Hempstead Schools Federation

Online Safety Policy

February 2025

Key Contacts

Role	Name
Designated Safeguarding Lead (DSL) and Online Safety Lead	Paul Cross
Deputy Designated Safeguarding Leads	Emma Taylor (SENDCo) Lynne McCann (DHT Infants) Al Browne (DHT Juniors)
Headteacher	Paul Cross
Safeguarding Governor	Wendy Harris/ Amy O'Leary
Other key staff	Abbie Stephens (Family Liaison Officer)

1 United Nations Convention on the Rights of the Child (UNCRC)

Both schools within Hempstead Schools Federation are 'Rights Promoting Schools', promoting the rights for children as set out in the UNCRC. The UNCRC sets out the civil, political, economic, social and cultural rights to which everyone under the age of 18 is entitled. Article 13 states that every child must be free to express their thoughts and opinions and be able to access all kinds of information, as long as it is in the law. Article 17 states that all children have the right to access reliable information, but that Governments must help protect children from materials that could harm them. Article 34 states that children must be protected from all forms of sexual abuse and exploitation, and Article 36 from any other forms of exploitation. This policy considers the implications of all these articles within the framework of Online Safety.

2 This policy document is reviewed by the head teacher (DSL and Online Safety Lead) and ICT Lead. It is revised and agreed by governors, senior management and the teaching staff.

3 At Hempstead Schools Federation (HSF) the welfare and well-being of our staff and pupils is paramount. However, we recognise the immense opportunities and value the internet offers in regards to communication and learning. We are committed to teaching our pupils the safe way to use the internet, ensuring they understand the opportunities it offers, but at the same time alerting them to the dangers and risks to which they may be exposing themselves.

4 Early Years Foundation Stage

This policy meets the requirements of the Statutory Framework for the Early Years Foundation Stage in regards to safeguarding and child protection. For pupils in the Foundation Stage, access to the internet is very limited and carefully managed by school staff in line with this policy.

5 Online Safety Officer

Any concerns or queries regarding online safety for pupils by either parents or staff should be directed to the Online Safety Officer. The school's Online Safety Officer is Paul Cross, Head Teacher, who is also the Designated Safeguard Lead.

6 Effective practice in online safety

6.1 Online safety depends on effective practice in each of the following areas:

- Education for responsible ICT use by staff and pupils;
- A comprehensive, agreed and implemented ICT Policies (online safety Policy, Acceptable Use Policies, Mobile Technology Policy);
- Secure, filtered broadband supplies by Atomwide in conjunction with Medway Council, but also monitored by SENSO software;
- A school network that complies with the National Education Network standards and specifications.

7 Links to other policies;

7.1 This policy supports other key safeguarding policies as follows;

- Safeguarding Policy
- ICT Acceptable Use Policy
- Anti-Bullying Policy
- Behaviour Support Policy
- Mobile Technology Policy

8 What is online safety?

8.1 HFS recognises online safety as ensuring pupils keep themselves safe when accessing the following aspects of the online world;

- Safer internet browsing
- Online gaming
- Cyber-bullying
- Online grooming
- Sexting
- Social Networking
- Sharing information
- Emailing/ blogging

8.2 The teaching of online safety covers the '4 Cs':

- Content: pupils being made aware of the risks of accessing illegal and inappropriate content
- Contact: pupils being made aware that perpetrators of online abuse may try to contact children and place them at risk of abuse
- Conduct: that pupils themselves have a responsibility to keep themselves and others safe in the way they use the internet
- Commerce: online gambling, inappropriate advertising, phishing and financial scams

9 Why the internet and digital communications are important

- The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience.

- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

10 Safer use of the internet

- School internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation
- Pupils will be shown how to publish and present information to a wider audience.
- Pupils need to be taught that the internet itself is not the threat; the threat comes from the people who use it, including themselves.

11 Safety advice for parents and pupils

For specific areas of online safety, the following messages are taught to pupils and communicated to parents through the website and via communications over the year.

- **Safer internet browsing;** being aware that not all what you read on the internet is necessarily factual or true and that we need to be critical of what we read and use
- **Online gaming;** that we need to keep our personal information off the internet; use usernames and avatars. Parents should know when you are playing online and should closely monitor who you are playing with. Only play with your friends, and be aware that people who you are playing against may not be who they say they are.
- **Cyber-bullying;** if you get ANY unwelcome messages or contact off anyone (whether you know them or not), don't just hope it will go away. Tell and show a trusted adult immediately. Ignore threats that the bully says about not telling anyone – you must; it's the only way to stop it.
- **Social Networking;** most social networking sites have an age limit of 13 years. Parents who allow their children to access such sites are knowingly breaching the rules. Be aware that if you lie about your age, you will start to get inappropriate adult content when the internet thinks you are 18.
- **Sharing information;** never share any personal information online. Despite what you hear, most major internet sites have full ownership of any images posted and it will ALWAYS be there, somewhere. You may live to regret images and comments posted when you are older. Use the 'granny test'; if you are sharing images or comments you would not share with your granny, then it probably isn't appropriate.
- **Emailing/ blogging;** this should only ever be done through school-approved sites. Be careful what you post; the system is designed to flag up inappropriate content and it will be traced back to whoever posted it.

