ONLINE SAFETY POLICY

This section should be completed following ratification of the Policy.

Audience	DSL's & All Safeguarding Staff, Trust Leaders & Trustees, All staff & All Parents
Ratified	March 2023
Other Related Policies	Code of conduct & General Data Protection Policy & Child Protection & Safeguarding Policy
Policy Owner	Trust Safeguarding Team & Compliance Committee
Review Frequency	Annually in March

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.

Contents:

Appendix 1	Preston Hedges Trust Filtering Change Log
	Twitter Appendix to Online Safety
	Facebook Appendix to Online Safety Policy
	Instagram Appendix to Online Safety Policy
	Seesaw - Remote Learning Appendix to Online Safety Policy
	Zoom - Remote Learning Appendix to Online Safety Policy
	ICT Risk Assessment Log
	List of words to block comments on Facebook:

1. Introduction

For clarity, the Online Safety policy uses the following terms unless otherwise stated:

Users – refers to staff, trustees, school volunteers, students and any other person working in or on behalf of the school, including contractors.

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school/Trust site, e.g. visits, conferences, school trips etc.

Wider school community – students, all staff, Trustees, parents

Computing and the internet have become integral to teaching and learning within schools, providing children, young people and staff with opportunities to improve understanding and access online resources at the touch of a button.

At present, the internet based technologies children and young people are using inside and outside of the classroom are:

- Websites
- Social Media
- Apps
- Mobile phones

- Other mobile devices such as tablets and gaming devices
- Online gaming
- Blogs and Wikis
- Learning Platforms and Virtual Learning Environments
- VR Headsets
- Email, Instant Messaging and Chat Rooms
- Podcasting
- Video sharing
- Downloading
- On demand streaming video, radio /Smart TVs

Whilst technology has many benefits for our school community, we recognize that clear procedures for appropriate use and educations for staff and students about online behaviours, age restrictions and potential risks are crucial. All schools have a duty to ensure that children and young people are protected from potential harm both within and beyond the school environment. Every effort will be made to safeguard against all risks, however it is likely that we will never be able to completely eliminate them.
Organisations must be aware that children and staff cannot be completely prevented from risks using the internet. In accordance with Ofsted requirements, young people need to be empowered and educated to make healthy and responsible decisions when using the internet – in particular social media. Online Safety, like safeguarding must be a whole school approach, and all staff must take appropriate measures to keep young people and themselves safe using the internet and social media. Members of staff also need to be aware of how to manage their own professional reputation online and demonstrate online behaviours that are in line with their professional role. Any incidents that do arise will be dealt with quickly and according to policy to ensure that children, young people and staff continue to be protected.

Online safeguarding, known as Online Safety, is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an Online Safety incident, whichever is sooner. This policy is to be used in conjunction with the Trust's Safeguarding and Child Protection Policy, with any Online Safety concerns noted to be immediately shared with the DSL or DDSL in the individual schools.

Both this policy and the Acceptable Use Agreement (for all stakeholders) are inclusive of fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboard, digital video equipment; and technologies owned by children and staff but brought onto school premises (such as mobile phones or other mobile devices).

2. Aim & scope of the policy

- To emphasise the need to educate staff and children about the pros and cons of technology in, and outside of, a school environment.
- To provide safeguards and rules for acceptable use to guide the wider school community in their online experiences.
- To ensure adults are clear about procedures for misuse of technology within and beyond the school setting.
- To ensure risks are identified, assessed. And mitigated (where possible) in order to reduce any foreseeable harm to the student, or liability to the school.
- To deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.

The scope of this policy:

This policy applies to all staff,children, trustees, visitors and contractors accessing the internet or using technological devices on school premises. This includes staff or pupil use of personal devices, such as mobile phones, which are brought onto school grounds. This policy is also applicable where staff or individual have been provided with school issued devices for use off-site e.g. a school laptop.

3. Responsibilities

Trust Compliance Committee
The Trust Compliance Committee is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy annually, or, in response to any online safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school and to ensure online safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.

Chief Operating Officer

Reporting to the Chief Executive Officer, Compliance Committee and Trust Board the Chief Operating Officer has strategic responsibility for Online Safety within the Trust.

The Chief Operating Officer will ensure that:

- The strategic responsibility for management of Online Safety is fulfilled through working in partnership with Trust and school leaders and external partners
- Ensure that Online Safety training is undertaken by all schools annually or in response to an Online safety incident
- Ensure the Compliance Committee is updated of any Online Safety related incidents and that appropriate mitigating steps are taken
- Ensure the policy is updated annually and distributed to Trust Leaders and the Trust Safeguarding Lead

Principal

Reporting to the Chief Executive Officer, the Compliance Committee and the Trust Board the Principal/Executive Principal has overall responsibility for Online Safety within the Trust's schools. The day-to-day management of this will be delegated to a member of staff, the Online Safety Lead (or more than one), as indicated below.

