THE HASELWORTH WAY PO12

GOSPORT

HASELWORTH PRIMARY SCHOOL
ACCEPTABLE USE OF ICT and AI Policy (Staff, Pupils and Stakeholders)

Policy approved:	**18th May 2026**	**FGB**
Signed:	*N Jones*	**Headteacher**
Signed:	*Dr C Roast*	**Chair of Governors**
Date of next review:	**Summer 2028**	**Bi-Annually**
Monitored and evaluated by:	**Headteacher**	**Termly**

1. Creating a Safe ICT Infrastructure in School

All users of the school's computer network have clearly defined access rights, enforced using a username/password login system. Account privileges are achieved through the file/folder permissions, and are based upon each user's particular requirements – children have more limitations in place through their standard pupil login, than staff members do with their individual logins. This helps to protect the network from accidental or malicious attempts to threaten its security or the stored data.

Visitors (eg supply teachers) are requested to login using a supply login to prevent them viewing any potentially confidential data that might be stored on the schools' drives.

A permanently-enabled and flexible filtering system is provided to the school, which is designed to filter out material found to be inappropriate for use in the education environment. As an additional safety measure, each individual web page is also dynamically scanned for inappropriate content as it is requested, categorised by its content and then access prevented to it if necessary.

ESET Endpoint Anti-virus Security software is installed on all our *Windows* operating machines to prevent any occurrence of malware (e.g. virus) attacks.

Staff should be aware that internet traffic is monitored and can be traced to the individual user. Professional conduct is essential. It is the responsibility of the user to ensure that they have logged off the system when they have completed their tasks and to keep their user credentials confidential to avoid impersonation on the network.

All staff MUST lock their screens and computers when away from their desk or workstation, as stated in the school's Data Protection Policy.

2. Rules for Publishing Material Online (inc. Images of Pupils)

Whilst we wish the school's website to be a valuable tool for sharing information and promoting children's achievements with a global audience, we do recognise the potential for abuse that material published may attract, no matter how small this risk may be. Therefore, when considering material for publication on the website, the following principles should be kept in mind:

- If an image/audio/video recording of a child is used then they should not be named (including in credits).
- If a pupil is named, their image/audio/video recording should not be used (**no surnames should be published**).
- Files should be appropriately named in accordance with these principles and care should be taken to include only suitable ALT tags as well.
- Only images of children in suitable dress should be used and group photographs are preferred in preference to individual photographs.

- Parents are given the opportunity to withdraw permission for the school to publish images/audio/video of their child on the school website.
- Content should not infringe the intellectual property rights of others – copyright may apply to: text, images, music or video that originate from other sources. All copied or embedded content should be properly referenced.
- Content should be polite and respect others.
- Material should be proof-read (e.g. to check for spelling or grammatical errors) before being published.

Comments submitted to posts on Seesaw must be moderated by the post's author before being published (to ensure they are appropriate and reveal no personal information).

Children will likely use a variety of online tools for educational purposes during their time at the school. They will be asked to only use their first name or a suitable avatar for any work that will be publicly accessible and be required to follow the principles listed above before sending any work for publishing. Staff should encourage contributions that are worthwhile and develop a particular discussion topic.

When photo/videos of school events (e.g. plays) are taken by the school, we will not publish them onto any public area of the Internet, including social networking sites. Parents are not permitted to take photographs at events.

3. Pupils' Rules for Acceptable Internet and Computer Use

Educational use of the Internet is characterised by activities that provide children with appropriate learning experiences. Clear rules which help children develop a responsible attitude to the use of the Internet have been devised. Clear expectations and rules regarding use of the Internet will be explained to all classes.

- Only use the internet in class when a teacher, Learning Support Assistant or other adult is there to supervise you.
- Always tell a responsible adult or whoever is looking after you what you intend to look at on the internet.
- Only use web sources that you know are reliable.
- Only use your own username and password on the network.
- Never give out contact or personal details e.g. mobile phone number for anyone else.
- Do not talk to people you don't know in chat rooms, on social media, via internet sites or via webcam.

  Respect other people's work and privacy.
- Only download or use materials with the owner's permission.
- If you come across anything that you think is not suitable or anything that makes you feel uncomfortable tell an adult.

- If you know that someone else is not behaving appropriately on the internet – either at school or home then tell someone in your family or a teacher.
- If you receive anything which upsets you, tell an adult.
- Never use a personal memory stick in the school computers.

All children in Key Stage 2 are given a network login and password. This provides them with a secure area where their work can be stored, whereas children in Key Stage 1 have a generic class login, which can be monitored by their teachers.

4. Visitor's Rules for Acceptable Internet Use

Whilst the nature of a visitor's Internet use will vary depending upon the purpose of their visit, it is still important to explain the school's expectations and rules regarding safe and appropriate Internet use to them. These differ slightly to those given to pupils to acknowledge the different situations in which visitors will likely be using the Internet, whether through school hardware or through their own internet enable devices, like mobiles, tablets etc:

- I will respect the facilities on offer by using them safely and appropriately.
- I will not use the Internet for: personal financial gain, political purposes, advertising, personal or private business.
- I will not deliberately seek out inappropriate websites.
- I will report any unpleasant material to a member of staff immediately because this will help protect myself and others.
- I will not download/install program files to prevent data from being corrupted and to minimise the risk of viruses.
- I will be polite and respect others when communicating over the Internet.
- I will not share my login details for websites with others.
- I will not carry out personal or unnecessary printing when using the Internet due to the high cost of ink.
- I understand that the school may check my computer files and monitor the Internet sites I visit.

5. Staff/Governor's Rules for Acceptable ICT Use

This section applies to the school governing body, all employed staff, whether employed by the County Council or employed directly by the school, external contractors providing services on behalf of the school or the County Council, teacher trainees and other trainees, volunteers and other individuals who work for or provide services on behalf of the school. These individuals are collectively referred to in this policy as staff or staff members.

