Online Safety Policy 2025-2026

Deaf Hill Primary School

Approved by Local Governors: March 2026

Date for Review: September 2026

Headteacher: Mr Paul Newton

Chair of Governors: Mrs Claire Smith

Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2024) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2024) 'Keeping children safe in education 2024'
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- DfE (2023) 'Generative artificial intelligence in education'
- Department for Science, Innovation and Technology and UK Council for Internet Safety (2024) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2020) 'Small Business Guide: Cyber Security'
- Keeping Children Safe in Education 2024

This policy operates in conjunction with the following school policies:

- Whistleblowing Policy
- Acceptable Use Agreement
- Data and Cyber-security Breach Prevention and Management Plan
- Safeguarding and Child Protection Policy
- RSE and PSHE Policy
- Peer on Peer Abuse Policy
- Weapons Policy
- Ad Astra Staff Behaviour Policy
- Behaviour Policy
- Data Protection Policy
- Staff, Pupil and Parent Privacy Notices
- Prevent Duty
- Pupil Remote Learning Guidance

- Technology Acceptable Use Agreement for Pupils – Appendix B
- Technology Acceptable Use Agreement for Staff

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit the user for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety
- Meeting digital and technology standards

- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education (RSE) and health education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

This policy complies with Ad Astra Academy Trust's funding agreement and articles of association.

Roles and responsibilities

The Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The Governing body will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The Governing Body will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The Governing Body will co-ordinate regular meetings with appropriate staff to discuss online safety and requirements for training and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The Governing Body will make sure that the school teaches pupils how to keep themselves and others safe, including online.

The Governing Body will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- Reviewing filtering and monitoring provisions at least annually
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning

- Having effective monitoring strategies in place that meet the school's safeguarding needs

All governors will:

- Make sure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school or college approach to safeguarding and related policies and/or procedures
- Make sure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

The Headteacher:

The headteacher is responsible for making sure that staff understand this policy, and that it is being implemented consistently throughout the school.

The designated safeguarding lead (DSL)

Details of the school's designated safeguarding lead (DSL) and deputies (DDSLs) are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in making sure that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and make sure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring

- Making sure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks pupils face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

ICT technicians* will be responsible for:

• Providing technical support in the development and implementation of online safety policies and procedures.

• Implementing appropriate security measures as directed by the Headteacher and wider members of Ad Astra Academy Trust staff.

• Ensuring that the school's filtering and monitoring systems are updated as appropriate.

• Working with the DSL/Headteacher to conduct regular light-touch reviews of this policy.3.5 All staff and volunteers

****At Deaf Hill Primary School, the ICT technician role is undertaken by OneIT***

All staff members will be responsible for:

• Taking responsibility for the security of ICT systems and electronic data they use or have access to, adhering to the Acceptable Use Agreement (Appendix 3)and other relevant policies.

• Modelling good online behaviours.

• Maintaining a professional level of conduct in their personal use of technology.

• Reporting concerns in line with the school's reporting procedure.

• Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

• Engaging with training to ensure that they have an awareness of online safety issues and are familiar with, and understand, the indictors that pupils may be unsafe online.

Pupils will be responsible for:

• Adhering to the Acceptable Use Agreement and other relevant policies. (Appendix 2)

• Seeking help from school staff if they are concerned about something they or a peer have experienced online.

• Reporting online safety incidents and concerns.

Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Make sure that their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Help and advice for parents/carers – Childnet
- Parents and carers resource sheet – Childnet

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

Handling online safety concerns

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection Policy. All concerns will be reported and recorded through our CPOMS platform. Concerns regarding a staff member's online behaviour are reported to the Headteacher, who decides on the best course of action in line with the relevant policies, e.g. the Ad Astra Staff Behaviour Policy, Low Level Concerns Policy, Allegations of Abuse Against Staff Policy, and Disciplinary Policy and Procedures. If the concern is about the Headteacher, it is reported to the chair of LAC or CEO of Ad Astra Academy Trust.

