is to keep me safe. I have discussed this agreement with my parents/carers and I understand my responsibilities when using ICT equipment and accessing information and media online.

Our Online Safety Expectations
Acceptable Use Agreement

- I will only use school IT equipment for school purposes
- I will only use my own school e-mail address and school accounts. I will not use other people's accounts and pretend to be them online
- I will not tell other people my passwords
- I will only open links or attachments from people I know, or that my teacher has approved
- I will only open or delete my own files
- I will make sure that all IT contact with other children and adults is responsible, polite and sensible
- If I come across anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, I will tell my teacher or an adult at home immediately
- If someone posts about me, sends me anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, I will not reply. I will tell my teacher or an adult at home immediately
- I will not give out my own or other people's details such as name, phone number or home address. I will tell a teacher or an adult at home if someone online asks me for any information
- I will not arrange to meet someone I have contacted online or send my image unless this is part of a school project and a teacher, or an adult at home is supervising me
- I will always seek permission before I share my image (photographs, videos, live streaming, video calling) online as this can put me at risk
- I will not bring a recordable device or internet accessible smart watch to school because I am not allowed to wear one during the school day
- I will not sign up to online services or social media accounts until I am old enough
- I will not access age-inappropriate internet technologies outside of school
- I will support the school approach to online safety and not upload any images, video, sounds or text that could upset any member of the school community
- I understand that everything I do or receive online can be traced, so I will be responsible for my behaviour when using IT because I know these rules keep me safe
- I know that my use of IT in school is checked and my parent/carer contacted if any member of staff is concerned about my safety
- I understand that as part of Howe Dell's commitment to safeguarding, the school is able to monitor activity on school accounts and devices. Content and use will be checked regularly to ensure all users comply with the acceptable use agreements. Unacceptable activity will be filtered and flagged