The section of the policy applies in respect of all ICT resources and equipment within the school and resources that have been made available to staff for working at home. ICT resources and equipment

includes computer resources, use of school internet access and email systems, software (including use of software such as SAP and Arbor), school telephones and text systems, cameras and recording equipment, intranet and virtual learning environment and any other electronic or communication equipment used in the course of the employee or volunteer's work.

This section also provides advice to staff in respect of the potential risks and consequences in relation to inappropriate use of their own personal ICT facilities, where this use is inconsistent with the expectations of staff working with children and young people.

5.1 *Access*

School staff will be provided with an individual log on where they are entitled to use the school ICT facilities and advised what hardware and software they are permitted to access, including access to the internet and email. Unless indicated, staff can use any facilities available subject to the facilities not being in use by pupils or other colleagues. Access is provided to enable staff to both perform their role and to enable the wider staff in the school to benefit from such facilities.

Where staff have been provided with a school email address to enable them to perform their role effectively, it would not normally be used to communicate with parents and pupils unless express permission has been provided by the Headteacher. Where staff are able to access email outside of school's hours, the email facility should not routinely be used to undertake school business outside of normal office hours.

Access to certain software packages and systems (e.g HCC intranet; SAP (HR, finance and procurement system, Arbor, school texting services and CPOMS) will be restricted to nominated staff and unless permission and access has been provided, staff must not access these systems.

Some staff may be provided with laptops and other equipment for the performance of their role. Where provided, staff must ensure that their school laptop/other equipment is not accessible by others when in use at home and that it is not used inappropriately by themselves or others. Staff must also ensure that they bring their laptop/equipment in as required for updating of software, licences and virus protection. Staff must ensure they do not leave school property including ICT equipment in vehicles or away from their person.

Where the school provides digital cameras and other recording equipment for educational and school business use and it is used away from the school site, it must be kept secure and safe. Where pictures of pupils are taken, staff must ensure that they ensure consent has been provided by parents, and that the school's policy in relation to use of pictures, is followed.

Staff may use, in urgent or emergency situations during off site visits, their personal mobile telephones. Where used in these emergency situations and a cost incurred, the school will provide reimbursement of the cost of any calls made. Should staff need to make contact whilst off site, this should normally be undertaken via the school rather than a direct call to an individual's personal mobile. School staff who have access to colleagues' personal contact details must ensure that they

are kept confidential. In the event of staff needing to use personal telephones they must ensure they withhold their number by using #141.

No mobile telephones or similar devices, even those with hands free facilities should be used whilst driving on school business.

The school telephone system should not be used for personal use. Where necessary in an emergency, calls must be made during break periods, must not be excessive and the school should require either the cost of the call or a donation to be made towards the cost of the call.

The school will ensure that Display Screen Equipment assessments are undertaken in accordance with its Health and Safety Policy.

5.2 Communication with parents, pupils and governors

The school communicates with parents and governors through a variety of mechanisms. The points below highlight who is normally authorised to use which systems and can directly communicate without requiring any approval before use or to agree content. School must indicate to staff if any other staff are permitted to make contact using the systems below:

- School Telephones – all teachers, LSAs, administrative staff and staff who have been permitted through their roles in pupil welfare or a home/school link staff.

- Text System – All Office staff. Where other staff need to send a text, this is normally approved by a member of the Senior Leadership Team.

- Letters – Staff should send a draft to the office to edit and send out. Sometimes it may be necessary for teachers to send communications and letters direct in hard copy to their parents. Copies of all letters sent out must be sent to the office.

- Email – school email accounts should not be used for communication with parents unless approved by the Headteacher. Email is used as a normal method of communication amongst school governors and where governors are linked in particular areas with members of staff, communication may take place via email.

- Visits home – All home visits are normally subject to approval by the senior leadership team

- Under no circumstances should a member of staff communicate directly with a pupil using any of the methods outlined above

Where pupils are submitting work electronically to school staff, this must be undertaken using school systems and not via personal email. Seesaw is the main method for this communication.

5.3 Staff Personal Use of Social Media

School staff are advised to exercise extreme care in their personal use of social networking sites, giving consideration to their professional role working with children. Staff should make appropriate use of the security settings available through social networking sites and ensure that they keep them updated as the sites change their settings. Staff are advised that inappropriate communications that come to the attention of the school can lead to disciplinary action, including dismissal.

The school recognises that many staff will actively use social media apps and websites including *WhatsApp, Facebook*, *Twitter, Instagram* and other such blogging, vlogging and messaging services. This includes sites to support their own professional development by fostering personal learning networks with other educational practitioners.

Staff must recognise that it is not appropriate to discuss issues relating to the children, school or other staff via these networks – discretion and professional conduct is essential. They are encouraged to review their privacy settings to make sure that their profiles and photographs are not accessible by the general public.

In accordance with school's *Child Protection Policy and Safeguarding Policies*, it is never acceptable to accept a friendship request from a child from the school as in almost all cases children of primary age using such networks will be breaching the terms and conditions of use of those networks. It is also extremely inadvisable to accept friend's requests from ex-pupils who are still minors, again avoid any possible misinterpretation of their motives or behaviour which could be construed as grooming.

Staff should not give their personal contact details to pupils including e-mail, home or mobile telephone numbers. All correspondence should be via school systems. Section 8 of this policy contains detailed advice on the expectations of all stakeholders when using social media.

5.4 Unacceptable Use

Appendix 1 provides a list of Do's and Don'ts for school staff to enable them to protect themselves from inappropriate use of ICT resources and equipment. School systems and resources must not be used under any circumstances for the following purposes:

- to communicate any information that is confidential to the school or to communicate/share confidential information which the member of staff does not have authority to share;

- to present any personal views and opinions as the views of the school, or to make any comments that are libellous, slanderous, false or misrepresent others;

- to access, view, download, post, email or otherwise transmit pornography, sexually suggestive or any other type of offensive, obscene or discriminatory material;
  to communicate anything via ICT resources and systems or post that may be regarded as defamatory, derogatory, discriminatory, harassing, bullying or offensive, either internally or externally;

- to communicate anything via ICT resources and systems or post that may be regarded as critical of the school, the leadership of the school, the school's staff or its pupils;

- to upload, download, post, email or otherwise transmit or store material that contains software viruses or any other computer code, files or programmes designed to interrupt, damage, destroy or limit the functionality of any computer software or hardware or telecommunications equipment;

- to collect, transfer or store personal information about others without direct reference to the General Data Protection Regulation (GDPR).