Concerns regarding a pupil's online behaviour are reported to a DSL, who investigates concerns with relevant staff members, e.g. the Headteacher and OneIT manages concerns in accordance with relevant policies depending on their nature, e.g. the Positive Relationships and Behaviour Policy and Child Protection and Safeguarding Policy. Where there is a concern

that illegal activity has taken place, the Headteacher will decide if the decision is taken to contact the Police. The school avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL and/or Headteacher will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

All online safety incidents and the school's response are recorded by the DSL or DDSLs

Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

In **Key Stage (KS) 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage (KS) 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- Be discerning in evaluating digital content

By the **end of primary school**, pupils will know:

- That the internet can be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health
- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data are shared and used online

- How to be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
- The benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing
- Why social media, computer games and online gaming have age restrictions and how to manage common difficulties encountered online
- How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private
- Where and how to report concerns and get support with issues online

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Pupils will be taught practical cyber security skills

This section is based on the DfE's non-statutory cyber security standards for schools and colleges.

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate education on safeguarding issues such as cyberbullying and the risks of online radicalisation.

Child on child sexual abuse and harassment

All staff will be aware of the indicators of abuse, neglect and exploitation and understand where the risk of such harms can occur online. Staff will understand that this can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

• Threatening, facilitating or encouraging sexual violence

• Upskirting, i.e. taking a picture underneath a person's clothing without consent and

with the intention of viewing their genitals, breasts or buttocks

• Sexualised online bullying, e.g. sexual jokes or taunts

• Unwanted and unsolicited sexual comments and messages

• Consensual or non-consensual sharing of sexualised imagery

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

If staff become aware of images on devices and confiscate them, they **MUST NOT** be returned to the child as this would be classed as sharing and distribution of images.

If staff become aware of images on a device, they **MUST NOT** take copies of these or forward then to anyone without authority from the Police as this would be classed as sharing and distribution of images

Educating parents/carers about online safety

Deaf Hill Primary school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

Cyber-bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Cyberbullying - please refer to our Anti-Bullying and Safeguarding Policies.

Cyberbullying can include, but is not limited to, the following:

• Threatening, intimidating or upsetting text messages.

• Threatening or embarrassing pictures and video clips sent via mobile phone cameras.

• Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible.

• Threatening or bullying emails, possibly sent using a pseudonym or someone else's name.

• Unpleasant messages sent via instant messaging.

• Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook.

• Abuse between young people in intimate relationships online i.e. teenage relationship abuse.

• Discriminatory bullying online e.g. homophobia/racism.

We are aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the AntiBullying Policy.

Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Headteacher

- Explain to the pupil why they are being searched, and how the search will happen; and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to DSL/Headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Ad Astra Academy Trust recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

Deaf Hill Primary School will treat any use of AI to bully pupils very seriously, in line with our anti-bullying and behaviour policy.

Staff should be aware of the risks of using AI tools while they are still being developed and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, including the following:

• The pupil believes they are talking to another child, when they are actually talking to an adult masquerading as someone younger with the intention of gaining their trust to abuse them.

• The pupil does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life.

• The pupil may have been manipulated into feeling a sense of dependency on their groomer due to the groomer's attempts to isolate them from friends and family.

• Talking to someone secretly over the internet may make the pupil feel 'special', particularly if the person they are talking to is older.

• The pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is

particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

• Being secretive about how they are spending their time.

• Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.

• Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

This Information has been classified as Customer / General.CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence.

While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Prevent Duty Policy.

Mental health

The internet, particularly social media, can be the root cause of a number of mental health issues in pupils, e.g. low self-esteem and suicidal ideation.

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health.

Concerns about the mental health of a pupil will be dealt with in line with the Social, Emotional and Mental Health (SEMH) Policy.

Online hoaxes and harmful online challenges

For the purposes of this policy, an "online hoax" is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, "harmful online challenges" refers to challenges that are

targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the Headteacher will decide whether each proposed response is:

• In line with any advice received from a known, reliable source, e.g. the UK Safer

Internet Centre, when fact-checking the risk of online challenges or hoaxes.

• Careful to avoid needlessly scaring or distressing pupils.

• Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils.

• Proportional to the actual or perceived risk.

• Helpful to the pupils who are, or are perceived to be, at risk.

• Appropriate for the relevant pupils' age and developmental stage.

• Supportive.

• In line with the Child Protection Policy.

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, e.g. it encourages children to participate in age-inappropriate activities that could increase safeguarding risks or become a child protection concern, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or even to individual children at risk where appropriate.

The DSL and Headteacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

Cyber-enabled – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.

Cyber-dependent – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a pupil's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The DSL and Headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully, and will ensure that pupils cannot access sites or areas of the internet that may encourage them to stray from lawful use of technology,e.g. the 'dark web', on school-owned devices or on school networks through the use of appropriate firewalls.

In addition, the school will implement a cyber awareness plan for pupils and staff to ensure that they understand the basics of cyber security and protecting themselves from cyber crime.