Principal will ensure that:

- In conjunction with the Chief Operating Officer ensure Online Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and parents.
- The designated Online Safety Lead(s) has had appropriate CPD in order to undertake the day-to-day duties.
- All Online Safety incidents are dealt with promptly and appropriately and shared with the Chief Operating Officer. The designated adults for updating Securus & Online concern logs are dealing with incidents promptly and appropriately.

DSL and DDSL

- Remain updated with relevant safeguarding needs regarding Online Safety
- Alert and advise the Principal and Online Safety Lead of any necessary additions needed in the policy
- Provide safeguarding training to staff including Online Safety procedures and how to respond to Online Safety incidents, alongside the Online Safety officer.

Online Safety Lead

The Online Safety Lead will:

- Keep up to date with the latest risks to children whilst using technology; familiarize him/herself with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Principal.
- Advise the Principal, on all Online Safety matters.
- Engage with parents and the school community on Online Safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for the Online Safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical Online Safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.
- Make him/herself aware of any reporting function with technical Online Safety measures, i.e. internet filtering reporting function; liaise with the Principal and Chief Operating Officer to decide on what reports may be appropriate for viewing.

ICT Technical Support Staff

Technical support staff are responsible for ensuring the following in partnership with the Chief Operating Officer.

- The IT technical infrastructure is secure; this will include at a minimum:
- Ensure all aspects of their contractual obligations are fulfilled.
- Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
- Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
- Any Online Safety technical solutions such as Internet filtering are operating correctly.
- Filtering levels are applied appropriately and according to the age of the user; those categories of use are discussed and agreed with the Online Safety Lead and Principal.
- That any problems or faults related to filtering are reported to a Designated Safeguarding Lead and the broadband provider immediately, and are passed to the DSL and Online Safety Lead.
- The Online Safety Incident Log is monitored and incidents are reported to the Online Safety Lead (s)

- Passwords are applied correctly and regularly changed.
- He/she keeps up to date with Online Safety information in order to maintain the security of the school network.
- The use of the network by all users is regularly monitored in order that any deliberate of accidental misuse can be reported to the Online Safety Lead and the Principal.

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Principal.
- Any Online Safety incident is reported to the Online Safety Lead (and an Online Safety Incident report is made), or in his/her absence to the Principal. If you are unsure the matter is to be raised with the Online Safety Officer or the Principal to make a decision.
- The reporting flowcharts contained within this Online Safety policy are fully understood.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- All staff must read and sign agreement with the Acceptable Use Policy. This is reviewed every 12 months.
- Personal use of social media sites outside of school is discreet. Advice is given to all staff on this matter. Staff understand the need to protect their reputations and that of the school, and sign the Acceptable Use Policy to demonstrate this.

All Students

The boundaries of use of ICT equipment and services in this school are given in the student Acceptable Use Policy which is shared with children and on display in the ICT suite; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

Online Safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly, all students will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to

ensure the safety of children outside the school environment. The school will keep parents up to date with new and emerging Online Safety risks, and will involve parents in strategies to ensure that students are empowered.

Parents must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded. As such parents will all receive a copy of the student Acceptable Use Policy

4. Legislation & Guidance

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

Teaching online safety in schools

Preventing and tackling bullying and cyber-bullying: advice for Principals and school staff

Searching, screening and confiscation

It also refers to the Department'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 children' electronic devices where they believe there is a 'good reason' to do so.

This policy complies with our funding agreement and articles of association.

5. Educating Children about Online Safety

Using the internet is part of the curriculum and is a fantastic and necessary tool. Its use raises educational standards, and allows children to demonstrate responsibility and a mature approach. However, it is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Preston Hedges Trust will have an annual programme of training which is suitable to the audience.

- Online Safety for students is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning.
- Key online safeguarding messages are reinforced whenever ICT is used in learning.
- Our RSE scheme of work incorporates lessons on Online Safety.
- Children are made aware of copyright issues, data protection, intellectual property and reliability of information sourced on the internet as part of the curriculum.
- Children have opportunities for informal discussions about on-line risks and strategies for protecting yourself as part of the Online Safety curriculum.
- The schools have termly assemblies, followed by online safety lessons discussing the aspect further, broken into phases at an age-appropriate level, to discuss important aspects of Online Safety. These include :

    - what to do when something inappropriate pops up online
    - not sharing personal information
    - the dangers of sharing information (both of themselves and others)
    - PEGI ratings, stranger-danger online, and general how to keep safe online.
    - As children get older, the Online Safety Curriculum becomes more advanced and includes:
    - copyright issues
    - illegal downloading
    - data protection
    - intellectual property
    - reliability of information sourced on the internet as part of the curriculum
    - viruses, trojans, piggybacks vias downloads and email
    - cyber-bullying
    - digital imagery, the prolific use of photo-editing and wellbeing
    - dangers of chatrooms and online gaming
    - mental health and resilience to what is being seen or heard online including negative comparison to perfection seen in apps and social media.
    - how online content and people online may manipulate and persuade other
    - recognise healthy and unhealthy friendships online
    - at all times, the curriculum outlines the wonderful aspects of being online, whilst understanding the dangers, and has a focus on

enabling the children to protect themselves and have strategies on how to protect themselves online.
    - https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811796/Teaching_online_safety_in_school.pdf
- Training or lessons are adapted as necessary in response to any incidents or inclusion of new media.
- All users understand that they must take responsibility for their network use.