- to use the school's facilities to undertake any trading, gambling, other action for personal financial gain, or political purposes, unless as part of an authorised curriculum project;

- to visit or use any online messaging service, social networking site, chat site, web based email or discussion forum not supplied or authorised by the school;

- to undertake any activity (whether communicating, accessing, viewing, sharing. uploading or downloading) which has negative implications for the safeguarding of children and young people;

Any of the above activities are likely to be regarded as gross misconduct, which may, after proper investigation, lead to dismissal. If employees are unsure about the use of ICT resources including email and the intranet, advice should be sought from a member of the Senior Leadership Team.

Where an individual accidently or unintentionally accesses a website or material that contains any prohibited content, they must leave the site immediately and inform the Headteacher, DSL, DDSL or other member of the senior leadership team. Schools are encouraged to use appropriate blocking software to avoid the potential for this to happen. Reporting to the Headteacher or senior leadership team equally applies where school staff are using school equipment or facilities at home and accidentally access inappropriate sites or material. Genuine mistakes and accidents will not be treated as a breach of this policy. Agile Web monitoring reports track an individual's use of the internet.

Where an individual has been communicated with in a manner outlined above (e.g. has received an inappropriate email or attachment), they are advised to report this immediately to the Headteacher or another member of the senior leadership team so that this can be dealt with appropriately.

5.5 Personal and private use

All school staff with access to computer equipment, including email and internet, are permitted to use them for occasional personal use provided that this is access is not:

- taking place at the expense of contracted working hours (i.e. is not taking place during paid working time)

- interfering with the individual's work
- relating to a personal business interest
- involving the use of news groups, chat lines or similar social networking services
- at a cost to the school
- detrimental to the education or welfare of pupils at the school

Excessive personal use of school facilities is likely to be considered to be a disciplinary matter, may lead to restricted access to computer equipment and where costs are incurred (e.g. personal telephone use), the school will seek reimbursement from the member of staff.

It is important for staff to also be aware that inappropriate use of their own personal or other ICT facilities in their personal time, can have implications for their employment situation where this becomes known and the activities that are undertaken are inconsistent with the expectations of staff working with children and young people.

School staff should not use any of their personal ICT equipment for school use. Mobile phones are the exception, when logging incidents on CPOMs due to the limited amount if ICT equipment. Please refer to the mobile phone policy for further details.

Whilst individuals may be required to use their personal mobile telephone to make contact with the school, staff should exercise care and seek reimbursement as outlined in section 3.

5.6 Security and confidentiality

Any concerns about the security of the ICT system should be raised with a member of the senior leadership team.

Staff are required to ensure that they keep any passwords confidential, do not select a password that is easily guessed and regularly change such passwords.

School staff must take account of any advice issued regarding what is permitted in terms of downloading educational and professional material to the school server. Where staff are provided with an encrypted memory stick for such activity, to both protect the integrity of the server and to save space, this should be used. All staff must review the appropriateness of the material that they are downloading prior to downloading and are encouraged to do so from known and reputable sites to protect the integrity of the school's systems. Where problems are encountered in downloading material, this should be reported to the school's Admin Team.

Staff are permitted to download and upload work to the school server through their encrypted memory stick. Staff will be held responsible for any data lost or misused according to the GDPR.

Staff must ensure that they follow appropriate and agreed approval processes before uploading material for use by pupils to the pupil ICT system and/or VLE.

If staff need to place content on the school website, please see the Headteacher for the school agreed approval processes before uploading material to the website.

Agile will be responsible for ensuring that all equipment is regularly updated with new software including virus packages and that licences are maintained on all school based and school issued equipment. Staff must ensure that they notify Agile if they have any concerns regarding potential viruses, inappropriate software or licences.

Staff must ensure that their use of the school's ICT facilities does not compromise rights of any individuals under the GDPR. This is particularly important when using data off site and electronic data must only be taken off site in a secure manner, either through password protection on encrypted memory sticks, with permission from a member of the senior Leadership Team. This is also particularly important when communicating personal data via email rather than through secure systems. In these circumstances, staff must ensure that they have the correct email address and have verified the identity of the person that they are communicating the data with. It is not acceptable for staff to download documents or photographs from the school network on to any device for transfer to a private device, staff must use their encrypted memory stick. Staff must not use their encrypted memory stick for personal use to download school documents to any personal device.

If it is necessary in your role to transfer personal data of staff or pupils to other organisations, including within the LA, the Transfer of Records procedures must be applied. These procedures are detailed in the Data Protection Policy. Please see the school's Data Protection Officer, Mrs S Rix, for advice regarding these procedures.

All staff taking paper copies of data or pupil work home, must securely transfer. Please see the Data Protection policy for further details.

Staff must also ensure that they do not compromise any rights of individuals and companies under the laws of Copyright through their use of ICT facilities.

5.7 Monitoring

The school uses Agile's IT services and therefore is required to comply with their email, internet and intranet policies.

The school and Agile reserve the right to monitor the use of email, internet and intranet communications and where necessary data may be accessed or intercepted in the following circumstances:

- to ensure that the security of the school and county council's hardware, software, networks and systems are not compromised
- to prevent or detect crime or unauthorised use of the school or county council's hardware, software, networks or systems
- to gain access to communications where necessary where a user is absent from work

Where staff have access to the internet during the course of their work, it is important for them to be aware that the school or Agile may track the history of the internet sites that have been visited.

To protect the right to privacy, any interception of personal and private communications will not take place unless grounds exist to show evidence of crime, or other unlawful or unauthorised use. Such interception and access will only take place following approval by the Chair of Governors, after discussions with relevant staff in Hampshire County Council's HR, Agile and Audit Services and following an assessment to determine whether access or interception is justified.

