ONLINE SAFETY POLICY

This section should be completed following ratification of the Policy.

Audience	Executive Leaders and Trustees, All staff, DSL's and DDSL's, All parents, volunteers and visitors
Ratified	October 2024
Other Related Policies	Code of Conduct & Safeguarding & Child Protection Policy, General Data Protection Policy, Disciplinary Policy
Policy Owner	Trust Safeguarding Team, ARC Committee
Review Frequency	Within 18 months

Ownership
Preston Hedges Trust is responsible for the production and maintenance of this document. It is issued by the clerk, clerk@prestonhedges.org to whom any change requests or queries should be directed.

Page	Content
3	Statement of Intent
3	Legislation and Guidance
4	Roles and Responsibilities
6	Managing Online Safety
8	Cyberbullying
8	Child-on-child sexual abuse and harassment
9	Grooming and Exploitation
10	Mental Health
11	Online hoaxes and harmful online challenges
12	Cyber-crime
13	Online safety training for staff
13	Online safety and curriculum
14	Use of technology in the classroom
15	Use of smart technology
16	Educating parents
16	Internet Access
16	Filtering and Monitoring online activity
17	Network Security
18	Emails
18	Generative Artificial Intelligence (AI)
19	Social Networking
19	The Trust and schools websites
20	Remote Learning
21	Appendix 1: Online Safety Incident Report Log
22	Appendix 2: Acceptable Use Agreement (*staff, governors, volunteers and visitors*)
23	Appendix 3: Acceptable Use Agreement (EYFS)
25	Appendix 4: Acceptable Use Agreement (KS1)
27	Appendix 5: Acceptable Use Agreement (KS2)

1. Statement of Intent

Preston Hedges Trust understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the schools; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- Content: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.
- Contact: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- Conduct: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- Commerce: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our Trust has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

2. Legislation and Guidance

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'

3. Roles and Responsibilities

The Audit, Risk and Compliance Committee (ARC) will be responsible for:

- Regular review of this policy.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.

The Chief Operating Officer will be responsible for:

- The strategic responsibility for management of Online Safety is fulfilled including ensuring appropriate filtering and monitoring is in place and reviewed annually to ensure its effectiveness.
- Report any online safety incidents to ARC and demonstrate actions taken
- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.

The Principal will be responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the DSL and the deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.

The DSL and DDSL will be responsible for:

- Taking the lead responsibility for online safety in the school.

- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT technicians.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.
- Understanding the filtering and monitoring processes in place at the school.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- Maintaining detailed, secure and accurate written records of reported online safety concerns as well as the decisions and whether or not referrals have been made.
- Understanding the purpose of record keeping.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Engage with parents and the school community on Online Safety matters at school and/or at home.
- Reporting to the COO about online safety incidents on a termly basis or sooner if considered significant.

ICT technicians (via our service provider Sweethaven) will be responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the COO and Principals.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Working with the COO to conduct interim light-touch reviews of this policy and procedures.

All staff members will be responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.

- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- 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.

Pupils will be responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

Parents will be responsible for:

- Notifying a member of staff or the Principal of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet

4. Managing Online Safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The DSL will have overall responsibility for the school's approach to online safety, with support from deputies and the Principal where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all school operations in the following ways:

- Staff and Trustees receive regular training
- Parents will be made aware of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents via each school website.
- Online safety is integrated into learning throughout the curriculum
- Assemblies are conducted at least termly on the topic of remaining safe online

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 and Safeguarding Policy. They must be recorded on My Concern.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully – the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered.

Concerns regarding a staff member's online behaviour are reported to the Principal, via Confide. The Principal will then decide on the best course of action in line with the relevant policies. If the concern is about the Principal, it is reported to the COO or CEO.

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the Principal and ICT technicians, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the Principal contacts 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 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 are recorded on My Concern by the member of staff who has the obtained the information; the school's response are recorded by the DSL on My Concern.

5. Cyberbullying

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 i.e. homophobia, racism, misogyny/misandry.

The school will be 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 Anti-bullying Policy.

6. 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
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

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.

The school will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking "sides", often leading to repeat harassment. The school will respond to these incidents in line with the Child Protection and Safeguarding Policy.