12 Allegations of abuse made against other pupils ('child on child abuse')

12.1 We recognise that children are capable of abusing their peers and that this can occur online. Abuse will never be tolerated or passed off as "banter", "just

having a laugh" or "part of growing up". The rise of social media use in children of primary age has led to an increase in incidents of abuse online.

12.2 More detail concerning the federation's approach to peer-on-peer abuse can be found in our Safeguarding Policy.

12.3 We are committed to ensuring all victims are reassured that they are being taken seriously and that they will be supported and kept safe. A victim should never be given the impression that they are creating a problem by reporting sexual violence or sexual harassment. Nor should a victim ever be made to feel ashamed for making a report.

12.4 Most cases of pupils alleged bullying whether online or otherwise will be dealt with under our school's behaviour policy, but this online safety policy and the safeguarding policy will apply to any allegations that raise safeguarding concerns.

13 Online grooming and sexting

The school recognises that online grooming and child-on-child abuse is a growing threat to the safety and well-being of our pupils. Staff are trained to be aware of these threats and also to be alert to indicators that pupils/ families may be involved. The school has rigorous safeguarding training and procedures in place to manage such issues if they arise. Pupils are taught about the vulnerabilities and threats to which they may be open if they are not careful online.

14 Evaluating internet content and using it safely

- The school will ensure that the use of internet-derived materials by staff and pupils complies with copyright law.
- Pupils will be taught to identify websites more likely to be appropriate to them when using the internet.
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant internet content e.g. informing an appropriate adult, using the CEOP 'report' icon or Jessie's friends (www.thinkukonow.co.uk).

15 Email

- Pupils may only use approved Medway email accounts (Office 365) on the school system, supplied by Atomwide.
- Pupils learn that they must immediately tell a teacher if they receive offensive email.
- In email communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone.
- Incoming email should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how email from pupils to external bodies is presented and controlled.
- The forwarding of 'chain' emails is not permitted.

16 Published content and the school web site

- Staff or pupil personal contact information will not generally be published.
- All contact details given online will be via the school office.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

17 Publishing pupils' images and work

- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Only images of pupils who have appropriate permissions will be used. Full names will never be associated with individual photographs.
- Pupils' full names will not be used anywhere on a school website or other online space, particularly in association with photographs.
- Consent from parents or carers will be obtained before photographs of pupils are published on the school website.
- Work can only be published with the permission of the pupil and parents/carers.
- Pupil image file names will not refer to the pupil by name.
- Parents are informed of the school policy on image taking and publishing, both on school and external social media or websites.

18 Data Protection

The school meets the guidance as set out by the General Data Protection Regulation (GDPR). The school has robust data protection procedures in place and places a high priority on confidentiality. All staff have signed a data protection code of conduct that ensures they are aware of and have agreed to the regulations on managing, storage and sharing of data.

19 Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. The school has also updated its procedures and policies in line with the General Data Protection Regulation (GDPR) which came into force in 2018.

20 Social networking and personal publishing

- The school will control access to social networking sites in line with the Acceptable Use Policies, and consider how to educate pupils in their safe use.
- News groups will be blocked unless a specific use is approved.
- Pupils will be taught never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use usernames and avatars when using social networking sites.

21 Information system security

- School ICT systems security will be reviewed regularly.

- Virus protection will be updated regularly, supplied by Atomwide and Medway Grid for Learning.

22 Managing monitoring and filtering

- This policy has been updated to reflect the requirements for monitoring and filtering as set out in the latest version of KCSIE.
- The school will work with Medway Council to ensure systems are filtered to protect pupils; only Atomwide nominated contacts can control filtering.
- Filtering software is provided by MGfL/ LGfL: Webscreen/ Safe-Search will filter 99% of inappropriate/ unsafe content to the extent that even safe content can be prevented from being permitted through and needs to be enabled.
- Access to inappropriate or extremist content is monitored through weekly reports checked by the Online Safety Officer via SENSO software monitoring all school-owned devices
- All school staff will monitor access to the computers and the content being accessed under their supervision
- If staff or pupils come across unsuitable online materials, whether intentionally or unintentionally, the material must be reported to the head teacher.
- The Online Safety Officer will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

23 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The school acknowledges that technologies such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- The school's secure wireless access code will not be given out to unauthorised persons.
- Mobile devices will only be used during learning time by staff as set out in the Mobile Technology Policy guidelines. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- All pupils are to hand mobile phones to their teachers for safe keeping.
- The use of cameras on mobile phones or smart watches by pupils is not permitted.
- Games machines including the Sony PlayStation, Microsoft Xbox and others which have internet access that may not include filtering are not to be brought into school.
- All teachers have access to school-provided devices to record or aid learning.
- The use of our learning platform alongside pupil and staff passwords will be available only from the technical support team or system administrator.