Children will be taught about online safety as part of the curriculum:

In Key Stage 1, children 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.

Children in Key Stage 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.

By the end of primary school, children will know:

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 online 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 is shared and used online

How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

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

6. Educating parents about Online safety

The school will raise parents' awareness 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 will also be covered during parents' evenings.

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

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

7. Cyber-Bullying

It is important to remember that bullying is not a specific criminal act in the UK, where some types of harassing or threatening behaviour or communications could be a criminal offence. There are a number of acts, such as the Malicious Communications Act 1988, the Communications Act 2003, Protection from Harassment Act 1997 and the Public Order Act 1986. If the school feels that an offense has been committed, assistance will be sought from the Police.

Definition:
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 one person or group by another person or group, where the relationship involves an imbalance of power. (See also the Behaviour & Fundamental Values policy.)

The majority of adults and young people find using the internet and mobile technology a positive and creative part of everyday life. Sadly, such technologies can also be used in a very negative way. Young people who are the target of bullying via mobile phones, gaming, social media, apps and chat rooms can often feel isolated and alone. Therefore, it is pivotal that children, staff, parents and carers understand how destructive cyberbullying can be, and how it differs from other forms of bullying. Therefore, the school actively uses assembly, and other Online Safety sessions to promote a culture of confident users who support online safety. The school also sends information/leaflets on cyber-bullying to parents so that they are

aware of the signs, how to report it and how they can support children who may be affected.

Cyber bullying may take place outside of the school gates, but will often be reported in school. If this occurs, it must be acted upon. The DFE guidance on 'Preventing & Tackling Bullying' 2017, states that teachers have the power to discipline children for misbehaving outside school premises: 'If an incident of bullying outside the school premises or online is reported to the school, it is important that it is investigated and appropriate action is taken. This will send a strong signal to children that bullying will not be tolerated and perpetrators will be held to account.'. Furthermore, The Education Act 2011 gives wider search powers to tackle cyberbullying by providing a specific power to search for, and if necessary, delete inappropriate images or files on electronic devices.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school Behaviour and Fundemental Values policy. Where illegal, inappropriate or harmful material has been spread among children, the school will use all reasonable endeavors to ensure the incident is contained.

Preston HedgesTrust does not tolerate any form of bullying, including cyber bullying. Incidents of cyber bullying must be recorded and investigated. Any evidence found must be kept. The school will take any number of steps to identify the bully: parents and carers will be informed; monitoring undertaken to provide evidence, where necessary; and the Police contacted if there is a suspicion of a criminal offence.

8. School staff being targeted over the Internet

All school stakeholders have rights and responsibilities in relation to cyberbullying. Staff have the right to work free from harassment and bullying towards them that is carried out over the internet. Parents have the right to raise concerns about the education of their child, but should do so in an appropriate manner. The school has a right to encourage parents who are misusing social media to use it in an appropriate manner (DFE guidance 2014).

Staff are expected, under the Acceptable Use Policy, to ensure that their security and privacy settings on social media are set appropriately. Staff must also be aware that comments and images on social media sites may be visible to friends of social media friends, who may also be friends of parents and children. Annual discussion of the Acceptable Use Policy embeds these reminders to all staff.

Staff posting inappropriate comments on social media could lead to disciplinary action and having their employment terminated. Social media friends tagging staff in inappropriate posts, photographs or videos may also lead to disciplinary action, therefore staff are responsible for ensuring that their professional reputation is being upheld at all times. Staff must not give out personal mobiles or emails addresses to parents, even for school trips.

If a member of staff is subject to cyberbullying, this must be reported to a senior leader. Staff are encouraged to keep evidence. If the perpetrator is a current pupil, the school will follow the appropriate disciplinary procedures, as related in the Behaviour Policy. If a member of staff is involved in cyber bullying of another member of staff, then staff disciplinary procedures will be followed. If a parent is involved in cyberbullying of a member of staff, the Principal will invite the parent into school to discuss their concerns. Advice will be given of the appropriate way to air their complaints, and a request will be made to remove the information, If the parent or carer refuses, the Principal reserves the right to contact the appropriate County Council Online Safety Officer, and if the comments are abusive, sexual or a hate-crime, the Police.

9. Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on children' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or

- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of children will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

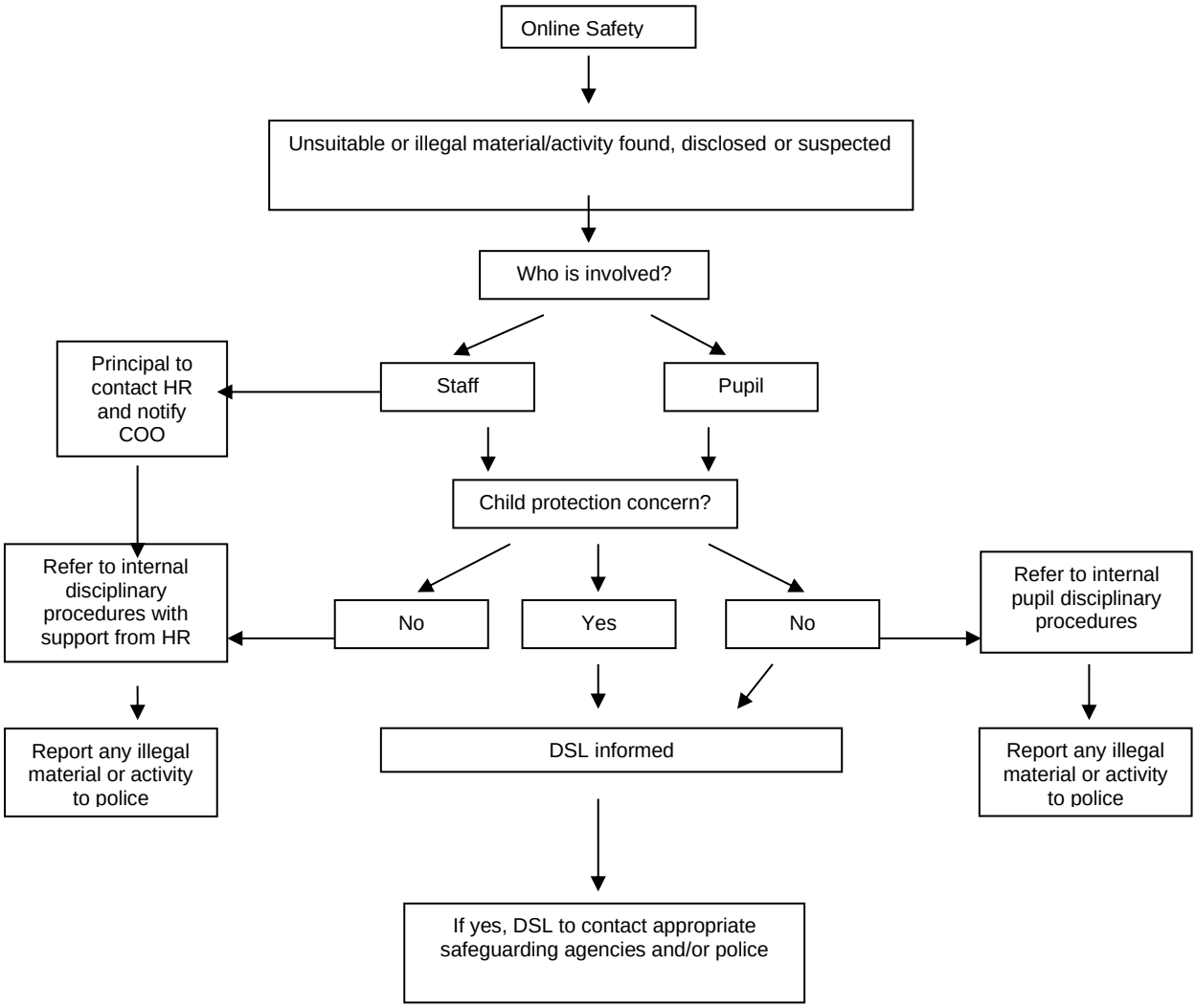
Any complaints about searching for or deleting inappropriate images or files on children' electronic devices will be dealt with through the Trust complaints procedure.

10. (Sexting) Youth produced imagery
Please see paragraph 24 of the Child Protection & Safeguarding Policy

11. Child on Child Abuse including Up skirting
Please see paragraph 25 of the Child Protection & Safeguarding Policy

12. Incident Reporting

In the event of misuse by staff or students, including the use of the school network in an illegal, unsuitable or abusive manner, a report must be made to the Principal / Safeguarding Officer immediately, and the Online Safety flowchart followed. If there is any suspicion that a website may contain child abuse images or any illegal activity, a report should be made to the Police immediately. In the event of minor or accidental misuse, internal investigation would be initiated and disciplinary procedures followed where appropriate. Please see overleaf:



In the event of minor or accidental misuse, internal investigations should be initiated and disciplinary procedures followed where appropriate. Additionally, all security breaches should be reported immediately to the Principal,Online Safety Lead and Chief Operating Officer

If there are concerns around on-line grooming, including images of child abuse, the Police must be contacted immediately.