The school will implement it's cyber security strategy in line with the DfE's 'Cyber security standards for schools and colleges' and the Cyber Security Policy.

All staff will access CPD linked to Cyber security and on-line safety as part of our statutory CPD schedule.

Online safety training for staff

The DSL ensures that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

Information about the school's full responses to online safeguarding incidents can be found in the Positive Behaviour and Relationships Policy and Safeguarding and Child Protection Policy.

All teaching staff will access On-line safety training delivered by Clennell Education Solutions.

All staff in school access CPD through Boxphish and DfE approved Cyber Security Training

https://www.ncsc.gov.uk/information/cyber-security-training-schools

Online safety and the curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

• RSE

• PSHE

• Computing

As a school we use Project Evolve to teach our online safety. ProjectEVOLVE - Education for a Connected World Resources

Online safety teaching is always appropriate to pupils' ages and developmental stages. Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using.

The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

• How to evaluate what they see online

• How to recognise techniques used for persuasion

• What healthy and respectful relationships, including friendships, look like

• Body confidence and self-esteem

• Consent, e.g. with relation to the sharing of indecent imagery or online coercion to perform sexual acts

• Acceptable and unacceptable online behaviour

• How to identify online risks

• How and when to seek support

• How to identify when something is deliberately deceitful or harmful

• How to recognise when something they are being asked to do puts them at risk or is age-inappropriate

The online risks pupils may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum can be found in Appendix A of this policy.

The DSL supports with the development of the school's online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

The school recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. pupils with SEND and LAC. Relevant members of staff, e.g. the

SENDCO and designated teacher for LAC, work together to ensure the curriculum is tailored so these pupils receive the information and support they need.

The school will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

Class teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils. When reviewing these resources, the following questions are asked:

- Where does this organisation get their information from?
- What is their evidence base?
- Have they been externally quality assured?
- What is their background?
- Are they age-appropriate for pupils?
- Are they appropriate for pupils' developmental stage?

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The Headteacher and DSL decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher and DSL consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL advises the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities are planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher ensures a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.

Use of technology in the classroom

A wide range of technology is used during lessons, including the following:

- Computers
- Laptops
- Tablets
- Cameras

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher always reviews and evaluates the resource. Class teachers ensure that any internet-derived materials are used in line with copyright law.

Pupils are supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

Acceptable use of the internet in school

Pupils, staff and other members of the school community will only be granted access to the school's internet network once they have read and signed the Acceptable Use Agreement. All members of the school community will be encouraged to use the school's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

Use of mobile devices

Requirements around the use of school-owned devices can be found in the school's Acceptable Use Agreement. For staff, the use of personal devices on the school premises and for the purposes of school work will be managed in line with the Staff Code of Conduct and Acceptable Use Agreement.

Remote Learning

All remote learning will be delivered in line with the school's Remote Education Plan. This specifically sets out how online safety will be considered when delivering remote education.

Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords can be made up of 3 random words, in combination with numbers and special characters if required, or generated by a password manager
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by promptly installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the Headteacher

Smart Technology

Whilst we recognise that the use of smart technology can have educational benefits, there are also a variety of associated risks.

Pupils will be educated on the acceptable and appropriate use of personal devices and will use

technology in line with the school's Acceptable Use Agreement.

Inappropriate use of smart technology may include:

- Using mobile and smart technology to sexually harass, bully, troll or intimidate peers.
- Sharing indecent images, both consensually and non-consensually.
- Viewing and sharing pornography and other harmful content.

Staff will use all smart technology and personal technology in line with the school's Staff Behaviour

Policy/Code of Conduct and Staff Acceptable Use Agreement.

Pupils will not be permitted to use smart devices or any other personal technology whilst on the school site.

Staff will seek to ensure that they are kept up to date with the latest devices, platforms, apps, trends and related threats.

As a school, we will consider the 4Cs (content, contact, conduct and commerce) when educating

pupils about the risks involved with the inappropriate use of smart technology and enforcing the

appropriate disciplinary measures

Educating Parents

Deaf Hill Primary School will work in partnership with pupils, parents and carers to ensure pupils stay safe online at school and at home. Parents and carers will be provided with information about the school's approach to online safety and their role in protecting their children. Parents and carers will be given a copy of the Acceptable Use Agreement at the point in which their child joins the school and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

Parents and carers will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents and carers will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age inappropriate content.