24 Authorising Internet access

- All staff must read and sign the Staff Acceptable Use Policy before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- Safe search will always be turned on, pupils will be taught how to search independently and specifically.
- Parents will be asked to sign and return a consent form on their child's admission to the school.
- Any person not directly employed by the school, e.g. volunteers, will be asked to sign the Acceptable Use Policy for volunteers before being allowed to access the internet from the school site.

25 Preventing radicalisation

Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism. Extremism is vocal or active opposition to fundamental British values, such as democracy, the rule of law, individual liberty, and mutual respect and tolerance of different faiths and beliefs.

25.1 Schools have a duty to prevent children from being drawn into terrorism. The DSL will ensure all staff undertake Prevent awareness training and make sure that staff have access to appropriate training to equip them to identify children at risk.

25.2 We will assess the risk of children in our school being drawn into terrorism. This assessment will be based on an understanding of the potential risk in our local area, in collaboration with our local safeguarding children board and local police force.

25.3 We will ensure that suitable internet filtering is in place, and equip our pupils to stay safe online at school and at home.

26 Online/ remote learning

As a school, we take the safety and privacy of pupils extremely seriously and have put measures in place to ensure pupil safety during remote learning, if required. The school uses Microsoft Office 365 to manage pupils' learning online. Each pupil has a secure student account and uses this to access Teams which is the platform used for online learning. Meetings (lessons) can only be access by those who have been invited and who have a school account.

27 Assessing risks

27.1 The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor Medway Council can accept liability for any material accessed, or any consequences of internet access beyond the reasonable efforts of the school to prevent this.

27.2 The school will audit ICT-use to establish if the online safety policy is adequate and that the implementation of the online safety policy is appropriate and effective.

28 Handling online safety complaints

- Complaints of internet misuse by staff or pupils will be dealt with by the Online Safety Officer (see section 5).
- Complaints of a child protection nature will be dealt with in accordance with school safeguarding procedures.
- Pupils and parents will be informed of the complaints procedure (see school's complaints policy).
- Pupils and parents will be informed of consequences for pupils misusing the internet.
- If appropriate, discussions will be held with the Police/ Children's Services to establish procedures for handling potentially illegal issues.

29 Teaching pupils about online safety

- Online safety rules will be posted next to all computers and discussed with pupils regularly.
- Pupils will be informed that network and internet use will be monitored and appropriately followed up.
- Pupils will be taken through, and asked to sign the pupil Acceptable Use Policy at the start of every academic year.
- A programme of training in online safety will be delivered through;
    - An online safety training embedded within the ICT scheme of work and the Personal Social and Health Education (PSHE) curriculum.
    - A specific focus on Internet Safety Day

30 Supporting parents with online safety advice

- Online safety advice will be posted on the school's website (see Appendix 1)
- Online safety updates will be circulated over the course of the year.

31 Breaches of online safety protocols

31.1 The following will apply to staff and pupils if breaches of any of the school's internet safety policies are found to have been committed.

- Staff and pupils are advised to not delete any inappropriate material and to take screen shots if it involves online abuse or bullying content.
- Where possible, screenshots and remote access will be used as evidence
- The individual concerned will be met with and if appropriate, evidence presented and concerns raised. If a pupil, parents will be contacted.
- Depending on the nature of the breach, access to the internet at school (and at home if appropriate) will be restricted or stopped altogether. A verbal or written warning concerning further action if there are any further breaches will be given. The head teacher will keep records of such incidents.
- Staff must not knowingly copy, print out or share any images of a sexual nature involving children, even as part of an incident brought to their attention as this could be construed as viewing or distributing illegal images of children.

32 Staff and the online safety policy

- All staff will review the school's online safety policies at the start of each academic year and asked to sign that they have read and understood.
- Staff must be informed that network and internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.

Paul Cross
Head Teacher/ DSL/ Online Safety Officer
Approved at the Pupil Progress and Standards Committee on March 11th 2025

APPENDIX 1;

Advice on the school website in regards to online safety

Safer internet browsing; being aware that not all what you read on the internet is necessarily factual and that we need to be critical of what we access

Online gaming; that we need to keep our personal information off the internet; use usernames and avatars. Parents should know when you are playing on line and should closely monitor who you are playing with. Only play with your friends, and be aware that people who you are playing against may not be who they say they are.

Cyber-bullying; if you get ANY unwelcome messages or contact off anyone (whether you know them or not), don't just hope it will go away. Tell and show a trusted adult immediately. Ignore threats that the bully says about not telling anyone – you must; it's the only way to stop it.

Social Networking; most social networking sites have an age limit of 13 years or above. Parents who allow their children to access such sites are knowingly breaching the rules. Be aware that if you lie about your age, you will start to get inappropriate adult content when the internet thinks you are 18.

Sharing information; never share any personal information online. Despite what you hear, most major internet sites have full ownership of any images posted and it will ALWAYS be there, somewhere. You may live to regret images and comments posted when you are older. The 'granny test'; if you are sharing images or comments you would not share with your granny, then it probably isn't appropriate.

Emailing/ blogging; this should only ever be done through school-approved sites. Be careful what you post, the system is designed to flag up inappropriate content and it will be traced back to whoever posted it.