Other circumstances when Online Safety concerns should be reported to the designated safeguarding officer and discussed with the Police are::

- Radicalisation – Further information and support can be gained from the website

- http://www.northamptonshirescb.org.uk/about-northamptonshire-safeguarding-children-partnership/news/violent-extremism-and-radicalisation/ and the contact email below prevent@northants.pnn.police.uk
- Prevent | Milton Keynes City Council (milton-keynes.gov.uk)
- Hacking
- Hate crimes
- Harassment
- Certain types of adult material
- Criminal conduct, activity or materials

All incidents must be recorded on the Online Safety Incident Log to allow for monitoring and auditing. Online Safety incidents may have an impact on children, staff and the wider community both on and off site. These can have legal and disciplinary consequences. Other situations could potentially be very serious and a range of sanctions may be required, which is linked to the school disciplinary policy and child protection policy.

13. Training

All new staff members will receive safeguarding training as part of their induction, which includes online safety 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).

The Safeguarding Team 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.

Trustees 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.

14. Monitoring

Users are reminded that Internet activity may be monitored at any time without prior notice. This is in order to ensure, as much as possible, that users are not exposed to illegal or inappropriate websites, and to ensure, as much as possible, that users do not actively seek access to illegal or inappropriate websites. Users are made aware of this is the Acceptable Use Policy. All monitoring activities comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Leaders log behaviour and safeguarding issues related to online safety. An incident report log can be found in the appendices.

This policy will be reviewed annually.

15. Prevent Duty

Please refer to Safeguarding & Child Protection Policy paragraph 15.

16. Safeguards for online activity

Preston Hedges Trust uses a range of devices including PC's, laptops, tablets. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

In School Monitoring Software

Securus software – a software system that enables leaders to monitor in school online activity, and receive alerts if safeguarding keywords are searched. This enables the safeguarding and leadership team to detect and provide early intervention where necessary.

Internet Filtering

(For Preston Hedges; Pineham Barns; Parklands Primary & Holne Chase): Broadband Provider –EXA Education SurfProtect Quantum (For Buckton Fields) Smoothwall Guardian:

Both systems perfors advanced content network-level filtering, ensuring all online activity is appropriately filtered.

The Principal is ultimately responsible for ensuring all reasonable precautions are met in order to protect young users from inappropriate or harmful content. To this end, the school has the following filtering measures in place:

- Filtering levels are managed in school via an administrations tool provided by our broadband supplier. Only the IT technician is authorised to allow access or block access to a site. These filters are age-appropriate.All users have unique usernames which ensures that they only have access to the appropriate level of filtering.
- Any changes to filtering levels are documented on the Filter Change Request Log – with reasons for changes requested and the name of the member of staff. Consent from the Chief Operating Officer, Principal or Online Safety Lead must be received before the request can be actioned.

Firewall –Draytek Vigor 2860 Router

Preston Hedges; Pineham Barns; Parklands Primary & Holne Chase each have their own Draytek Vigor 2860 Router which provide gateway to EXA cloud Firewall. The firewall protects against attacks including DoS (Denial of Service) attacks, IP-based attacks and access by unauthorised remote systems. For Buckton Fields, Smoothwall Guardian provides the same service.

The content control enables schools to set restrictions on web site access, blocking download of certain file or data types, blocking specific web sites with whitelists or blacklists, blocking IM/P2P applications or other potentially harmful or wasteful content. Restrictions can be per user, per PC or universal.

The Principal is ultimately responsible for ensuring all reasonable precautions are met in order to protect young users from inappropriate or harmful content. To this end, the school has the following filtering measures in place:

- Filtering levels are managed in school via an administrations tool provided by our broadband supplier. Only the IT technician is authorised to allow access or block access to a site. These filters are age-appropriate.
- All users have unique usernames which ensures that they only have access to the appropriate level of filtering.
- Any changes to filtering levels are documented on the Filter Change Request Log – with reasons for changes requested and the name of the member of staff. Consent from the Chief Operating Officer, Principal or Online Safety Lead must be received before the request can be actioned.

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of

Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Thousands of inappropriate websites are created each day, and staff and children are trained on the protocols to follow if an inappropriate website is found, and children are supervised during internet sessions. Neither the school nor the schools' Internet filter provider can accept liability for the material accessed, or any consequences of Internet access. An internet log is kept of inappropriate websites, and a report made to the appropriate agencies.

In addition to above, the following safeguards are also in place:

- Anti-Virus – All capable devices will have anti-virus software. This software is updated on a regular basis.
- All USB peripherals such as keydrives are to be scanned for viruses before use.
- Email Filtering – we use software that prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.
- Supervision – Children are supervised when using the internet and acceptable use policy is adhered to. An incident log will report breaches of filtering, and will be reported to the appropriate agencies
- Passwords – all staff and students will be unable to access any device without a unique username and password. The iTunes account for the Ipads is password protected and only accessible by the IT support.
- Staff – should pre-view any websites for suitability before use, including those recommended to children for homework support
- Personal Data – No personal data (as defined by the Data Protection Act 1998) is to leave the school; all devices that contain personal data are kept on school property and are password protected. Any breach is to be brought to the attention of the Principal /immediately. The Principal / will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office

17. Safe use of school and personal ICT equipment

childrenchildrenchildrenParents & Carers

- It is the responsibility of parents and carers to ensure that they are using their phone appropriately on the school site. During class assemblies and performances, parents will be alerted when they are able to use the phones to record and photograph their own child. Parents are given clear

communication during these school events that they must not share images of video of other children on social media sites

Visitors / contractors

- Visitors and contractors to the site for business related purposes must not utilise their phone to take images of children, unless the correct approvals have been obtained

Internet

- Use of the Internet in school is a privilege, not a right. All staff must sign the staff Acceptable Use Policy
- Children and parents will all receive a copy of the Student Acceptable Use Policy, and understand that unacceptable use may mean withdrawal of Internet privileges.

