PIONEER ACADEMIES COMMUNITY TRUST

Parkside Primary Academy

On-line Safety Policy

1.

Review/Approve	By Whom	Date	Review Date
Approved	PACT	April 2020	April 2022
Reviewed	LBS	March & July 2023	

Contents

1. Creating an Online Safety Ethos

1.1 Aims and policy scope

This policy applies to all staff including the Governing Body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of the school or Multi Academy Trust (collectively referred to as 'staff' in this policy) as well as children and parents/carers.

This policy takes into account the DfE statutory guidance 'Keeping Children Safe in Education', Early Years and Foundation Stage 2017, 'Working Together to Safeguard Children' 2018 and the Barnsley Safeguarding Children Partnership procedures.

This policy links with several other policies including (but not limited to)

- Safeguarding and Child Protection
- Staff Code of Conduct
- Anti-bullying
- Behaviour
- Use of Digital Images
- Information Security Policy and Acceptable Use Agreement
- Social Media Policy
- UK GDPR and Data Protection
- Relevant curriculum policies including computing, Personal Social Health and Citizenship
  Education (PSHCE) and Sex and Relationships Education (SRE)

The school believes that online safety (e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, mobile phones or games consoles.

The school identifies that the internet and information communication technologies are an important part of everyday life so children must be supported to be able to learn how to develop strategies to manage and respond to risk so they can be empowered to build resilience online.

The school has a duty to provide quality internet access to raise education standards, promote pupil achievement, support professional work of staff and enhance the school's management functions and to ensure that children are protected from potential harm online.

The school believes that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.

The purpose of the Online Safety Policy is to:

- Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use of technology to ensure a safe and secure environment.
- Safeguard and protect all members of the school community online.
- Identify approaches to educate and raise awareness of online safety throughout the community.

- Raise awareness with all members of the school community regarding the potential risks as well as benefits of technology.
- To enable all staff to work safely and responsibly, to model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the school community.

This policy applies to all access to the internet and use of information communication devices including personal devices or where children, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptop or mobile phone.

The school identifies that the issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful material
- **Contact:** being subjected to harmful online interaction with other users
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.
- **Commerce:** risks such as online gambling, phishing and / or financial scams

1.2 Monitoring and Review

Technology in this area evolves and changes rapidly. The school will review this policy at least annually. The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure.

We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.

To ensure they have oversight of online safety, the headteacher will be informed of online safety concerns, as appropriate.

The named governor for safeguarding will report on a regular basis to the governing body on online safety practice and incidents, including outcomes.

Any issues identified via monitoring will be incorporated into our action planning.

1.3 Key responsibilities for the community

The Designated Safeguarding Lead (DSL) has lead responsibility for online safety. **Whilst activities of the designated safeguarding lead may be delegated to an appropriately trained deputy, overall the ultimate lead responsibility for safeguarding and child protection, including online safety remains with the DSL.**

The school recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

1.3.1 Key responsibilities of the management team are:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Developing, owning and promoting the online safety vision and culture to all stakeholders in line with national and local best practice recommendations with appropriate support and consultation throughout the school community.
- Auditing and evaluating current online safety practice to identify strengths and areas for improvement.
- Ensuring there are appropriate and up-to-date policies including a staff code of conduct and acceptable use policy, which covers acceptable use of technology.
- Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.
- Support the DSL and any deputies by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensuring that online safety is embedded within a progressive whole school curriculum which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.
- Making appropriate resources available to support the development of an online safety culture.
- Taking responsibility for online safety incidents and liaising with external agencies as appropriate.
- Receiving and regularly reviewing CPOMS for any online safety incidents and using them to inform and shape future practice.
- Ensuring there are robust reporting channels for the school community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.
- To work with ICT support in monitoring the safety and security of school's systems and networks.
- Audit and evaluate online safety practice to identify strengths and areas for improvement
- To ensure a member of the Governing Body with responsibility for safeguarding is aware of their responsibility for supporting online safety.

1.3.2 Key responsibilities of the Designated Safeguarding Lead are:

- Acting as a named point of contact on all online safety issues and liaising with other members of staff and agencies as appropriate.
- Work alongside deputy DSLs to ensure online safety is recognised as part of the settings safeguarding responsibilities and that a coordinated approach is implemented.
- Ensure that suitable, age-appropriate and relevant filtering and monitoring systems are in place and work with our IT technician to monitor the safety and security of our systems and networks.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and up to date required to keep learners safe online.

- Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.
- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Work with the school lead for data protection and data security to ensure that practice is in line with legislation.
- Maintaining an online safety incident/action log to record incidents and actions taken as part of the school's safeguarding recording structures and mechanisms
- Monitor the school online safety incidents to identify gaps/trends and update the education response to reflect need and to report to the SLT, Governing Body and other agencies as appropriate.
- Report online safety concerns, as appropriate, to the setting management team and Governing Body.
- Work with the leadership team to review and update online safety policies and other procedures at least annually with stakeholder input.
- Ensuring that online safety is integrated with other appropriate school policies and procedures.
- Leading an online safety team/group with input from all stakeholder groups.
- Meet regularly with the governor member with a lead responsibility for online safety.

1.3.3 Key responsibilities of all members of staff are:

- Contributing to the development of online safety policies.
- Reading and adhering to the online safety and acceptable use policies.
- Taking responsibility for the security of school systems and data.
- Having an awareness of online safety issues, and how they relate to the children in their care.
- Modelling good practice in using new and emerging technologies and demonstrating an emphasis on positive learning opportunities rather than focusing on negatives.
- Embedding online safety education in curriculum delivery wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by children in their care.
- Identifying online safety concerns and take appropriate action by following the school's safeguarding policies and procedures.
- Identifying individuals of concern, and taking appropriate action by working with the DSL.
- Knowing when and how to escalate online safety issues, internally and externally.
- Being able to signpost appropriate support available for online safety issues, internally and externally.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site.
- Taking personal responsibility for professional development in this area.

1.3.4 Key responsibilities of staff managing the technical environment are:

- Providing technical support to the DSL and leadership team, especially in the development and implementation of appropriate on line safety policies and procedures.
- Implement appropriate security measures as directed by the DSL and leadership team e.g. passwords and encryption, to ensure that the school's IT infrastructure is secure and not open to misuse or malicious attack, whilst ensuring that learning opportunities are still maximised.
- Taking responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team.
- To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices.
- Ensuring that the school's filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the DSL.
- Ensuring that the use of the setting's network is regularly monitored in order that any deliberate or accidental misuse can be reported to the DSL.
- Report any breaches or concerns to the DSL and SLT and together ensure that they are recorded on the e Safety incident log and appropriate action is taken as advised.
- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
- Report any breaches and liaise with the DFE as appropriate on technical infrastructure issues.
- Ensuring that the school's ICT infrastructure/system is secure and not open to misuse or malicious attack.
- Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.
- Ensure that appropriately strong passwords are applied and enforced for all but the youngest users.

1.3.5 Key responsibilities of pupils (at a level that is appropriate to their individual age and ability):

- Contributing to the development of online safety policies.
- Reading the school Acceptable Use Policies (AUPs) and adhering to them.
- Respecting the feelings and rights of others both on and offline.
- Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.

At a level that is appropriate to their individual age, ability and vulnerabilities:

- Engaging in age appropriate online safety education opportunities.
- Taking responsibility for keeping themselves and others safe online.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

1.3.6 Key responsibilities of parents and carers are:

- Reading the school's AUPs, encouraging their children to adhere to them, and adhering to them themselves where appropriate.

- Supporting our online safety approaches by discussing online safety issues with their children and reinforcing appropriate safe online behaviours at home.
- Role modelling safe and appropriate uses of new and emerging technology.
- Identifying changes in behaviour that could indicate that their child is at risk of harm online.
- Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.
- Contributing to the development of the school online safety policies.
- Using school systems, such as learning platforms, and other network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new
  and emerging technologies

2. Online Communication and Safer Use of Technology

2.1 Managing the school website

The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education.

We will ensure that our website complies with guidelines for publications including: accessibility; UK GDPR; respect for intellectual property rights; privacy policies and copyright.

The contact details on the website will be the school address, email and telephone number. Staff or pupils' personal information will not be published.

The Headteacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.

Pupils work will only be published with their permission or that of their parents/carers.

The administrator account for the school website will be safeguarded with an appropriately strong password.

The school will post information about safeguarding, including online safety on the school website.

2.2 Publishing images and videos online

The school will ensure that all images are used in accordance with the associated policies, including image use, Information Security and Acceptable Use Policy, Codes of Conduct, Social Media.

In line with the school's policy, written permission from parents or carers will always be obtained before images/videos of pupils are electronically published.

2.3 Managing email

Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use policies and Code of Conduct

Pupils may only use the school's provided email accounts for educational purposes.