5.8 Protected Disclosure and cyberbullying

Staff who have concerns about any abuse or inappropriate use of ICT resources, virtual learning environments, camera/recording equipment, telephony, social networking sites, email or internet facilities or inappropriate communications, whether by pupils or colleagues, should alert the Headteacher to such abuse. Where a concern relates to the Headteacher, this should be disclosed to the Chair of Governors. If any matter concerns child safety, it should also be reported to the Designated Safeguarding Lead (DSL).

It is recognised that increased use of ICT has led to cyberbullying and/or concerns regarding e-safety of school staff. Staff are strongly advised to notify their Headteacher where they are subject to such circumstances. Advice can also be sought from professional associations and trade unions. Support is also available through Hampshire's confidential counselling service, Employee Support (0800 030 5182) and also via the UK Safer Internet Centre helpline@safetinternet.otg.uk or 0844 381 4772.

5.9 Signature

It will be normal practice for staff to read and sign a declaration as outlined in Appendix 2, to confirm that they have had access to the acceptable use policy and that they accept and will follow its terms.

Staff must comply with the terms of this policy. Any breach will be considered to be a breach of disciplinary rules, which may lead to a disciplinary sanction (e.g. warning), dismissal, and/or withdrawal of access to ICT facilities. Staff should be aware, that in certain instances, inappropriate use of ICT may become a matter for police or social care investigations.

6. Internet Use Contracts

Both pupils and their parents/carers are asked to read the school's *Rules for Acceptable Internet and Computer Use* and are required to consent to them before independent access to the Internet is allowed for them within school:

- Pupils will need to agree to use the internet in a safe and responsible way, observing all of the restrictions explained to them.
- Parents will need to acknowledge that whilst the school will take reasonable precautions to prevent children from accessing inappropriate materials, the school will not ultimately be

held responsible for the nature of the content they access and that they will be deemed to be accountable for their own actions.

These agreements will be distributed annually at the Year R parents meetings.

7. E-Safety Education & Training

Whilst regulation and technical solutions are very important, their use must be balanced by educating users of potential e-safety risks as well as how to develop safe and responsible behaviours to minimise them, wherever and whenever they go online.

E-Safety education will be provided in the following ways:

7.1 E-Safety within the Curriculum

- *Early Years Foundation Stage and Key Stage 1*

  At this level, use of the Internet will either be quite heavily supervised or based around preselected, safe websites. Children will be regularly reminded about how to take care when clicking and to seek help/advice from an adult if they see anything that makes them unhappy or that they are unsure about.
- *Lower Key Stage 2*

  Children will now be given more opportunities to develop their digital literacy skills (e.g. using online simulations and coding websites). They will be shown how to develop a responsible attitude towards searching the World Wide Web and will be reminded of the need to report any concerns they have. The importance of creating strong passwords and the benefits of only joining child-friendly websites will also be taught.
- *Upper Key Stage 2*

  Children will now be encouraged to become more independent when researching for information on the World Wide Web, being taught the necessary skills to critically evaluate sites for their accuracy and suitability. They will be supported in using online collaboration tools more for communicating and sharing ideas with others, including being taught the need for not revealing personal information to strangers. The aim is to children how to manage and deal with risks they encounter by themselves, whilst at the same time encouraging them to become positive users of both new and emerging technologies including AI.

7.2 E-Safety Training for Staff and Governors

Staff and governors will receive regular training about how to protect and conduct themselves professionally online and to ensure that they have a good awareness of issues surrounding modern technologies, including safeguarding. They are also directed to relevant websites to help support their understanding of these issues.

7.3 E-Safety Training for Parents

The school understands that everyone has a role to play in empowering children to stay safe while they enjoy new technologies, just as it is everyone's responsibility to keep children safe in the nondigital world.

For these reasons, the school will provide opportunities for parents/carers to receive e-safety education and information (e.g. via the school website) to enable them to better understand the issues surrounding new technologies and to help them support their children in developing good e-safety behaviour – this includes delivery via newsletters and the school website.

8. Acceptable use of Social Media

Due to the rising popularity of social networking sites such as Facebook and Twitter, the staff and governors have agreed that they will be setting a good example to the children in our school, when using these sites.

All parents are invited to join staff in setting a good example for our children by:

- Demonstrating courtesy and respect for staff, other parents and pupils when comments are placed on social networking sites.
- Using appropriate language when discussing school.
- Addressing any issues or concerns regarding school, directly with the Headteacher, member of staff or governors rather than posting them on social media.

All parents are invited to join staff in setting a good example for our children by not:

- Using social networking sites to make derogatory comments or posting photographs which could bring staff into disrepute, including making comments about pupils, parents, other staff members, the senior leadership team, governors, Local Authority (LA) or the wider community.
- Posting photographs of other people's children on social networking sites without their permission.

Our promise as a school is:

- We will meet with you and use the Governing Body's policies and procedures to resolve concerns.
- We will work hard to resolve any concerns in the best interest of the whole community.
- We will act in the best interest of the whole community and honour our duty of care to our children.
- We will never conduct school business through social network sites.

The staff and governors of Haselworth Primary School's agreement for using social networking sites:

- Demonstrate courtesy and respect for staff, parents and pupils when comments are placed on social networking sites.
- Ensure appropriate language is used in any comments placed on social networking sites.
- Ensure that any comments and/or images could not be deemed as defamatory or in breach of any relevant legislation set out in LA or school policies and handbooks.
- Review and adjust their privacy settings to give them the appropriate level of privacy and confidentiality.

We agree not to:

- Use social networking sites to make derogatory comments which could bring staff into disrepute, including making comments about pupils, parents, other staff members, the senior leadership team, governors, LA or the wider community.
- Use social networking sites to communicate with any pupil in the school.
- Post information or opinions about Haselworth Primary School or pictures of school events.
- Use social networking sites within lesson times (for personal use).

Our promise to parents is that:

- We will meet with them and use the Governing Body's policies and procedures to resolve concerns.
- We will work hard to resolve any concerns in the best interest of the whole community.
- We will act in the best interest of the whole community and honour our duty of care to our pupils.
- We will never conduct school business through social network sites.