18. Published content and media

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or children' personal information will not be published.
- The Principal will take overall editorial responsibility and ensure that content is accurate and appropriate, with support from the Trust Marketing and Communications Leader
- The security of staff and children is paramount. The Principal takes responsibility for ensuring that children are protected and full names of children are not published alongside photos. Parents give consent via Arbor for images of their children to be used on the school website or social media
- School leaders promote the privacy of children on school events such as sports days and class assemblies.
- Parents annually from September 2023 will have the option of opting out of their child been used in all published content.

Photos and videos

- Digital media, such as photos and videos, are used by the school for core business use only.

Social Networking

- At this point in time each school chooses Twitter, Facebook or Instagram as a broadcast and marketing service, therefore dialogue between school and parents does not occur.

Incidents

- Any Online Safety incident is to be brought to the immediate attention of the Online Safety Lead, or in his/her absence the Principal the Online Safety Lead will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

Parents

- The Online Safety policy and any other parental Online Safety information are available on the school website
- Parents are encouraged to read the school acceptable use policy

19. Emerging technologies

Online Safety is an ever growing area and is always developing as things are constantly changing. The school will take all reasonable precautions to identify and minimise risk from emerging technologies:

- Emerging technologies will be examined for risk and an educational assessment carried out before school use.
- Children are regularly instructed and reminded on the safe and appropriate use of technology and personal devices on and off site in accordance with acceptable use policies.

20. Information & Support websites

These websites are available for staff to utilise for further information on keeping children safe online:

www.thinkuknow.co.uk
www.disrespectnobody.co.uk
www.saferinternet.org.uk
www.internetmatters.org
www.pshe-association.org.uk
www.educateagainsthate.com
https://www.gov.uk/government/publications/teaching-online-safety-in-schools
https://www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

Appendix 1
Preston Hedges Trust
Filtering Change Log

Website/Category	Date	Requested by	Reason for change	Authorised by	Date for Review

Twitter Appendix to Online Safety Policy – March 2023

Preston Hedges Trust intends to use Twitter to inform parents of events as a 'broadcast service'.

A broadcast service is a one-way communication method in order to share school information with the wider school community. No persons will be "followed" or "friended" on these services and as such no two-way, private communication will take place.

No full names, or other details, of children will be 'tweeted', and parents will sign a disclosure form in order to allow photos of their child to be uploaded. The Principal / or a delegated senior member of staff will regularly check images for unauthorised pupil pictures.

Staff will not use personal Twitter accounts to follow any of the schools within the Trust, comment on the school broadcast, or engage in two way dialogue with children or parents using Twitter.

Twitter has been risk-assessed by the Online Safety Lead, and has been determined as a low risk when used as a broadcast service.

Facebook Appendix to Online Safety Policy – March 2023

Trust and school Facebook accounts are intended to be used to market the school (for engaging with potential new children and to share events) and recruit staff.

This is intended to be a one-way communication method. No persons will be "followed" or "friended" on these services and as such no two-way, private communication will take place.

The Principal / or a delegated senior member of staff or office, will be the only adults allowed to upload information or recruitment advertisements to Facebook. Only prior agreed marketing images of children will be used, with parents having signed a disclosure form in order to allow photos of their child to be used in this way.

Facebook has been risk-assessed by the Online Safety Lead, and has been determined as a low risk when used for these purposes.

Instagram Appendix to Online Safety Policy – March 2023

To promote the marketing of the schools in our Trust on social media, Instagram can be used to reach a wider audience. Instagram can be used to market the school to potential families, share events and recruitment vacancies. This will be a one-way communication tool and the Instagram page will not be used to follow other people, or private message. The engagement will be solely to promote the school effectively on social media.

The Principal / or a delegated senior member of staff or office will be the only adults allowed to upload images and information on Instagram. For images of children to be used on Instagram, parents must have signed consent that they are happy for their child's photo to be shared on this platform.

Following completion of a risk assessment, Instagram has been determined as low risk when used for the above purposes.

Seesaw - Remote Learning Appendix to Online Safety Policy – March 2023

In response to Covid-19, it is an expectation that all learning can be accessed remotely. The following software are utilised by some or all schools in the Trust.

Seesaw

Seesaw is a program that enables children to download work, upload responses and engage in dialogue with teachers.

Children and staff have all been trained on how to use this. To ensure that children remain only able to communicate safely with their teacher, the ability for children to comment on each other's work is disabled on the child's account. Each child is giving their own QR code to enable access to only their account. Furthermore, it does not provide 'live feed' video calling, so it is not possible for a situation to occur where a non-school member can gain access and have a real time conversation with children. It therefore has been risk assessed as a low risk.

