ONLINE SAFETY POLICY
(INC. CYBERBULLYING)

This section should be completed following ratification of the Policy.

	Name	Signature	Date
Chair of Sub-Committee's Approval	Esther Stephenson		July 2018
Chief Executive Officers Approval	Paul Watson		July 2018
Chair of Trust's Approval	Becky Hickford		
Recommended Review Date:	Annually – July 2019		

Ownership
Preston Hedge's Primary School is responsible for the production and maintenance of this document. It is issued by the Clerk,claire.clayson@prestonhedges.northants.co.uk to whom any change requests or queries should be directed.

Version Control
This document is issued and maintained in accordance with Preston Hedge's Primary School procedures. Any change to the document will increase its version number. It is the responsibility of the reader to check with the Clerk that this is a currently valid copy.

Version	Date	Description of Change	Changed By
1	Sept 2011	Adoption of NCC Policy	n/a
2	May 2013	Complete update using NCC website guidelines	T Coles
3	May 2014	No changes	P Watson
4	May 2015	Update & contents page for accessibility	T Coles
5	May 2016	Prevent Duty & support websites added	T Coles
Now SWB 5 V1	July 2017	Updates of titles	C Stewart
V2	Sept 2017	Updates regarding Youth Produced Imagery	T Coles
V3	July 2018	Terminology update	T Coles

References/Related Documents

Doc. No.	Title
SWB-001	Safeguarding Policy
SWB 12	Anti-bullying Policy

File Name/Path S: Data/Admin/Governors/1-Governorsrevised/4-Safeguarding&Wellbeing/Policies

Contents

Writing and reviewing the Online Safety Policy

- The Online Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and for child protection.
- Our Online Safety Policy has been written by the Trust, building on the Northamptonshire Online Safety Policy and government guidance. It has been agreed by senior management and approved by governors in our schools.

Policy Statement

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

Users - refers to staff, governing body, 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 site, e.g. visits, conferences, school trips etc.

Wider school community – students, all staff, governing body, parents

ICT 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 TC, 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 to 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 Trusts Safeguarding Policy, with any Online Safety concerns noted to be immediately shared with the Lead Safeguarding Officer 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 pupils and staff, but brought onto school premises (such as mobile phones or other mobile devices).

The aim of this policy is:

- 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.

<u>The scope of this policy</u>:

This policy applies to all staff, pupils, governors, 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.

<u>Responsibilities</u>

Trust SWB Committee

The Trust SWB 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.

Local Governing Bodies

Local Governing Bodies have a responsibility for checking Online Safety in line with with the document: Keeping Children Safe in Education 2018.

Headteacher / Principal

Reporting to the governing body, the Headteacher /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 Officer (or more than one), as indicated below.

The Headteacher/ Principal will ensure that:

- 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 governing body, parents.
- The designated Online Safety Officer(s) has had appropriate CPD in order to undertake the day to day duties.
- All Online Safety incidents are dealt with promptly and appropriately.

Lead Designated Child Protection Officer

- Remain updated with relevant safeguarding needs regarding Online Safety
- Alert and advise the Head and Online Safety Officer 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 Officer

The Online Safety Officer 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 Headteacher/ Principal.
- Advise the Headteacher / Principal, governing body 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 Headteacher /Principal and responsible governor to decide on what reports may be appropriate for viewing.

ICT Technical Support Staff

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
    - 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; that categories of use are discussed and agreed with the Online Safety officer and Headteacher/ Principal.
  - That any problems or faults related to filtering are reported to the Safeguarding Officer and the broadband provider immediately, and recorded on the Online Safety Log.
  - The Online Safety Incident Log is monitored and incidents are reported to the Online Safety Officer(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 Officer and the Head / 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 Headteacher / Principal.
- Any Online Safety incident is reported to the Online Safety Officer (and an Online Safety Incident report is made), or in his/her absence to the Headteacher / Principal. If you are unsure the matter is to be raised with the Online Safety Officer or the Headteacher / 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 pupils 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.