Parental awareness regarding how they can support their children to be safe online will be raised in the following ways:

- Parents' evenings
- Dedicated training sessions
- Newsletters
- Online resources
- Promotion via social media the school website

Filtering and Monitoring Online Activity

The Governing Body, together with the wider Ad Academy Trust, will ensure the school's ICT network has appropriate filters and monitoring systems in place and that it is Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk).

The Governing Body will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The Headteacher and ICT technicians from OneIT will undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems implemented will be appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks. ICT technicians will undertake regular checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system will be directed to the Headteacher.

Prior to making any changes to the filtering system, ICT technicians and the Headteacher/DSL will conduct a risk assessment. Reports of inappropriate websites or materials will be made to an ICT technician immediately, who will investigate the matter and make any necessary changes.

Deliberate breaches of the filtering system will be reported to the Headteacher/DSL and ICT Technicians, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy.

If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g.

- Internet Watch Foundation - Eliminating Child Sexual Abuse Online – Internet Watch Foundation (iwf.org.uk)

- CEOP - CEOP Safety Centre

- Police

The school's network and school-owned devices will be appropriately monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Child Protection and Safeguarding Policy.

Network Security

Technical security features, such as anti-virus software, will be kept up-to-date and managed by ICT technicians through OneIT. Firewalls will be switched on at all times. OneIT will review the firewalls to ensure they are running correctly, and to carry out any required updates. Staff and pupils will be advised not to download unapproved software or open unfamiliar email attachments, and will be expected to report all malware and virus attacks directly to OneIT.

All members of staff will have their own unique usernames and private passwords to access the school's systems. Pupils in Key Stage 2 will be provided with their own unique username and private passwords. Staff members and pupils will be responsible for keeping their passwords private. Passwords will have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible. Users are not permitted to share their login details with others and will not be allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, the Headteacher will be informed and will decide the necessary action to take. Users will be required to lock access to devices and systems when they are not in use

Emails

Access to and the use of emails will be managed in line with the Acceptable Use Agreement. Staff will be given approved school email accounts and will only be able to use these accounts at school and when doing school-related work outside of school hours.

Prior to being authorised to use the email system, staff must agree to and sign the Acceptable Use Agreement – these will be sent out annually. Personal email accounts will not be permitted to be used on the school site.

Staff members and pupils will be required to block spam and junk mail, and report the matter to OneIT. The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened. Deaf Hill Primary School will work to improve its cyber security culture and educate staff through the use of Boxphish, which provides real-world phishing simulations, training content and actionable data - Cyber Awareness Training & Phishing Simulations | Boxphish

School Website

The Headteacher will be responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements. This will be done in liaison with OneIT.

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training for staff, governors and volunteers

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
  - Abusive, threatening, harassing and misogynistic messages
  - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
  - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks

- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and DDSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

Monitoring arrangements

The senior leaders, teachers and DSLs log behaviour and safeguarding issues related to online safety on CPOMs.

This policy will be reviewed annually by the Headteacher. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

Appendix A: Online harms and risks – curriculum coverage

Subject area	Description and teaching content	Curriculum area the harm or risk is covered in
How to navigate the internet and manage information		
Age restrictions	Some online activities have age restrictions because they include content which is not appropriate for children under a specific age. Teaching includes the following: • That age verification exists and why some online platforms ask users to verify their age • Why age restrictions exist • That content that requires age verification can be damaging to under-age consumers • What the age of digital consent is (13 for most platforms) and why it is important	This risk or harm is covered in the following curriculum areas: • Health education • Computing
How content can be used and shared	Knowing what happens to information, comments or images that are put online. Teaching includes the following: • What a digital footprint is, how it develops and how it can affect pupils' futures • How cookies work • How content can be shared, tagged and traced • How difficult it is to remove something once it has been shared online • What is illegal online, e.g. youth-produced sexual imagery (sexting)	This risk or harm is covered in the following curriculum areas: • Relationships education • RSE • Health education • Computing
Disinformation, misinformation and hoaxes	Some information shared online is accidentally or intentionally wrong, misleading or exaggerated. Teaching includes the following: • Disinformation and why individuals or groups choose to share false information in order to deliberately deceive • Misinformation and being aware that false and misleading information can be shared inadvertently	This risk or harm is covered in the following curriculum areas: • Relationships and health education • Computing

	• Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons • That the widespread nature of this sort of content can often appear to be a stamp of authenticity, making it important to evaluate what is seen online • How to measure and check authenticity online • The potential consequences of sharing information that may not be true	
Fake websites and scam emails	Fake websites and scam emails are used to extort data, money, images and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or other, gain. Teaching includes the following: • How to recognise fake URLs and websites • What secure markings on websites are and how to assess the sources of emails • The risks of entering information to a website which is not secure • What pupils should do if they are harmed, targeted, or groomed as a result of interacting with a fake website or scam email • Who pupils should go to for support	This risk or harm is covered in the following curriculum areas: • Relationships education • RSE • Computing
Online fraud	Fraud can take place online and can have serious consequences for individuals and organisations. Teaching includes the following: • What identity fraud, scams and phishing are • That children are sometimes targeted to access adults' data • What 'good' companies will and will not do when it comes to personal details	This risk or harm is covered in the following curriculum areas: • Relationships education • RSE • Computing
Password phishing	Password phishing is the process by which people try to find out individuals' passwords so they can access protected content. Teaching includes the following: • Why passwords are important, how to keep them safe and that others might try to get people to reveal them • How to recognise phishing scams • The importance of online security to protect against viruses that are designed to gain access to password information	This risk or harm is covered in the following curriculum areas: • Relationships education • Computing

	• What to do when a password is compromised or thought to be compromised	
Personal data	Online platforms and search engines gather personal data – this is often referred to as 'harvesting' or 'farming'. Teaching includes the following: • How cookies work • How data is farmed from sources which look neutral • How and why personal data is shared by online companies • How pupils can protect themselves and that acting quickly is essential when something happens • The rights children have with regards to their data • How to limit the data companies can gather	This risk or harm is covered in the following curriculum areas: • Relationships education • Computing
Persuasive design	Many devices, apps and games are designed to keep users online for longer than they might have planned or desired. Teaching includes the following: • That the majority of games and platforms are designed to make money, and that their primary driver is to encourage people to stay online for as long as possible • How notifications are used to pull users back online	This risk or harm is covered in the following curriculum areas: • Health education • Computing
Privacy settings	Almost all devices, websites, apps and other online services come with privacy settings that can be used to control what is shared. Teaching includes the following: • How to find information about privacy settings on various devices and platforms • That privacy settings have limitations	This risk or harm is covered in the following curriculum areas: • Relationships education • RSE • Health education • Computing
Targeting of online content	Much of the information seen online is a result of some form of targeting. Teaching includes the following: • How adverts seen at the top of online searches and social media have often come	This risk or harm is covered in the following curriculum areas:

	from companies paying to be on there and different people will see different adverts • How the targeting is done • The concept of clickbait and how companies can use it to draw people to their sites and services	• Relationships education • PSHE • Health education • Computing
How to stay safe online		
Online abuse	Some online behaviours are abusive. They are negative in nature, potentially harmful and, in some cases, can be illegal. Teaching includes the following: • The types of online abuse, including sexual harassment, bullying, trolling and intimidation • When online abuse can become illegal • How to respond to online abuse and how to access support • How to respond when the abuse is anonymous • The potential implications of online abuse • What acceptable and unacceptable online behaviours look like	This risk or harm is covered in the following curriculum areas: • Relationships education • RSE • Health education • Computing • PSHE
Challenges	Online challenges acquire mass followings and encourage others to take part in what they suggest. Teaching includes the following: • What an online challenge is and that, while some will be fun and harmless, others may be dangerous and even illegal • How to assess if the challenge is safe or potentially harmful, including considering who has generated the challenge and why • That it is okay to say no and to not take part in a challenge • How and where to go for help • The importance of telling an adult about challenges which include threats or secrecy, such as 'chain letter' style challenges	This risk or harm is covered in the following curriculum areas: • Relationships education • RSE • PSHE
Content which incites violence	Knowing that violence can be incited online and escalate very quickly into offline violence. Teaching includes the following: • That online content (sometimes gang related) can glamorise the possession of weapons and drugs	This risk or harm is covered in the following curriculum areas: • Relationships education