If an event arises where a child has used the comments section inappropriately, the school's response will follow the Behavior and Fundamental Values Policy processes. If an event arises where a member of staff has used the comments

section inappropriately, the school's response will follow staff disciplinary procedures.

Zoom – Remote Learning Appendix to Online Safety Policy – March 2023

To enable children to take part in real-time learning when they are isolating, some of the schools use Zoom as a virtual learning space. This enables the children to take part in the lesson that is happening on the school site and continue their education.

When Zoom is used, access to the virtual meeting room is password protected, and only children who have access to this password are able to be admitted. Teachers hold a 'waiting room' so that they can ensure that they only let appropriate people gain admittance.

As with all remote learning, schools expectations are that those interacting virtually follow the Behaviour and Fundamental Values Policy. If any incident occurs that breaches this, or the staff code of conduct, the school's response will follow the steps outlined in those policies.

PRESTON HEDGES TRUST

FUN
CREATIVITY
ACHIEVEMENT

ICT Risk Assessment Log

The school uses ICT auditing to establish if the Online Safety policy is adequate and the implementation is appropriate.

DISCLAIMER: The school will take all reasonable precaution to ensure that users access only appropriate material. However, due to the internet and social media being so vast, it is not possible to guarantee that access to undesirable material will never occur. The school cannot accept liability for the material accessed, or any consequence resulting from the internet use. Risk is shown from 1 (low) to 5 (High) on the basis of the likelihood of this happening and the impact it would have. These are then multiplied to give a risk score.

Score	Risk Description	Action Requirements
15 - 20	High Risk	Risk will be actively managed with control measures
6 - 12	Medium Risk	Take appropriate action to reduce risk if possible
5 and below	Low Risk	Risk to be removed from the risk register, activity monitored incase of escalation

No.	Activity	Risk	Likelihood	Impact	Risk	Owner
1.	Internet browsing	Access to inappropriate/illegal content – staff	2	5	10	Online Safety Lead IT Support Safeguarding Team

2.	Facebook	Inappropriate comments made by parents. This is a higher risk as comments on business pages cannot be disabled. However such comments can be deleted,. Furthermore adding the list of blocked words (see final appendix) will block almost all possible comments available.	3	3	9	Principal
3.	Internet browsing	Access to inappropriate/illegal content – students	2	3	8	Online Safety Lead IT Support Safeguarding Team
4.	Twitter	Photos of children in public view without parental approval – this is a low risk as parents will sign a disclosure form and all uploads will be approved by PW or designated senior member of staff	2	3	6	Principal
5.	Twitter	Data Protection rights infringed – low risk as no full names of children or other details will be used online. Designated senior member of staff to upload any tweets.	2	3	6	Principal
6.	Facebook	Photos of children in public view without parental approval – this is a low risk as parents will sign a disclosure form and all uploads will be approved by PW or designated senior member of staff	2	3	6	Principal

PRESTON HEDGES TRUST

FUN
CREATIVITY
ACHIEVEMENT

List of words to block comments on Facebook:

a, able, about, above, across, act, action, actually, add, addition, adjective, afraid, Africa, after, again, against, age, ago, agreed, ahead, air, all, allow, almost, alone, along, already, also, although, always, am, America, among, amount, an, and, angle, animal, another, answer, any, anything, appear, apple, are, area, arms, army, around, arrived, art, as, ask, at, away, baby, back, bad, ball, bank, base, be, bear, beat, beautiful, became, because, become, bed, been, before, began, begin, behind, being, believe, bell, belong, below, beside, best, better, between, big, bill, birds, bit, black, block, blood, blow, blue, board, boat, body, bones, book, born, both, bottom, bought, box, boy, branches, break, bright, bring, British, broken, brother, brought, brown, build, building, built, burning, business, but, buy, by, call, came, can, can't, cannot, capital, captain, car, care, carefully, carry, case, cat, catch, cattle, caught, cause, cells, center, cents, century, certain, chance, change, chart, check, chief, child, children, choose, church, circle, city, class, clean, clear, climbed, close, clothes, cloud, coast, cold, color, column, come, common, company, compare, complete, compound, conditions, consider, consonant, contain, continued, control, cook, cool, copy, corn, corner, correct, cost, cotton, could, couldn't, count, country, course, covered, cows, create, cried, crops, cross, crowd, current, cut, dance, dark, day, dead, deal, death, decided, decimal, deep, describe, desert, design, details, determine, developed, dictionary, did, didn't, died, difference, different, difficult, direct, direction, discovered, distance, divided, division, do, doctor, does, doesn't, dog, dollars, don't, done, door, down, draw, drawing, dress, drive, drop, dry, during, each, early, ears, earth, east, easy, eat, edge, effect, eggs, eight, either, electric, elements, else, end, energy, engine, England, English, enjoy, enough, entered, entire, equal, equation, especially, Europe, even, evening, ever, every, everyone, everything, exactly, example, except, exciting, exercise, expect, experience, experiment, explain, express, eye, face, fact, factories, factors, fair, fall, family, famous, far, farm, farmers, fast, father, fear, feel, feeling, feet, fell, felt, few, field, fig, fight, figure, filled, finally, find, fine, fingers, finished, fire, first, fish, fit, five, flat, floor, flow, flowers, fly, follow, food, foot, for, force, forest, form, forward, found, four, fraction, France, free, French, fresh, friends, from, front, fruit, full, fun, game, garden, gas, gave, general, get, girl, give, glass, go, God, gold, gone, good, got, government, grass, great, Greek, green, grew, ground, group, grow, guess, gun, had, hair, halt, hand, happened, happy, hard, has, hat, have, he, head, hear, heard, heart, heat, heavy, held, help, her, here, high, hill, him, himself, his, history, hit, hold, hole, home, hope, horse, hot, hours, house, how, however, huge, human, hundred, hunting, I, I'll, ice, idea, if, important, in, inches, include, increase, Indian, indicate, industry, information, insects, inside, instead, instruments, interest, interesting, into, iron, is, island, isn't, it, it's, its, itself, Japanese, job, joined, jumped, just, keep, kept, key, killed, kind, king, knew, know,