All members of staff and Governors are provided with a specific school email address to use for any official communication.

The use of personal email addresses by staff for any official school business is not permitted. The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.

Any electronic communication which contains any content which could be subject to data protection legislation must only be sent using secure and encrypted methods.

Members of the school community must immediately tell a member of the SLT if they receive offensive communication and this should be recorded in the school online safety incident log.

Sensitive or personal information will only be shared via email in accordance with data protection legislation.

Access in school to external personal email accounts may be blocked.

Excessive social email use can interfere with learning and will be restricted.

Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.

School email addresses and other official contact details will not be used for setting up personal social media accounts.

2.3.1 Staff email

The use of personal email addresses by staff for any official school business is not permitted.

All members of staff are provided with an email address to use for all official communication.

Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, learners and parents.

Any emails sent between staff and parents/carers should be discussed with the Head teacher or appropriate senior leader prior to being sent. Once the content is agreed the Head teacher should be copied into communication and kept informed of any future correspondence.

School admin email account should always be used. Staff should not use their personal school email address

2.4 Official video conferencing and webcam use

Only in exceptional circumstances does the school participate in video conferencing or webcam use. This is for emergency communication within the staff team. Video/webcam or other such methods of communication are not used directly with pupils.

2.5 Appropriate and safe classroom use of the internet and associated devices

The school uses a wide range of technology. This includes access to:

- Computers, laptops and other digital devices
- Internet which may include search engines and educational websites
- Email
- Games consoles and other games-based technologies
- Digital cameras, web cams and video cameras

The school's internet access will be designed to enhance and extend education. Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.

Pupils will use age and ability appropriate tools to search the internet for content.

Internet use is a key feature of educational access and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum.

The school will ensure that the use of internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information.

All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential. Supervision of pupils will be appropriate to their age and ability.

At Early Years Foundation Stage and Key Stage 1 pupils' access to the internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials which supports the learning outcomes planned for the pupils' age and ability.

At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary. Children will be directed to online material and resources which support the learning outcomes planned for the pupils' age and ability.

All school owned devices will be used in accordance with the school's AUPs and with appropriate safety and security measure in place. Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

The school will use age appropriate search tools as decided by the school following an informed risk assessment to identify which tool best suits the needs of our community.

The school will use the internet to enable pupils and staff to communicate and collaborate in a safe and secure environment.

Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum. Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

2.6 Management of school learning platforms/portals/gateways

The use of a school learning platform is monitored closely by a member of the senior leadership team. The security and management of the platform will be the responsibility of the school's IT officer and its use will adhere to all aspects of online safety and comply with the necessary UK GDPR regulations.

3. Social Media

3.1 General social media use

Expectations regarding safe and responsible use of social media will apply to all members of school community and exist in order to safeguard both the school and the wider community, on and offline. Examples of social media may include blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.

All the school community will be encouraged to engage in social media in a positive, safe and responsible manner at all times.

Information about safe and responsible use of social media will be communicated clearly and regularly.

All members are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others or the school.

The school will control pupils and staff access to social media and social networking sites whilst on site and using school provided devices and systems.

The use of social networking applications during school hours for personal use is not permitted.

Inappropriate or excessive use of social media during school hours or whilst using school devices may result in disciplinary or legal action and/or removal of internet facilities.

Any concerns regarding the online conduct of any member of the school on social media sites should be reported to the Designated Safeguarding Lead and will be managed in accordance

with existing school policies such as, Social Media, Anti-bullying, Allegations Against Staff, Code of Conduct, Behaviour, Safeguarding and Child Protection.

Any breaches of school policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the breaches of policy. Action taken will be accordance with the relevant school policies, such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.

3.2 Official use of social media

Official use of social media sites by the school will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.

Official use of social media sites as communication tools will be risk assessed and formally approved by the Headteacher.

Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.

Official social media use by the school will be in line with existing policies including anti-bullying and child protection.

Information about safe and responsible use of school social media channels will be communicated clearly and regularly to all members of the school community.

Official social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.

Staff use setting provided email addresses to register for and manage any official social media channels.

Official social media sites are suitably protected and, where possible, are linked to our website.

Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.

All communication on official social media platforms will be clear, transparent and open to scrutiny. Parents/carers and learners will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.

Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.

Parents and carers will be informed of any official social media use with learners; written parental consent will be obtained, as required.

We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Staff expectations

Members of staff who follow and/or like our official social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.