The school will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse will be reported to the DSL via My Concern, who will investigate the matter in line with the Child Protection and Safeguarding Policy.

7. 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, e.g. 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 Safeguarding and 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 online.
- 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.

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 via My Concern, who will handle the situation in line with the Prevent Duty Policy.

8. Mental Health

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 / Online Safety Lead will 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 should be raised with the Principal or DSL.

9. 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 via My Concern.

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 Principal 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 and Safeguarding Policy.

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, 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 individual pupils at risk where appropriate.

The DSL and Principal 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.

10. 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 Principal will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

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.

11. Online safety training for staff

The DSL will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. 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.

12. Online safety and the curriculum

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

- Relationships and health education
- PSHE
- ICT

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
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- Knowledge and behaviours that are covered in the government's online media literacy strategy

The online risks pupils may face online are always considered when developing the curriculum.

Relevant members of staff, e.g. the SENCO and designated teacher for LAC, will work together to ensure the curriculum is tailored so that pupils who may be more vulnerable to online harms, e.g. pupils with SEND and LAC, 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 will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The Principal and DSL will 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 will 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 will advise the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities will be 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 will ensure 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.

13. Use of technology in the classroom

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

- Laptops
- Tablets
- Internet
- Apps
- VR Headsets

- Email
- 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 will review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law.
Pupils will be supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

14. Use of smart technology

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 for Pupils.

Staff will use all smart technology and personal technology in line with the school's Staff Acceptable Use Policy and agreement.

To ensure school is a safe place for our children and to enable them to be fully engaged with their learning, mobile phone use is prohibited throughout the school day, which includes break and lunchtimes.

This approach allows our schools to provide children with access to their mobile phone before and after school, while ensuring use is prevented during the school day. Pupils hand their phone in to a member of staff upon arrival and collect it at the end of the day.

Our schools will always consider reasonable adjustments to a ban on mobile phones. This may be required in line with the Equality Act 2010. For instance, where a pupil with SEND may need access to a mobile phone or similar device due to the nature of their disability, or where a child uses it to support a medical condition. These adjustments are also applied to staff.

Staff should not use their own mobile phone for personal reasons in front of pupils throughout the school day.

Smart watches which have the same kind of capabilities, technology and communication access as mobile phones, will be treated in the same way as phones and are required to be handed in on arrival at school.

The school will hold assemblies, where appropriate, which address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner.

The school will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

The school 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.

15. Educating parents

The school will work in partnership with parents to ensure pupils stay safe online at school and at home. Parents will be provided with information about the school's approach to online safety and their role in protecting their children. Parents will be sent a copy of the Acceptable Use Agreement at the beginning of each academic year and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

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

- Communications home
- Information via our website
- Online Safety Policy, accessed via the website

16. Internet Access

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. A record will be kept of users who have been granted internet access in the school office.

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.

17. Filtering and Monitoring online activity

ARC will ensure the school's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's 'Filtering and monitoring standards for schools and colleges'. ARC 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 DSL will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs.

The COO, Principal and ICT technicians will undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school implements 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 monthly 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 COO. Prior to making any changes to the filtering system, COO, ICT technicians with input from the DSL will conduct a risk assessment. Any changes made to the system will be recorded by ICT technicians. Reports of inappropriate websites or materials will be made to an ICT technicians immediately, who will investigate the matter and makes any necessary changes.

Deliberate breaches of the filtering system will be reported to the DSL and ICT technicians, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, this will be dealt with under 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. the Internet Watch Foundation (IWF), CEOP and/or the police.

The school's network and school-owned devices will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL via My Concern who will manage the situation in line with the Child Protection and Safeguarding Policy.

18. Network security

Technical security features, such as anti-virus software, will be kept up-to-date and managed by ICT technicians. Firewalls will be switched on at all times. ICT technicians will review the firewalls on a weekly basis 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 to ICT technicians.

All members of staff will have their own unique usernames and private passwords to access the school's systems. Pupils will be unable to access any device without a unique username and private passwords. Staff members will be responsible for keeping their passwords private.