known, lady, lake, land, language, large, last, later, laughed, law, lay, lead, learn, least, leave, led, left, legs, length, less, let, let's, letter, level, lie, life, lifted, light, like, line, list, listen, little, live, located, long, look, lost, lot, loud, love, low, machine, made, main, major, make, man, many, map, march, mark, match, material, matter, may, maybe, me, mean, measure, meat, meet, melody, members, men, metal, method, middle, might, mile, milk, million, mind, mine, minutes, miss, modern, molecules, moment, money, months, moon, more, morning, most, mother, mountain, mouth, move, movement, much, music, must, my, name, nation, natural, near, necessary, need, never, new, next, night, no, nor, north, northern, nose, not, note, nothing, notice, noun, now, number, numeral, object, observe, ocean, of, off, office, often, oh, oil, old, on, once, one, only, open, opposite, or, order, other, our, out, outside, over, own, oxygen, page, paint, pair, paper, paragraph, park, part, particular, party, passed, past, pattern, pay, people, per, perhaps, period, person, phrase, picked, picture, piece, place, plains, plan, plane, planets, plant, play, please, plural, poem, point, pole, poor, position, possible, pounds, power, practice, prepared, present, president, pretty, printed, probably, problem, process, produce, products, property, provide, pulled, pushed, put, question, quickly, quiet, quite, race, radio, rain, raised, ran, rather, reached, read, ready, really, reason, received, record, red, region, remain, remember, repeated, report, represent, rest, result, return, rhythm, rich, ride, right, ring, rise, river, road, rock, rolled, room, root, rope, rose, round, row, rule, run, safe, said, sail, same, sand, sat, save, saw, say, scale, school, science, scientists, score, sea, seat, second, section, see, seeds, seem, seen, sell, send, sense, sent, sentence, separate, serve, set, settled, seven, several, shall, shape, sharp, she, ship, shoes, shop, short, should, shoulder, shouted, show, shown, side, sight, sign, silent, similar, simple, since, sing, single, sir, sister, sit, six, size, skin, sky, sleep, slowly, small, smell, smiled, snow, so, soft, soil, soldiers, solution, solve, some, someone, something, sometimes, son, song, soon, sound, south, southern, space, speak, special, speed, spell, spot, spread, spring, square, stand, stars, start, state, statement, stay, steel, step, stick, still, stone, stood, stop, store, story, straight, strange, stream, street, stretched, string, strong, students, study, subject, substances, such, suddenly, suffix, sugar, suggested, sum, summer, sun, supply, suppose, sure, surface, surprise, swim, syllables, symbols, system, table, tail, take, talk, tall, teacher, team, tell, temperature, ten, terms, test, than, that, the, their, them, themselves, then, there, these, they, thick, thin, thing, think, third, this, those, though, thought, thousands, three, through, thus, tied, time, tiny, to, today, together, told, tone, too, took, tools, top, total, touch, toward, town, track, trade, train, travel, tree, triangle, trip, trouble, true, truck, try, tube, turn, two, type, uncle, under, underline, understand, unit, until, up, upon, us, use, usually, valley, value, various, verb, very, view, village, visit, voice, vowel, wait, walk, wall, want, war, warm, was, wash, Washington, wasn't, watch, water, waves, way, we, we'll, wear, weather,

week, weight, well, went, were, west, western, what, wheels, when, where, whether, which, while, white, who, whole, whose, why, wide, wife, wild, will, win, wind, window, wings, winter, wire, wish, with, within, without, woman, women, won't, wonder, wood, word, work, workers, world, would, wouldn't, write, written, wrong, wrote, yard, year, yellow, yes, yet, you, you're, young, your, yourself,