Cyberbullying

Haselworth Primary School is committed to ensuring that all of its staff, governors, parents/ carers and pupils are treated with dignity and respect. Bullying and harassment of any kind will not be tolerated. Cyber-bullying methods could include text messages, emails, phone calls, instant messenger services, circulating photos or video clips or by posting comments on web sites, blogs or in chat rooms.

9. Data Protection

All data held on the school's network is subject to GDPR 2018 and the school's *Child Protection Policy and Safeguarding Policies.*

Unlicensed or personal software must not be installed on the school's hardware or connected in any way to the school's equipment or systems. If software is deemed to be of use to the school then it should be duly acquired by the school under licence.

Where data of a personal nature such as: school reports, PEPs, correspondence and assessment data needs to be accessed at home by staff, this must be only accessed through the remote dashboard facility or via the individual staff's encrypted memory stick.

Any loss of data or a data breach must be reported to the School Data Protection Officer, Mrs S Rix. Please see the Data Protection Policy for further details.

Data stored on the school's networked drives are backed up regularly so that copies of files may be recovered if the original becomes either lost or damaged.

The servers containing these networked drives are locked away each night as an extra security measure to prevent against theft.

10. Responding to Unacceptable Internet and Computer Use by Pupils

Pupils should be made aware that all e-safety concerns will be dealt with: promptly, sensitively and effectively so that they will feel able and safe to report any incidents.

Children are encouraged to respect the facilities offered to them, however staff are trained in how to proceed following a breach of the *Rules for Acceptable Internet and Computer Use*, in accordance with the school's *Safeguarding Policy*. This includes guidance on preservation of evidence and immediate reporting – the school's Designated Safeguarding Lead has overall responsibility for Internet safety so any misuse should be reported to them without delay.

Depending on the severity and nature of the misuse offence, sanctions include: first warnings, temporary bans from using the ICT resources and meetings with parents/carers, all in accordance with the school's Positive Relationships and *Behaviour Policy* and in consideration of the age of the child.

All incidents should be recorded in the school's behaviour log book.

A 'report abuse' button (CEOP) is visible on the home page of the school's website for children to click on if they are concerned about something that has happened online whilst they are on the

Internet at home (e.g. cyber-bullying). This takes them to a portal to access support and advice from the *Child Exploitation and Online Protection Agency*.

11. Responding to Unacceptable Internet and Computer Use by Staff and Visitors

Failure to comply with the *Rules for Responsible Internet and Computer Use* could lead to sanctions being imposed and possible disciplinary action being taken, in accordance with the school's *Safeguarding Policy*, *Child Protection Policy* and the law. Misuse should be reported without delay to Mrs Jones, Headteacher.

12. Artificial Intelligence (AI)

Here at Haselworth Primary School we understand the valuable potential that artificial intelligence (AI), including generative AI, holds for schools. For example, it can be used to enhance pedagogical methods, customise learning experiences and progress educational innovation.

We are also aware of the risks posed by AI, including data protection breaches, copyright issues, ethical complications, safeguarding and compliance with wider legal obligations.

Therefore, the aim of this policy is to establish guidelines for the ethical, secure and responsible use of AI technologies across our whole school community.

This policy covers the use of AI tools by school staff, governors and pupils. This includes generative chatbots such as ChatGPT and Google Gemini (please note, this list is not exhaustive).

This policy aims to:

- Support the use of AI to enhance teaching and learning
- Support staff to explore AI solutions to improve efficiency and reduce workload
- Prepare staff, governors and pupils for a future in which AI technology will be an integral part
- Promote equity in education by using AI to address learning gaps and provide personalised support
- Ensure that AI technologies are used ethically and responsibly by all staff, governors and pupils, including in compliance with intellectual property law

Protect the privacy and personal data of staff, governors and pupils in compliance with the UK GDPR

13. Legislation and guidance

This policy reflects good practice guidelines / recommendations in the following publications:
Generative artificial intelligence (AI) in education, published by the Department for Education (DfE)
Generative AI: product safety standards, published by the DfE

How Ofsted looks at AI during inspection and regulation, published by Ofsted
AI use in assessments, published by the Joint Council for Qualifications
This policy also meets the requirements of the:
UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
Data Protection Act 2018 (DPA 2018)

14. Roles and responsibilities

14.1 Governing Body

The Governing Body will:
Ensure the headteacher is appropriately supported to make informed decisions regarding the effective and ethical use of AI in the school
Governors will adhere to the guidelines below to protect data when using generative AI tools themselves:
Seek advice from the data protection officer (DPO) and the designated safeguarding lead, as appropriate
Ensure there is no identifiable information included in what they put into generative AI tools (unless strictly necessary and they have been approved to do so – check with your DPO/AI lead where appropriate)
Acknowledge or reference any use of generative AI in their work
Fact-check results to make sure the information is accurate

14.2 Headteacher
The headteacher will:
Take responsibility for the day-to-day leadership and management of AI use in the school
Liaise with the data protection officer (DPO) to ensure that the use of AI in the school is in accordance with data protection legislation
Liaise with the other designated safeguarding leads (DSLs) to ensure that the use of AI is in accordance with Keeping Children Safe in Education (KCSIE), and the school's child protection and safeguarding policy
Ensure that the guidance set out in this policy is followed by all staff
Review and update this policy as appropriate, and at least every three years
Ensure staff are appropriately trained in the effective use and potential risks of AI
Make sure pupils are taught about the effective use and potential risks of AI

14.3 Data protection officer (DPO)
The data protection officer (DPO) is responsible for monitoring and advising on our compliance with data protection law, including in relation to the use of AI.