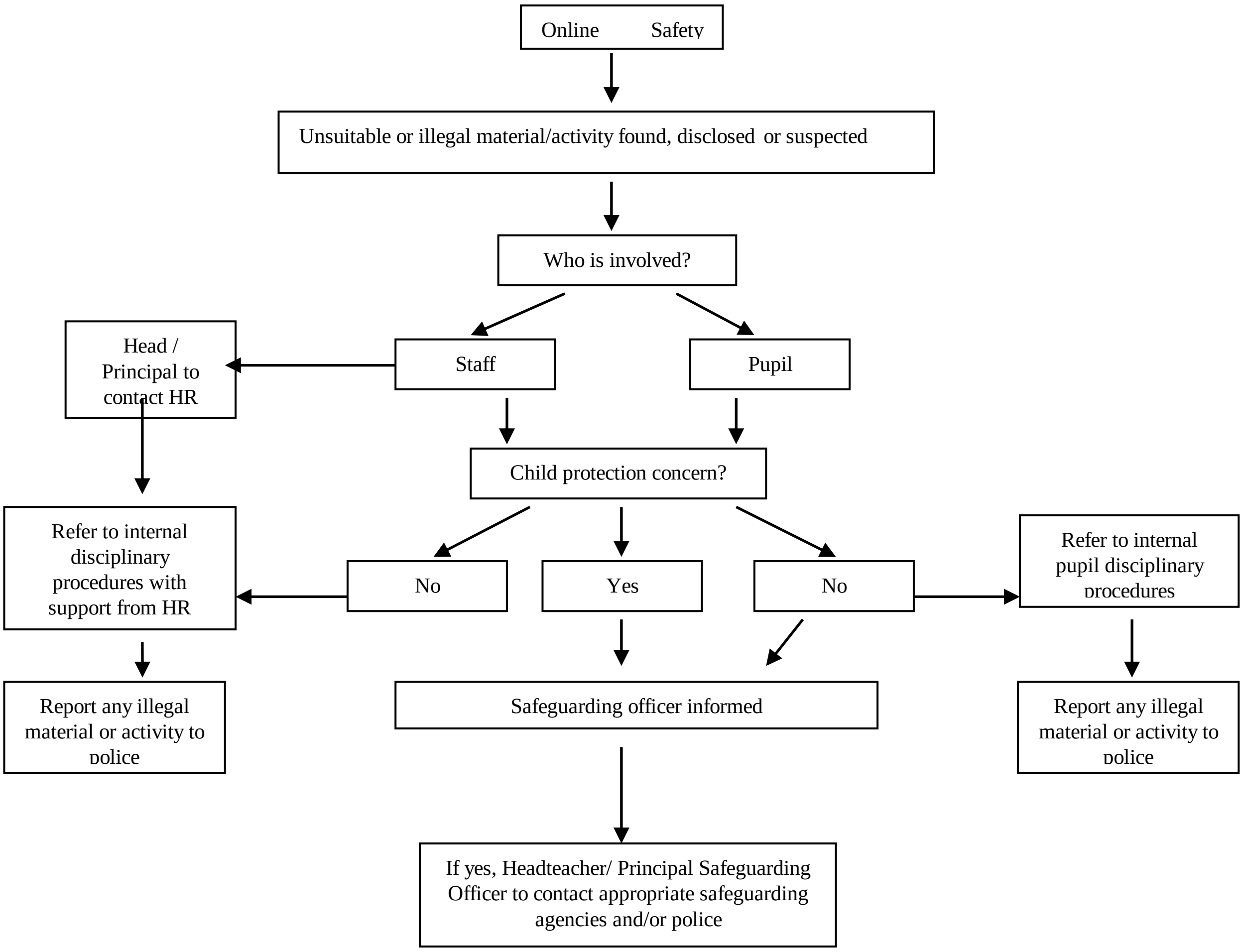
Online Safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly all students will be fully aware how they can report areas of concern whilst at school or outside of school.

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

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 Head/ 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.



Online Safety
Unsuitable or illegal material/activity found, disclosed or suspected
Who is involved?
Staff
Pupil
Head / Principal to contact HR
Child protection concern?
No
Yes
No
Refer to internal disciplinary procedures with support from HR
Refer to internal pupil disciplinary procedures
Report any illegal material or activity to police
Safeguarding officer informed
Report any illegal material or activity to police
If yes, Headteacher/ Principal Safeguarding Officer to contact appropriate safeguarding agencies and/or police

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 Head / Principal and Online Safety Officers.
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 contact jason.farmer@northants.pnn.police.uk and **lscbn**orthamptonshire.org.uk/schools/violent...**radicalisation**
- 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 pupils, 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.

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.

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.

Cyberbullying is best defined "The use of Information and Communications Technology, particularly mobile phones and the Internet, deliberately to upset someone else". (DCSF 2009)

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 pupils, staff, parents and carers understand how destructive cyberbullying can be, and how it differs from other forms of bullying. Therefore, the school uses assembly, and other Online Safety sessions to promote a culture of confident users who support online safety.