Users will inform ICT technicians if they forget their login details, who will arrange for the user to access the systems under different login details. Users will not be 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 Principal 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. Full details of the school's network security measures can be found in the Cyber-security Policy.

19. Emails

Access to and the use of emails will be managed in line with the Data Protection Policy, Acceptable Use Agreements.

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. Personal email accounts will not be permitted to be used on the school site. Any email that contains sensitive or personal information will only be sent using secure and encrypted email.

Staff members will be required to block spam and junk mail, and report the matter to ICT technicians. 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. The COO will ensure education to staff on what phishing emails and other malicious emails might look like:

- How to determine whether an email address is legitimate
- The types of address a phishing email could use
- The importance of asking "does the email urge you to act immediately?"
- The importance of checking the spelling and grammar of an email

Any cyber-attacks initiated through emails will be managed in line with the Cyber Response and Recovery Plan.

20. Generative Artificial Intelligence (AI)

The school will take steps to prepare pupils for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to pupils' age.

The school will ensure its IT system includes appropriate filtering and monitoring systems to limit pupil's ability to access or create harmful or inappropriate content through generative AI.

The school will ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI.

The school will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.

The school will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

21. Social networking

The Trust and schools have an official Facebook, Twitter and Instagram accounts, managed by the Marketing and Communications Officer and Principals. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

All posts made to Trust or school social media accounts will not breach copyright, data protection or freedom of information legislation. The Trust and school's social media accounts will comply with the platform's rules.

Staff

Staff will not be prohibited from having personal social media accounts; however, it is important that staff protect their professional reputation by ensuring they use personal social media accounts in an appropriate manner.

Parents

Parents are able to comment on or respond to information shared via social media sites; however, parents should do so in a way which does not damage the reputation of the school.

Parents will be asked not to share any photos or personal details of pupils when commenting on school social media sites, nor post comments concerning other pupils or staff members.

Any parents that are seen to be breaching the guidance in this policy will be required to attend a meeting with the Principal, and may have their ability to interact with the Trust or schools social media websites removed.

22. The Trust and schools websites

The Marketing and Communications Officer and Principal will be responsible for the overall content of the Trust and schools website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

23. Remote learning

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

PRESTON HEDGES TRUST

FUN
CREATIVITY
ACHIEVEMENT

Appendix 1: online safety incident report log

Details of ALL online safety incidents to be recorded by the DSL/DDSL or Principal. This incident log will be monitored termly by the Principal, COO and ARC Committee. Any incidents involving cyber-bullying may also need to be recorded in Arbor under the behaviour log.

ONLINE SAFETY INCIDENT LOG					
Date	Name of pupil or staff member	Where the incident took place	Description of the incident	Action taken	Recorded by (Name & Signature)

PRESTON HEDGES TRUST

FUN
CREATIVITY
ACHIEVEMENT

Appendix 2: acceptable use agreement (staff, trustees, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
• When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way that could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material that might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	Date:

Appendix 3: Acceptable Use Agreement (EYFS)

My Learning 	• I will use school devices (PCs, laptops, tablets/ ipads) for my learning. • I will ask a teacher before using a device and ask for help if I can't work the device. • I will only use activities that a teacher has told or allowed me to use. • I will ask a teacher if I am not sure what to do or I think I have done something wrong. • I will look after the school's computing equipment and tell a teacher if something is broken or not working properly.
My Online Safety 	• I will always use what I have learned about Online Safety to keep myself safe. • I will tell a teacher if I see something that upsets me on the screen.
Using the Internet at School 	• I will only use the internet when the teacher says I can. • I will only go on websites that my teacher allows me to. • I will tell my teacher if I go on a website by mistake.
Using the Internet at Home 	• I will tell a trusted adult if I see something that upsets me on the screen

I understand that these rules help me to stay safe and I agree to follow them. I also understand that if I break the rules I might not be allowed to use the school's computing equipment.