If members of staff are participating in online social media activity as part of their capacity as an employee of the setting, they will:

- Sign our acceptable use policy.
- Always be professional and aware they are an ambassador for the setting.
- Disclose their official role and/or position but make it clear that they do not necessarily speak on behalf of the setting.
- Always be responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
- Always act within the legal frameworks they would adhere to within the workplace, including: libel, defamation, confidentiality, copyright, data protection and equalities laws.
- Ensure that they have appropriate consent before sharing images on the official social media channel.
- Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.
- Not engage with any direct or private messaging with current, or past, learners, parents and carers.
- Inform their line manager, the DSL (or deputy) and/or the headteacher of any concerns, such as criticism, inappropriate content or contact from learners.

3.3 Staff personal use of social media

Personal use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.

Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school's AUPS.

Reputation

All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the setting. Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.

All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and should ensure that their social media use is compatible

with their professional role, in accordance with school's policies (safeguarding, confidentiality, data protection etc.) and the wider professional and legal framework.

Members of staff are encouraged not to identify themselves as employees of the school on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members and the wider school community.

Information staff members have access to as part of their employment, including photos and personal information about pupils and their family members, colleagues etc. will not be shared or discussed on personal social media sites.

Members of staff will notify the SLT immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the school.

Communicating with learners and parents / carers

All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or current or past pupils' family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with the SLT.

If ongoing contact with pupils is required once they have left the school roll, then members of staff will be expected to use official school provided communication tools.

All communication between staff and members of the school community on school business will take place via official approved communication channels (such as school email address or phone numbers). Staff must not use personal accounts or information to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher.

Any communication from pupils/parents received on personal social media accounts will be reported to the school's DSL.

Members of staff will be encouraged to manage and control the content they share and post online. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis.

Member of staff will ensure that they do not represent their personal views as that of the school on social media.

School email addresses will not be used for setting up personal social media accounts.

3.4 Pupils' use of social media

Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach, via age appropriate sites and resources.

Safe and responsible use of social media sites will be outlined for pupils and their parents as part of the school AUP.
Pupils will be advised to consider the risks of sharing personal details of any kind on social media sites

The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the school will not create accounts for any children under this age.

Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour. Concerns will be raised with their parents/carers, particularly when concerning any underage use of social media sites.

Pupils will be advised:

- To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
- To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
- Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
- To use safe passwords.
- To use social media sites which are appropriate for their age and abilities.
- How to block and report unwanted communications.
- How to report concerns both within the setting and externally.

4. Use of Personal Devices and Mobile Phones

4.1 Rationale regarding personal devices and mobile phones

The widespread ownership of mobile phones and a range of other personal devices among children, young people and adults will require all members of the school community to take steps to ensure that mobile phones and personal devices are used responsibly.

The use of mobile phones and other personal devices by young people and adults will be decided by the school and covered in appropriate policies including the school's AUPs

The school recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers but requires that such technologies need to be used safely and appropriately within school.

4.2 Expectations for safe use of personal devices and mobile phones

Electronic devices of all kinds that are brought in to school are the responsibility of the user at all times. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.

Mobile phones and personal devices are not permitted to be used by children in school.

The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.

Members of staff will be issued with a school/work phone number and/or email address where contact with pupils or parents/carers is required.

All members of the school community will be advised to take steps to protect their mobile phones or devices from loss, theft or damage.

All members of the school community will be advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen.
Passwords and pin numbers should be kept confidential. Mobile phones and personal devices should not be shared.

All members of the school community will be advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school policies.

School mobile phones and devices must always be used in accordance with the AUP

School mobile phones and devices used for communication with parents and pupils must be suitably protected via a passcode/password/pin and must only be accessed and used by members of staff.

4.3 Pupil use of personal devices and mobile phones

Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones. All use of mobile phones and personal devices by children will be kept in the school office during the school day and be switched off.

If members of staff have an educational reason to allow children to use their mobile phones or personal devices as part of an educational activity, then it will only take place when approved by the SLT.

Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personal devices.

If a pupil breaches the school policy, then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.

School staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene the school's behaviour or bullying policy. The phone or device may be searched by a member of the SLT with the consent of the pupil or parent/carer.

If there is suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, then the device will be handed over to the police for further investigation.

4.4 Staff use of personal devices and mobile phones

Members of staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity. Any pre-exiting relationships which could compromise this must be discussed with leaders/managers.

Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and will only use work-provided equipment for this purpose.

Staff will not use any personal devices directly with children and will only use work-provided equipment during lessons/educational activities.