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' 2014, states that teachers have the power to discipline pupils for misbehaving outside school premises 'to such extent as is reasonable'. 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.

Preston Hedge's Academy Trust 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.

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 pupils. 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 Head / 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 Head / Principal reserves the right to contact the Northamptonshire County Council Online Safety Officer, and if the comments are abusive, sexual or a hate-crime, the Police.

<u>Youth Produced Imagery (Sexting) including Peer on Peer Abuse and Sexual Harrassment Online</u>

<u>The Law</u>

Making, possessing and distributing any imagery of someone under 18 which is 'indecent' is illegal. This includes imagery of yourself if you are under 18. The relevant legislation is contained in the Protection of Children Act 1978 (England and Wales) as amended in the Sexual Offences Act 2003 (England and Wales). Specifically: • It is an offence to possess, distribute, show and make indecent images of children. • The Sexual Offences Act 2003 (England and Wales) defines a child, for the purposes of indecent images, as anyone under the age of 18. (UKCCIS)

In the event of an Online Safety disclosure being made with regard to youth produced imagery, staff will alert the DSL who will follow the guidelines detailed on the Safeguarding Children Policy (SWB-001).
Any device (pupil or staff) considered as evidence for the Police will be confiscated immediately, turned off and locked away until the Police are able to retrieve it.

Adults should not view youth produced sexual imagery unless there is good and clear reason to do so. Wherever possible responses to incidents should be based on what DSLs have been told about the content of the imagery.

We recognise that peer on peer abuse can happen and we would deal with issues in line with child protection actions if a child came to harm (additionally, use associated guidance and policies). This can also be gender specific issues – for example, girls being sexually touched or boys being subject to an initiation/ violence.

Our school insists on high standards of behaviour and appropriate uses of technology, and staff are vigilant in the monitoring of this.

Any pupil or staff member who are aware of, or have received any online communication will be supported appropriately, following the procedures laid out in this and linked policies of Safeguarding Children and Anti-Bullying.

The Curriculum & Online Safety

Using the internet is part of the curriculum and is a fantastic and necessary tool. Its use raises educational standards, and allows pupils 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 Hedge's Academy 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 ICT scheme of work incorporates lessons on Online Safety. For KS1 children these lessons involve age-appropriate guidance, advice and discussion from the teacher; KS2 children, work through the online safeguarding units from both SWGFL and the CEOP website as appropriate (www.thinkuknow.co.uk).
- Pupils are made aware of copyright issues, data protection, intellectual property and reliability of information sourced on the internet as part of the curriculum.
- Pupils have opportunities for informal discussions about on-line risks and strategies for protecting yourself as part of the Online Safety curriculum.
- The academies 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, 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 proflific use of photo-editing and wellbeing; dangers of chatrooms and online gaming; and mental health and resilience to what is being seen or heard online including negative comparison to perfection**

seen in apps and social media. 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.

- 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.

Technology

Preston Hedge’s Academy 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:

Internet Filtering – Broadband Provider –EXA Education

EXA education work with leading firewall provider Fortinet to supply the industry’s best protection against the most advanced security threats and targeted attacks. Delivering end-to-end network security, a Fortinet firewall ensures that schools receive complete and comprehensive protection in one centrally managed device, ensuring that the school’s infrastructure and network is as safe and secure as is reasonably possible. SurfProtect Quantum performs network-level filtering, ensuring all online activity is appropriately filtered.

The Headteacher / 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 Head / Principal or Online Safety Officer must be received before the request can be actioned.

Prevent Duty

Preventing Radicalisation KCSIE Section 26 of the Counter-Terrorism and Security Act 2015 places a duty on ‘schools’ in the exercise of their functions, to have “due regard to the need to prevent people from being drawn into terrorism”.

Preventing radicalisation
Children are vulnerable to extremist ideology and radicalisation. Extremism101 is the vocal or active opposition to our fundamental values, including therule of law, individual liberty and the mutual respect and tolerance of different faiths and beliefs. This also includes calling for the death of members of the armed forces.

Radicalisation refers to the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. There is no single way of identifying whether a child is likely to be susceptible to an extremist ideology. Background factors combined with specific influences such as family and friends may contribute to a child’s vulnerability. Similarly, radicalisation can occur through many different methods (such as social media) and settings (such as the internet). However, it is possible to protect vulnerable people from extremist ideology and intervene to prevent those at risk of radicalisation being radicalised. As with other safeguarding risks, staff should be alert to changes in children's behaviour which could indicate that they may be in need of help or protection. Staff should use their judgement in identifying children who might be at risk of radicalisation and act proportionately which may include the designated safeguarding lead (or deputy) making a referral to the Channel programme. KCSIE 2018

In our schools, we are aware of the risks posed by the internet and have appropriate online safety procedures in place. Additionally, we ensure the promotion of Modern British Values and have Citizenship and PSHE themes within the curriculum that would give the opportunity to recognise extreme views and teach children in a way to allow them not to be radicalised as easily.