	• That to intentionally encourage or assist in an offence is also a criminal offence • How and where to get help if they are worried about involvement in violence	• RSE • PSHE
Fake profiles	Not everyone online is who they say they are. Teaching includes the following: • That, in some cases, profiles may be people posing as someone they are not or may be 'bots' • How to look out for fake profiles	This risk or harm is covered in the following curriculum areas: • Relationships education • PSHE • Computing
Grooming	Knowing about the different types of grooming and motivations for it, e.g. radicalisation, child sexual abuse and exploitation, and gangs and county lines. Teaching includes the following: • Boundaries in friendships with peers, in families, and with others • Key indicators of grooming behaviour • The importance of disengaging from contact with suspected grooming and telling a trusted adult • How and where to report grooming both in school and to the police At all stages, it is important to balance teaching pupils about making sensible decisions to stay safe whilst being clear it is never the fault of the child who is abused and why victim blaming is always wrong.	This risk or harm is covered in the following curriculum areas: • Relationships education • PSHE
Livestreaming	Livestreaming (showing a video of yourself in real-time online, either privately or to a public audience) can be popular with children, but it carries a risk when carrying out and watching it. Teaching includes the following: • What the risks of carrying out livestreaming are, e.g. the potential for people to record livestreams and share the content • The importance of thinking carefully about who the audience might be and if pupils would be comfortable with whatever they are streaming being shared widely	This risk or harm is covered in the following curriculum areas: • PSHE

	• That online behaviours should mirror offline behaviours and that this should be considered when making a livestream • That pupils should not feel pressured to do something online that they would not do offline • Why people sometimes do and say things online that they would never consider appropriate offline • The risk of watching videos that are being livestreamed, e.g. there is no way of knowing what will be shown next • The risks of grooming	
Unsafe communication	Knowing different strategies for staying safe when communicating with others, especially people they do not know or have not met. Teaching includes the following: • That communicating safely online and protecting your privacy and data is important, regardless of who you are communicating with • How to identify indicators of risk and unsafe communications • The risks associated with giving out addresses, phone numbers or email addresses to people pupils do not know, or arranging to meet someone they have not met before • What online consent is and how to develop strategies to confidently say no to both friends and strangers online	This risk or harm is covered in the following curriculum areas: • Relationships education • Computing
Wellbeing		
Impact on confidence (including body confidence)	Knowing about the impact of comparisons to 'unrealistic' online images. Teaching includes the following: • The issue of using image filters and digital enhancement • The role of social media influencers, including that they are paid to influence the behaviour of their followers • The issue of photo manipulation, including why people do it and how to look out for it	This risk or harm is covered in the following curriculum areas: • PSHE • Computing

Impact on quality of life, physical and mental health and relationships	Knowing how to identify when online behaviours stop being fun and begin to create anxiety, including that there needs to be a balance between time spent online and offline. Teaching includes the following: • How to evaluate critically what pupils are doing online, why they are doing it and for how long (screen time) • How to consider quality vs. quantity of online activity • The need for pupils to consider if they are actually enjoying being online or just doing it out of habit, due to peer pressure or due to the fear or missing out • That time spent online gives users less time to do other activities, which can lead some users to become physically inactive • The impact that excessive social media usage can have on levels of anxiety, depression and other mental health issues • That isolation and loneliness can affect pupils and that it is very important for them to discuss their feelings with an adult and seek support • Where to get help	This risk or harm is covered in the following curriculum areas: • PSHE
Online vs. offline behaviours	People can often behave differently online to how they would act face to face. Teaching includes the following: • How and why people can often portray an exaggerated picture of their lives (especially online) and how that can lead to pressures around having perfect or curated lives • How and why people are unkind or hurtful online when they would not necessarily be unkind to someone face to face	This risk or harm is covered in the following curriculum areas: • Relationships education • PSHE
Suicide, self-harm and eating disorders	Pupils may raise topics including eating disorders, self-harm and suicide. Teachers must be aware of the risks of encouraging or making these seem a more viable option for pupils and should take care to avoid giving instructions or methods and avoid using language, videos and images.	

Appendix 2 - Technology acceptable use agreement for pupils

Deaf Hill Primary School understands the benefits technology can have on enhancing the curriculum and pupils' learning; however, we must ensure that pupils respect school property and use technology appropriately. To achieve this, we have created this acceptable use agreement which outlines our expectations of pupils when using technology, whether this is on personal or school devices and on or off the school premises.

Please read this document carefully and sign below to accept that you agree to the terms outlined.