14.4 Designated safeguarding lead (DSL)

The DSL is responsible for monitoring and advising on our compliance with safeguarding requirements including in relation to the use of AI, such as:

Being aware of new and emerging safeguarding threats posed by AI

Updating and delivering staff training on AI safeguarding threats

Responding to safeguarding incidents in line with KCSIE and the school's child protection and safeguarding policy

Understanding the filtering and monitoring systems and processes in place on school devices

14.5 All staff

As part of our aim to reduce staff workload while improving outcomes for our pupils, we encourage staff to explore opportunities to meet these objectives through the use of approved AI tools. Any use of AI must follow the guidelines set out in this policy.

To protect data when using generative AI tools, staff must:

Seek advice from the data protection officer / Agile/DSL, as appropriate

Report safeguarding concerns to the DSL in line with our school's child protection and safeguarding policy

Ensure there is no identifiable information included in what they put into generative AI tools

Acknowledge or reference the use of generative AI in their work

Fact-check results to make sure the information is accurate

All staff play a role in ensuring that pupils understand the potential benefits and risks of using AI in their learning. All of our staff have a responsibility to guide pupils in critically evaluating AI-generated information and understanding its limitations.

14.6 Pupils

Pupils must:

Follow the guidelines set out in section 7 of this policy

15. Process for approving AI use

The headteacher is responsible for signing off on approved uses of AI, or new AI tools, taking into account advice from the DPO.

Any use of generative AI by staff and pupils will be risk assessed, which will include plans for mitigating against unauthorised use cases. The intended use case will be specified and have clear benefits that outweigh the risks.

As part of this process, we will seek assurances from suppliers of AI tools about how their products meet the DfE's AI product safety standards.

If it is strictly necessary to use an AI tool to process personal data, we will carry out a data protection impact assessment (DPIA) in addition to the risk assessment. The DPO will advise on this. If the use case is approved, we will also update our privacy notices accordingly.
In the case of AI tools intended for use by pupils, the risk assessment process must consider:
Age restrictions set by AI tools
Statutory requirements of KCSIE and our child protection and safeguarding policy
Filtering and monitoring standards to make sure we have the appropriate systems in place to protect pupils from harm
The DfE's AI product safety standards

16. Staff and governors' use of AI

16.1 Approved use of AI
We are committed to helping staff and governors reduce their workload. Generative AI tools can make certain written tasks quicker and easier to complete, but cannot replace the judgement and knowledge of a human expert. Technology, including generative AI, should not replace the valuable relationship between teachers and pupils.
Any content produced using AI requires critical judgement to check for appropriateness and accuracy. Whatever tools or resources are used to produce plans, policies or documents, the quality and content of the final document remains the professional responsibility of the person who produced it.
Any plans, policies or documents created using AI should be clearly attributed. Any member of staff or governor using an AI-generated plan, policy or document should only share the AI-generated content with other members of staff or governors for use if they are confident of the accuracy of the information, as the content remains the professional responsibility of the person who produced it.
Always consider whether AI is the right tool to use. Just because the school has approved its use doesn't mean it will always be appropriate.
Staff are welcome to suggest new ways of using AI to improve pupil outcomes and reduce workload. They should contact the headteacher to discuss any ideas they may have with regards to using AI, so they – in consultation with others, as appropriate – can assess whether they deem it to be a satisfactory new method of working.

16.2 Data protection and privacy
To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into generative AI tools or chatbots that have not been approved as safe for this use case.
If personal and/or sensitive data is entered into an unauthorised generative AI tool, Haselworth will treat this as a data breach and will follow the personal data breach procedure outlined in our data protection policy.

16.3 Intellectual property

Most generative AI tools use inputs submitted by users to train and refine their models.
Pupils own the intellectual property (IP) rights to original content they create. This is likely to include anything that shows working out or is beyond multiple choice questions.
In addition, materials created by teachers may be copyright material. Examples of what may be deemed original creative work include:
Homework or any other materials written or drawn by a pupil aside from multiple-choice questions responses
Lesson plans created by a teacher
Prompts entered into generative AI tools

We will not allow or cause intellectual property, including pupils' work, to be used to train generative AI models without appropriate consent or exemption to copyright.
We are aware that secondary infringement could happen if AI products are trained on unlicensed material and outputs and then used in schools or published more widely, such as on the school's website This may include:
Publishing a policy that has been created by an AI tool that used input taken from another school's policy without that school's permission
Using an image on a website that has been created by an AI tool using input taken from the copyright holder without their permission
Exemptions to copyright are limited – we will seek legal advice if we are unsure as to whether we are acting within the law.

16.4 Bias
We are aware that AI tools can perpetuate existing biases, particularly towards protected characteristics including sex, race and disability. For this reason, critical thought must be applied to all outputs of authorised AI applications. This means fact and sense-checking the output.
We will ensure we can identify and rectify bias or error by training staff in this area.
We also regularly review our use of AI to identify and correct any biases that may arise.
If parents/carers or pupils have any concerns or complaints about potential unfair treatment or other negative outcomes as a consequence of AI use, these will be dealt with through our usual complaints procedure.

16.5 Raising concerns
We encourage staff and governors to speak to the headteacher in the first instance if they have any concerns about a proposed use of AI, or the use of AI that may have resulted in errors that led to adverse consequences or unfair treatment.
Safeguarding concerns arising from the use of generative AI must be reported immediately to the DSL in accordance with our school's child protection and safeguarding policy.

16.6 Ethical and responsible use
We will always:

Use generative AI tools ethically and responsibly
Remember the principles set out in our school's equality policy when using generative AI tools [insert link here to your school's equality policy]
Consider whether the tool has real-time internet access, or access to information up to a certain point in time, as this may impact the accuracy of the output
Fact and sense-check the output before relying on it
Staff and governors must not:
Generate content to impersonate, bully or harass another person
Generate explicit or offensive content
Input offensive, discriminatory or inappropriate content as a prompt

16.7. Educating pupils about AI
Here at Haselworth, we acknowledge that pupils benefit from a knowledge-rich curriculum that allows them to become well-informed users of technology and understand its impact on society. Strong foundational knowledge will ensure that pupils develop the right skills to make the best use of generative AI.
Include details of how pupils are taught in your curriculum about the potential benefits of using AI tools to aid their learning, while also covering subjects such as:
Creating and using digital content safely and responsibly
The limitations, reliability and potential bias of generative AI
How information on the internet is organised and ranked
Online safety to protect against harmful or misleading content

17. Use of AI by pupils
We recognise that AI has many uses to help pupils learn.
Pupils may use AI tools:
When specifically studying and discussing AI in schoolwork, for example in IT lessons or art homework about AI-generated images

AI may also lend itself to cheating and plagiarism. To mitigate this, pupils may not use AI tools:
During assessments, including internal and external assessments, and coursework
To write their homework or class assignments, where AI-generated text is presented as their own work
To complete their homework, where AI is used to answer questions set and is presented as their own work (for example, maths calculations)
This list of AI misuse is not exhaustive.