EXA Education use SurfProtect Quantum to ensure that the school fully adheres to the Prevent duty. The software uses a Prevent setting to automatically block all sites that could contain radical content. This includes the categories: Weapons, Violence, Intolerance & Hate, and Criminal Activity. The Prevent setting will also enforce a block on search terms relating to extremism; this keyword list includes all terms identified by the DfE as being commonly used in ISIL dialogue and propaganda.

Furthermore, Exa Education is a member of the Internet Watch Foundation. The IWF was established in 1996 to provide the UK internet Hotline for child sexual abuse content to be reported in a secure and confidential way. The IWF publishes a list of websites that contain indecent images, advertisements for, or links to such content. This list is automatically incorporated behind the scenes into SurfProtect Quantum twice daily to ensure that these websites are instantly blocked to users.

Any concerns that the school has regarding the Prevent Duty will be passed to the Designated Lead Child Protection Officer.
Concerns can also be raised by email to: Counter.extremism@education.gsi.gov.uk

Safeguards for online activity

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 pupils are trained on the protocols to follow if an inappropriate website is found, and pupils are supervised during internet sessions. Neither the school nor Talkstraight (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** – Pupils 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 pupils 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 Headteacher / Principal immediately. The Headteacher / Principal will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office. USB Sticks for sensitive data are to be encrypted.

Safe use of school and personal ICT equipment

- A log of ICT equipment is kept by the School Site Manager.
- Personal or sensitive data is not stored on school devices that can be removed from site.

Mobile phones -

Pupil Use :

- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden, and will be dealt with as part of our Cyber-bullying policy
- All mobile devices are brought to school at the child's own risk, and the school is not liable for loss or breakages.
- Mobile phones that are used inappropriately can be confiscated by teachers and returned to pupils at the end of the day.

Staff Use:

- It is the responsibility of the staff member to ensure that there is no illegal or inappropriate content stored on their device when brought onto school grounds.
- Personal mobile phones should not be used to contact children or families; nor should they be used to take videos or photos of pupils. School issued devices **only** should be used in these situations.

Internet

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

Email

- The school gives all staff their own e-mail account to use for school business to protect staff. All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted.
- At this point in time (May 2015), students do not use the school email system.

Published content and the school web site –

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Head Teacher / Principal will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The security of staff an pupils is paramount. The Head Teacher / Principal takes responsibility for ensuring that pupils are protected and full names of pupils are not

published alongside photos. Parents give written consent for images of their children to be used on the school website or Twitter,

- School leaders promote the privacy of pupils on school events such as sports days and class assemblies.

Photos and videos

- Digital media, such as photos and videos, are used by the school for core business use only. Parents can opt out of this annually, if they choose to do so.

Social Networking

- At this point in time, the school does not engage in social networking. As this changes, the Online Safety policy will be updated and appropriate risk assessments will be created.

Incidents

- Any Online Safety incident is to be brought to the immediate attention of the Online Safety Officer, or in his/her absence the Headteacher / Principal. The Online Safety Officer 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

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.
- Pupils 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.

Information & Support websites

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

www.thinkuknow,co.uk
www.disrespectnobody,co.uk
www.saferinternet.org,uk
www.internetmatters.org
www.pshe-association.org.uk
educateagainsthate.com
www.gov.uk/government/publications/the-use-of-social-meida-for-online-radicalisation

Acceptable Use Policy – Staff

You must read this policy in conjunction with the Online Safety Policy. Once you have read and understood both, you must sign that you have read and agreed to the Acceptable Use Policy. This policy forms part of the terms and conditions set out in your contract of employment.

Internet access - You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an Online Safety incident, reported to the Online Safety officer and an incident sheet completed. Any incidents may result in disciplinary action and may need to be reported to the Police

Social networking – Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should not seek to become “friends” with parents or pupils on personal social networks. It is understood that there may be existing relationships of staff living on the estate, but these must be open & disclosed to the Head teacher / Principal and the Child Protection Officer.

Use of Email – staff are not permitted to use school email addresses for personal business. All email should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

Passwords - Staff should keep passwords private.