My Name is_____

Parents / Carers: I understand that the school has discussed the Acceptable Use Agreement with my child and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my child's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Parents Signature_____ Date_____

Appendix 4: Acceptable Use Agreement (KS1)

My Learning 	• I will use school devices (laptops, tablets/ ipads) for my learning. • I will ask a teacher before using a device and ask for help if I can't work the device. • I will only use activities that a teacher has told or allowed me to use. • I will ask a teacher if I am not sure what to do or I think I have done something wrong. • I will look after the school's computing equipment and tell a teacher if something is broken or not working properly.
My Online Safety 	• I will always use what I have learned about Online Safety to keep myself safe. • I will tell a teacher if I see something that upsets me on the screen.
Using the Internet at School 	• I will only use the internet when the teacher says I can. • I will only go on websites that my teacher allows me to. • I will tell my teacher if I go on a website by mistake.
Using the Internet at Home 	• I will not share personal information about myself when on-line (names, addresses, telephone numbers, age, gender, school details) • Where I have my own username and password, I will keep it safe and secret. • I will tell a trusted adult if I see something that upsets me on the screen. My use of Social Media and Gaming • I understand that certain sites and games have age restrictions to keep me safe.

	• I understand that by accessing such sites and games, I maybe putting myself at risk of accessing inappropriate content and cyberbullying.

I understand that these rules help me to stay safe and I agree to follow them. I also understand that if I break the rules I might not be allowed to use the school's computing equipment.

My Name is_____

Parents / Carers: I understand that the school has discussed the Acceptable Use Agreement with my child and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my child's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Parents Signature_____ Date_____

Appendix 5: Acceptable Use Agreement (KS2)

My Learning 	• I will use school devices (PCs, laptops, tablets/ ipads) for my learning. • I will ask a teacher before using a device and ask for help if I can't work the device. • I will only use activities that a teacher has told or allowed me to use. • I will ask a teacher if I am not sure what to do or I think I have done something wrong. • I will look after the school's computing equipment and tell a teacher if something is broken or not working properly. • When logging on using my own username and password, I will keep it safe and secret. • I will save only school work on the school computer and will check with my teacher before printing. • I will log off or shut down a computer when I have finished using it.
Using the Internet at School 	• I will only visit sites that are appropriate to my learning at the time My School Accounts • I will keep my username and password safe and secure - I will not share it. I will not try to use any other person's username and password. • I understand that I should not write down or store a password where it is possible that someone may steal it. My role as a Digital Citizen. • I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online to a trusted adult.

	• I will respect other people's work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission. • I will not take or distribute images of anyone without their permission.
Using the Internet at Home 	• I will ask permission and only use the devices, apps, sites and games I am allowed to and when I am allowed to • I will be a good friend online – I won't share or say anything I know would upset another person or they wouldn't want shared. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them. • I will not bully other – I know just calling something fun or banter doesn't stop it maybe hurting someone else. I will not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell a trusted adults. • I will be careful what I click on and not click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so I will always check. • I will ask for help if I am scared or worried and talk to a trusted adult if anything upsets me or worries me on an app, site or game. • I will tell a trusted adult if I see or someone send me something bad – I know it's not my fault and I won't get in trouble, but I will not share it. • I will only communicate and collaborate online – with people I already know and have met in real life or that a trusted adult knows about. • I know online friends might not be who they say they are – I will be careful when someone wants to be my friend. Unless I have met them face to face, I know I can't be sure who they are. • I will never pretend to be someone else online – it can be upsetting or even dangerous.

	• I will check with a parent/carer before I meet an online friend the first time; I will never go alone. • I will not go live (videos anyone can see) on my own – and always check if it is allowed. I will check with a trusted adult before I video chat with anybody for the first time. • I will not take photos or videos or people without them knowing or agreeing to it – and I will never film fights or people when they are upset or angry. Instead ask an adult or help if it's safe. • I will keep my body to myself online and will never get changed or show what's under my clothes when using a device with a camera. I remember my body is mine and no-one should tell me what to do with it; I will not send any photos or videos without checking with a trusted adult. • I will not do something just because someone dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I will say no, stop chatting and tell a trusted adult immediately. • I will follow all age rules and only register for sites or apps that are suitable for my age • I will be private online and only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.

I understand that these rules help me to stay safe and I agree to follow them. I also understand that if I break the rules I might not be allowed to use the school's computing equipment.

My Name is_____

Parents / Carers: I understand that the school has discussed the Acceptable Use Agreement with my child and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my child's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Parents Signature_____ Date_____