1. **Using technology in school**

- I will only use ICT systems, e.g. computers, laptops and tablets, which my **class teacher** has given me permission to use.
- I will only use the approved email account that has been provided to me by OneIT.
- I will not store or use any personal data relating to a pupil or staff member for non-school related activities. If I have any queries about storing or using personal data, I will speak to my **class teacher**.
- I will delete any chain letters, spam, and other emails from unknown senders without opening them.
- I will ensure that I get permission from my **class teacher** before accessing learning materials, e.g. source documents, from unapproved sources.
- I will only use the internet for personal use during out-of-school hours, including break and lunchtimes. During school hours, I will use the internet for school work only.
- I will not share my passwords, e.g. to my school email account, with anyone.
- I will not install any software onto school ICT systems unless instructed to do so by my **class teacher**.
- I will only use recommended removable media, e.g. encrypted USB drives, and I will keep all school-related information stored on these secure.
- I will adhere to the online safety guidelines I have been taught.
- I will only use the school's ICT facilities to:
  - Complete homework and coursework.
  - Prepare for lessons and tests.
  - Undertake revision and research.
  - Gather or process information for extracurricular activities, e.g. creating the school newsletter.

- I will not use the school's ICT facilities to access, download, upload, send, receive, view or display any of the following:
    - Illegal material
    - Any content that could constitute a threat, bullying or harassment, or anything negative about other persons or the school
    - Content relating to a person's sexual orientation, gender, religion, race, disability or age
    - Online gambling
    - Content which may adversely affect the reputation of any organisation (including the school) or person, whether or not they are known to be true or false
    - Any sexually explicit content
    - Any personal data or information

2. Mobile devices

- I will not use my own devices in school, all devices will be left at home or handed in when I arrive at school if I accidentally bring it to school or Mrs Haylock has given me permission to bring it to school.
- I will not take or store images or videos of staff members on any mobile device, regardless of whether or not it is school-owned.

3. Social media

- I will not use any school-owned mobile devices to access personal social networking platforms.
- I will not communicate or attempt to communicate with any staff member over personal social networking platforms.
- I will not accept or send 'friend' or 'follow' requests from or to any staff member over personal social networking platforms.
- I will ensure that I apply the necessary privacy settings to any social networking sites.
- I will not publish any comments or posts about the school on any social networking platforms which may affect the school's reputation.
- I will not post or upload any defamatory, objectionable, copyright-infringing or private material, including images and videos of pupils, staff or parents, on any online website.
- I will not post any material online that:
    - Is offensive.
    - Is private or sensitive.

- Infringes copyright laws.
- Damages the school's reputation.
- Is an image or video of any staff member, parent or nonconsenting pupil.

4. Reporting misuse

- I will ensure that I report any misuse or breaches of this agreement by pupils or staff members to the **headteacher**.
- I understand that my use of the internet will be monitored by the **online safety officer** and recognise the consequences if I breach the terms of this agreement, e.g. having personal devices confiscated.
- I understand that the **headteacher** may decide to take disciplinary action against me in accordance with the school's **Behavioural Policy** if I breach this agreement.

I acknowledge that I have read and understood this agreement, and ensure that I will abide by each principle.

Name of pupil:	
Signed:	
Date:	
Name of class teacher:	
Signed:	
Date:	

-

To be sent out annually – recorded on Trust Safeguarding CPD Record

Appendix 3 Device and technology acceptable use agreement for staff

Whilst our school promotes the use of technology or devices, and understands the positive effects they can have on enhancing pupils' learning and community engagement, we must also ensure that staff use technology and devices appropriately. Any misuse of technology and devices will not be taken lightly and will be reported to the **headteacher** in order for any necessary further action to be taken.

This agreement outlines staff members' responsibilities when using technology and devices, both school-owned and personal, and applies to all staff, volunteers, contractors and visitors.

Please read this agreement carefully, and sign at the bottom to show you agree to the terms outlined.

Data protection and cyber-security

I will:

- Use technology and devices, including the use and storage of personal data, in line with data protection legislation, including the Data Protection Act 2018 and UK GDPR.
- Follow the school's **Data Protection Policy** and any other relevant school policies and procedures.

I will not:

- Attempt to bypass any filtering, monitoring and security systems.
- Share school-related password with pupils, staff, parents or others unless permission has been given for me to do so.

Using technology in school

I will:

- Follow the **Staff Behaviour Policy**.
- Only use ICT systems which I have been permitted to use.
- Ensure I obtain permission prior to accessing materials from unapproved sources.
- Only use the internet for personal use during out-of-school hours, including break and lunch time.
- Only use recommended removable media and keep this securely stored.

I will not:

- Install any software onto school ICT systems unless instructed to do so by the **headteacher** or **ICT technician**.
- Search for, view, download, upload or transmit any inappropriate material when using the internet.