Where AI tools have been used as a source of information, pupils should reference their use of AI. The reference must show the name of the AI source and the date the content was generated.

Pupils must consider what is ethical and appropriate in their use of AI and must not:

Generate content to impersonate, bully or harass another person
Generate or share explicit or offensive content, including, but not limited to, generating inappropriate or sexualised images of pupils
Input offensive, discriminatory or inappropriate content as a prompt

18. Staff training

Staff training takes the form of CPD, INSETs, Safeguarding training and subject specific training.

19. Referral to our child protection and safeguarding policy

The school is aware that the use of generative AI may in some circumstances lead to safeguarding concerns including, but not limited to:

Sexual grooming
Sexual harassment
Sexual extortion
Child sexual abuse/exploitation material
Harmful content
Harmful advertisements and promotions
Bullying

Where there are safeguarding concerns arising from the use of generative AI, a report must be made to the DSL immediately.

Any such incident will be dealt with according to the procedures set out in the school's child protection and safeguarding policy, and child protection referral process

20. Breach of this policy

20.1 By staff

Breach of this policy by staff will be dealt with in line with our staff code of conduct.

Where disciplinary action is appropriate, it may be taken whether the breach occurs:

During or outside of working hours
On an individual's own device or a school device
At home, at school or from a remote working location

Staff members will be required to co-operate with any investigation into a suspected breach of this policy. This may involve providing us with access to:

The generative AI application in question (whether or not it is one authorised by the school)
Any relevant passwords or login details

You must report any breach of this policy, either by you or by another member of staff, to the headteacher immediately.

20.2 By governors

Governors found in breach of this policy will be dealt in line with the safeguarding policies and the Governor Code of Conduct.

11.3 By pupils

Any breach of this policy by a pupil will be dealt with in line with our behaviour policy and safeguarding policies.

12. Monitoring and transparency

AI technology, and the benefits, risks and harms related to it, evolve and change rapidly. Consequently, this policy is a live document that must be kept updated by the SLT and the SBM whenever there is a significant change to either AI use by the school or the associated risks of AI usage.

This policy will also be regularly reviewed and updated to align with emerging best practices, technological advancements and changes in regulations.

The policy will be shared with the full Governing Body at least annually.

All teaching staff are expected to read and follow this policy.

SLT will monitor the effectiveness of AI usage across the school.

We will ensure we keep members of the school community up to date on the use of AI technologies for educational purposes. As part of our regular surveys, feedback from pupils, parents/carers and staff will be considered in the ongoing evaluation and development of AI use in school.

Do's and Don'ts: Advice for Staff **Appendix 1**

Whilst the wide range of ICT systems and resources available to staff, both in school and outside of school, have irrefutable advantages, there are also potential risks that staff must be aware of. Ultimately if staff use ICT resources inappropriately, this may become a matter for a police or social care investigation and/or a disciplinary issue which could lead to their dismissal. Staff should also be aware that this extends to inappropriate use of ICT outside of school.

This Dos and Don'ts list has been written as a guidance document. Whilst it is not fully comprehensive of every circumstance that may arise, it indicates the types of behaviours and actions that staff should not display or undertake as well as those that they should in order to protect themselves from risk.

General issues

Do	**Don't**
Ensure that you do not breach any restrictions that there may be on your use of school resources, systems or resources	Access or use any systems, resources or equipment without being sure that you have permission to do so
Ensure that where a password is required for access to a system, that it is not inappropriately disclosed	Access or use any systems or resources or equipment for any purpose that you don't have permission to use the system, resources or equipment for
Respect copyright and intellectual property rights	Compromise any confidentiality requirements in relation to material and resources accessed through ICT systems
Ensure that you have approval for any personal use of the school's ICT resources and facilities	Use systems, resources or equipment for personal use without having approval to do so
Be aware that the school's systems will be monitored and recorded to ensure policy compliance	Use other people's log on and password details to access school systems and resources

Ensure you comply with the requirements of the GDPR when using personal data	Download, upload or install any hardware or software without approval
Seek approval before taking personal data off of the school site	Use unsecure removable storage devices to store personal data
Ensure personal data is stored safely and securely whether kept on site, taken off site or accessed remotely	Use unsecure removable storage devices to store personal data
Report any suspected misuse or concerns that you have regarding the school's systems, resources and equipment to the Headteacher or designated manager	Use school systems for personal financial gain, gambling, political activity or advertising

Be aware that a breach of your school's Acceptable Use Policy will be a disciplinary matter and in some cases, may lead to dismissal	Communicate with parents and pupils outside normal working hours unless absolutely necessary
Ensure that you have received adequate training in ICT Ensure that any equipment provided for use at home is not accessed by anyone not approved to use it	
Ensure that your use of ICT bears due regard to your personal health and safety and that of others	
Always use a school issued encrypted memory stick when using school data and documents	

Use of email, the internet, VLEs and school and HCC intranets:

Do	Don't
alert your Headteacher or designated manager if you receive inappropriate content via email	send via email or download from email, any inappropriate content
be aware that the school's email system will be monitored and recorded to ensure policy compliance	send messages that could be misinterpreted or misunderstood
ensure that your email communications are compatible with your professional role	use personal email addresses to communicate with pupils or parents
give full consideration as to whether it is appropriate to communicate with pupils or parents via email, or whether another communication mechanism (which may be more secure and where messages are less open to misinterpretation) is more appropriate	send messages in the heat of the moment
be aware that the school may intercept emails where it believes that there is inappropriate use seek support to block spam	send messages that may be construed as defamatory, discriminatory, derogatory, offensive or rude
alert your Headteacher or designated manager if you accidentally access a website with inappropriate content	use email systems to communicate with parents or pupils unless approved to do so
be aware that a website log is recorded by the school and will be monitored to ensure policy compliance	download attachments from emails without being sure of the security and content of the attachment
answer email messages from pupils and parents within your directed time mark personal emails by typing 'Personal/Private' within the subject header line	forward email messages without the sender's consent unless the matter relates to a safeguarding concern or other serious matter which must be brought to a senior manager's attention
	access or download inappropriate content (material which is illegal, obscene, libellous, offensive or threatening) from the internet or upload such content to the school or HCC intranet upload any material onto the school website that doesn't meet style requirements and without approval

Use of telephones, mobile telephones and instant messaging:

Do	Don't
Ensure that your communications are compatible with your professional role	Send messages that could be misinterpreted or misunderstood
Ensure that you comply with your school's policy on use of personal mobile telephones	Excessively use the school's telephone system for personal calls
Ensure that you reimburse your school for personal telephone calls as required	Use personal or school mobile telephones when driving

Use of cameras and recording equipment:

Do	Don't
Ensure that material recorded is for educational/school purposes only	Bring personal recording equipment into school without the prior approval of the Headteacher
Ensure that where recording equipment is to be used, approval has been given to do so by the Headteacher	Inappropriately access, view, share or use material recorded other than for the purposes for which it has been recorded
Ensure that material recorded is stored appropriately and destroyed in accordance with the school's policy	Put material onto the VLE, school intranet or intranet without prior agreement from a member of senior staff
Ensure that parental consent has been given before you take pictures of school pupils	Use your personal phone to take photos or videos of children

Use of social networking sites:

Do	**Don't**
Ensure that you understand how any site you use operates and therefore the risks associated with using the site	Utilise social networking sites while at work
Familiarise yourself with the processes for reporting misuse of the site	Accept friendship requests from pupils or parents of pupils attending the school – you may be giving them access to personal information, and allowing them to contact you inappropriately
Consider carefully who you accept as friends on a social networking site	Put information or images on line or share them with colleagues, pupils, or parents (either on or off site) when the nature of the material may be controversial
Report to your Headteacher any incidents where a pupil has sought to become your friend through a social networking site	Post anything that may be interpreted as slanderous towards colleagues, pupils or parents
Take care when publishing information about yourself and images of yourself online – assume that anything you release will end up in the public domain	Use social networking sites to contact parents and/or pupils
Ask yourself about whether you would feel comfortable about a current or prospective employer, colleague, pupil or parent viewing the content of your page	
Follow school procedures for contacting parents and/or pupils	
Only contact pupils and/or parents via school based computer systems	
Through your teaching, alert pupils to the risk of potential misuse of social networking sites (where employed in a teaching role)	

Staff Code of Conduct for ICT **Appendix 2**

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with parents, pupils and others, they are asked to sign this code of conduct. Staff should consult the detail of the school's Policy for Staff Acceptable Use of ICT for further information and clarification.

- I appreciate that ICT includes a wide range of system, including mobile phones, personal digital assistants, cameras, email, internet and HCC intranet access and use of social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that it may be a criminal offence to use the school ICT system for a purpose not permitted.
- I understand that I must not communicate information which is confidential to the school or which I do not have the authority to share.
- I understand that school information systems and hardware may not be used for personal or private without the permission of the Headteacher.
- I understand that my use of school information systems, internet and email may be monitored and recorded, subject to the safeguards outlined in the policy to ensure policy compliance.
- I understand the level of authority required to communicate with parents and pupils using the various methods of communication.
- I understand that I must not use the school ICT system to access inappropriate content.
- I understand that accessing, viewing, communicating and downloading material which is pornographic, offensive, defamatory, derogatory, harassing or bullying is inappropriate use of ICT.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager. I will not use anyone's account except my own.
- I will not install any software or hardware without permission.
- I will follow the school's policy in respect of downloading and uploading of information and material including the use of AI.
- I will ensure that personal data is stored securely and is used appropriately whether in school, taken off the school premises or accessed remotely. I will not routinely keep personal data on removable storage devices. Where personal data is required, it will be stored on a school issued encrypted memory stick and removed directly after use.
- I will respect copyright, intellectual property and data protection rights as stated in the new GDPR.
- I understand use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

Resources

- I will report any incidences of concern regarding children's safety to the Designated Safeguarding Lead or Headteacher.
- I will report any incidences of inappropriate use or abuse of ICT and inappropriate electronic communications, whether by pupils or colleagues, to the Headteacher, or if appropriate, the Chair of Governors.
- I will ensure that any electronic communication undertaken on behalf of the school, including email and instant messaging are compatible with my professional role and that messages do not present personal views or opinions and cannot be misunderstood or misinterpreted.
- I understand the school's stance on use of social networking and given my professional role working with children, will exercise care in any personal use of social networking sites.
- I will ensure that any electronic communications with pupils, where permitted, are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote e-safety with pupils in my care and help them to develop a responsible attitude to system use, communication and publishing.
- I understand that inappropriate use of personal and other non-school based ICT facilities can have implications for my employment at the school where this becomes known and where activities undertaken are inconsistent with expectations of staff working with children.

The school may exercise its right to monitor the use of the school's ICT systems and accesses, to intercept email and to delete inappropriate materials where it believes unauthorised use of the school's ICT systems may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, images or sound.

I have read and understand the Policy for Staff Acceptable Use of ICT and understand that inappropriate use may be considered to be misconduct or gross misconduct and may, after proper investigation, lead to a disciplinary sanction or dismissal. I understand that if I need any clarification regarding my use of ICT facilities, I can seek such clarification from any member of the Senior Leadership Team.

SIGNED: ……

DATE:……..

NAME (PRINT): ……