Data Protection – If it is necessary for you to take work home, or off site, you should ensure that no data concerning personal information is taken offsite. If it is necessary to take sensitive data off-site, permission should be gained from the Head teacher / Principal and the information must be encrypted (eg on a password protected memory stick).

Personal Use of School ICT - You are not permitted to use ICT equipment for personal use unless specific permission has been given from the Headteacher / Principal who will set the boundaries of personal use.

Images and Videos - You should not upload onto any internet site or service images or videos of other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings). The school must be supported in its approach to online safety and staff must not deliberately upload any images or videos that could upset a member of the school community

Professional Role –Staff should ensure that all online activity, inside and outside school, will not bring themselves, colleagues or the school into disrepute.

Use of Personal ICT - use of personal ICT equipment is at the discretion of the Headteacher / Principal. Permission must be sought stating the reason for using personal equipment; a risk assessment will be carried out by IT support and the Online Safety Officer.

Viruses and other malware - any virus outbreaks are to be reported to IT support as soon as it is practical to do so, along with the name of the virus (if known).

Online Safety – like health and safety, Online Safety is the responsibility of everyone to everyone. As such you will promote positive Online Safety messages in all use of ICT whether you are with other members of staff or with students.

Note – All users are reminded that Internet activity may be monitored 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.

ONLINE SAFETY / ACCEPTABLE USE POLICY

I have read and agree to adhere to the terms of the Acceptable Use Policy

Date	Name	Signature

Acceptable Use Policy
Our Charter of Online Behaviour

Note: All Internet and email activity is subject to monitoring

I will – only use the school ICT for schoolwork that the teacher has asked me to do.

I will – avoid looking for, or showing other people, things that may be upsetting.

I will – show respect for the work that other people have done.

I will – only use other people’s work or pictures if I have permission to do so.

I will – treat the ICT equipment carefully and respectfully; if I accidentally damage something I will tell my teacher.

I will – only use my username to log on.

I will – keep my personal information private and not share it online with anyone.

I will – not download anything from the Internet unless my teacher has asked me to.

I will – let my teacher know if anybody asks me for personal information.

I will – let my teacher know if anybody says or does anything to me that is hurtful or upsets me.

I will – be respectful to everybody online; I will treat everybody the way that I want to be treated.

I will – practise online safety at all times, and will inform an adult if I see or hear anything upsetting online.

I understand – that some people on the Internet are not who they say they are, and some people can be nasty. I will tell my teacher if I am ever concerned in school, or tell my parents if I am at home.

I understand – that these rules are important for my safety and that I will only be allowed Internet access if I follow these.

Preston Hedge's Academy Trust
Filtering Change Log

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

Preston Hedge's Academy Trust
Online Safety Incident Log

Date of Incident	Name of Individual (s) involved	Media Device & location	Detail of Incident	Actions	Actioned by/ Referred to

Twitter Appendix to Online Safety Policy – May 2018

Preston Hedge's Academy 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.

The Headteacher / Principal or a delegated senior member of staff, will be the only adults allowed to broadcast on behalf of the school. No full names, or other details, of pupils will be 'tweeted', and parents will sign a disclosure form in order to allow photos of their child to be uploaded. The Headteacher / Principal, or a delegated senior member of staff will check images for unauthorised pupil pictures prior to upload.

Staff will not use personal Twitter accounts to follow any of the academies within the Trust, comment on the school broadcast, or engage in two way dialogue with pupils or parents using Twitter.
Twitter has been risk-assessed by the Online Safety Officer, and has been determined as a low risk when used as a broadcast service.

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.

No.	Activity	Risk	Likelihood	Impact	Owner
1.	Internet browsing	Access to inappropriate/illegal content – staff	1	3	Online Safety Officer IT Support
2.	Internet browsing	Access to inappropriate/illegal content – students	2	3	
3.	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	1	3	Head teacher / Principal
4.	Twitter	Data Protection rights infringed – low risk as no full names of pupils or other details will be used online. Designated senior member of staff to upload any tweets.	1	3	Head teacher/ Principal

Likelihood: How likely is it that the risk could happen (foreseeability).

Impact: What would be the impact to the school (e.g. this could be in terms of legality, reputation, complaints from parents, reporting in press etc.)

Likelihood and Impact are between 1 and 3, 1 being the lowest.

Owner: The person who will action the risk assessment and recommend the mitigation to the Headteacher/Principal and Local Governing Body.

The final decision rests with Headteacher/Principal and Local Governing Body

End of document