Emails

I will:

- Only use the approved email accounts that have been provided to me when sending communications regarding school business.
- Ensure any personal information that is being sent via email is only sent to the relevant people and is appropriately protected.

I will not:

- Use personal emails to send and/or receive school-related personal data or information, including sensitive information.
- Use personal email accounts to contact pupils or parents.

School-owned devices

I will:

- Only use school-owned devices for the purpose of carrying out my school responsibilities.
- Only access websites and apps that have been approved by the **headteacher**.
- Understand that the usage of my school-owned devices will be monitored.
- Keep my school-owned devices with me or within my sight at all times.
- Transport school-owned devices safely.
- Provide suitable care for my school-owned devices at all times.
- Only communicate with pupils and parents on school-owned devices using appropriate channels.
- Ensure I install and update security software on school-owned devices as directed by the **OneIT**.
- Seek permission from the **headteacher** before using a school-owned device to take and store photographs or videos of pupils, parents, staff and visitors.
- Immediately report any damage or loss of my school-owned devices to the **OneIT** Immediately report any security issues, such as downloading a virus, to the **OneIT** Understand that I am expected to pay an excess for any repair or replacements costs where the device was damaged or lost as a result of my own negligence.
- Make arrangements to return school-owned devices to the **OneIT** upon the end of my employment at the school.

I will not:

- Not permit any other individual to use my school-owned devices without my supervision, unless otherwise agreed by the **headteacher**.
- Install any software onto school-owned devices unless instructed to do so by the **headteacher** or **OneIT**.
- Use school-owned devices to send inappropriate messages, images, videos or other content.
- Use school-owned devices to view, store, download or share any inappropriate, harmful or illegal content.
- Use school-owned devices to access personal social media accounts.

Personal devices

I will:

- Only use personal devices during out-of-school hours, including break and lunch times.
- Ensure personal devices are either switched off or set to silent mode during school hours.
- Only make or receive calls in specific areas, e.g. the staff room.
- Store personal devices appropriately during school hours, e.g. a lockable cupboard in the classroom.
- Understand that I am liable for any loss, theft or damage to my personal devices.

I will not:

- Use personal devices to communicate with pupils or parents.
- Access the school's WiFi using a personal device unless permission to do so has been granted by the **headteacher** or **OneIT**.
- Use personal devices to take photographs or videos of pupils or staff.
- Store any school-related information on personal devices unless permission to do so has been given by the **headteacher**.

Social media and online professionalism

I will:

- Follow the school's **Staff Behaviour Policy**.
- Understand that I am representing the school and behave appropriately when posting on school social media accounts.
- Ensure I apply necessary privacy settings to social media accounts.

I will not:

- Communicate with pupils or parents over personal social media accounts.
- Accept 'friend' or 'follow' requests from any pupils or parents over personal social media accounts.
- Post any comments or posts about the school on any social media platforms or other online platforms which may affect the school's reputability.
- Post any defamatory, objectionable, copyright-infringing or private material, including images and videos of pupils, staff or parents, on any online website.
- Post or upload any images and videos of pupils, staff or parents on any online website without consent from the individuals in the images or videos.
- Give my home address, phone number, mobile number, social networking details or email addresses to pupils or parents – any contact with parents will be done through authorised school contact channels.

Working from home

I will:

- Ensure I obtain permission from the **headteacher** before any personal data is transferred from a school-owned device to a personal device.
- Ensure any data transferred from a school-owned device to a personal device is encrypted or pseudonymised.
- Ensure any sensitive personal data is not transferred to a personal device unless completely necessary – and, when doing so, that it is encrypted.
- Ensure my personal device has been assessed for security by **OneIT**. before it is used for home.
- Ensure no unauthorised persons, such as family members or friends, access any personal devices used for home working.

Training

I will:

- Participate in any relevant training offered to me, including cyber-security and online safety.
- Allow **OneIT**. to undertake regular audits to identify any areas of need I may have in relation to training.
- Employ methods of good practice and act as a role model for pupils when using the internet and other digital devices.
- Deliver any training to pupils as required.

Reporting misuse

I will:

- Report any misuse by pupils or staff members breaching the procedures outlined in this agreement to the **headteacher**.
- Understand that my use of the internet will be monitored by **OneIT**.and recognise the consequences if I breach the terms of this agreement.
- Understand that the **headteacher** may decide to take disciplinary action against me, in accordance with the **Disciplinary Policy and Procedure**, if I breach this agreement.