Staff personal mobile phones and devices will be switched off/switched to 'silent' mode during lesson times.

Bluetooth or other forms of communication should be "hidden" or switched off during lesson times.

Personal mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the SLT in emergency circumstances.

Staff will ensure that any content bought on site via mobile phones and personal devices are compatible with their professional role and expectations.

If a member of staff breaches the school policy, then disciplinary action will be taken in line with our code of conduct, allegations against staff policy, safeguarding and child protection policy.

If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, then the police will be contacted and allegations will be responding to following the allegations management policy.

4.5 Visitors use of personal devices and mobile phones

Parents/carers and visitors must use mobile phones and personal devices in accordance with the school's policy.

Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos is not permitted.

The school will ensure appropriate signage and information is displayed and provided to inform visitors of expectations of use.

Staff are expected to challenge visitors if they have concerns and will always inform the DSL of any breaches of use by visitors.

4.6 Officially provided mobile phones and devices

Members of staff will be issued with a work phone number and email address, where contact with learners or parents/ carers is required.

Setting mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.

Setting mobile phones and devices will always be used in accordance with the acceptable use policy and other relevant policies.

5. Policy Decisions

5.1 Reducing online risks

The school recognises that the internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace. We will ensure that:

- Emerging technologies will be examined for educational benefit and the school SLT will undertake the appropriate risk assessments before use in school is allowed.
- Appropriate filtering systems are in place to prevent staff and pupils from accessing unsuitable or illegal content.
- All reasonable precautions are taken to ensure that users access only appropriate material. However, due to the global and connected nature of internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer or device.
- Technology use is audited to establish if the online safety policy is adequate and that the implementation of the policy is appropriate.
- Methods to identify, assess and minimise online risks will be reviewed regularly by the school's SLT.
- Filtering decisions, internet access and device use by pupils and staff will be reviewed regularly by the school's SLT.

All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in our acceptable use policies and highlighted through a variety of education and training approaches.

5.2. Internet use within the community

The school will liaise with local organisations to establish a common approach to online safety (e–Safety).

The school will provide an AUP for any guest/visitor who needs to access the school computer system or internet on site.

5.3 Managing internet access

The school will maintain a current record of all staff and pupils who are granted access to the school's devices and systems.

All staff learners and visitors will read and sign the school's AUP before using any school ICT resources.

All pupils will be informed of acceptable use of the internet. Posters are displayed across the school.

Parents will be informed that pupils will be provided with supervised internet access which is appropriate to their age and ability.

Parents will be asked to read the school's AUP for pupil access and discuss it with their child, where appropriate.

When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

6. Engagement Approaches

6.1 Engagement and education of pupils

Online safety (e-Safety) will be established and embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible internet use amongst pupils.

Education about safe and responsible use will precede internet access.

Pupils input will be sought when writing and developing school online safety policies and practices.

Pupils will be supported in reading and understanding the school's AUP in a way which suits their age and ability.

All users will be informed that network and internet use will be monitored.

Online safety will be included in the PSHCE (Jigsaw), SRE and Computing programmes of study covering both safe school and home use.

Online safety education and training will be included as part of the transition programme across the key stages and when moving between establishments.

The pupil Acceptable Use expectations and posters will be displayed in all rooms with internet access.

Safe and responsible use of the internet and technology will be reinforced across the curriculum and within all subject areas.

External support will be used to complement and support the school's internal online safety (e-Safety) education approaches.

The school will reward positive use of technology by pupils.

The school will implement peer education to develop online safety as appropriate to the needs of the pupils.

6.2 Engagement and education of pupils who are considered to be vulnerable

The school recognises that some learners are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.

The school will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners, with input from specialist staff as appropriate (e.g. SENCo, designated LAC lead).

6.3 Engagement and education of staff

The Online Safety (e-Safety) Policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of school safeguarding practice.

To protect all staff and pupils, the school will implement AUPs which highlights appropriate online conduct and communication.

Staff will be made aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Up-to-date and appropriate staff training in safe and responsible internet use, both professionally and personally, will be provided for all members of staff on a regular basis.

Those responsible for managing filtering systems or monitoring ICT use will be supervised by the SLT and network manager, and will have clear procedures for reporting issues or concerns.

The school will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils.

All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

6.4 Engagement and education of parents and carers

The school recognises that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology.

Parents' attention will be drawn to the school online safety (e-Safety) policy and expectations in newsletters, letters and on the school website.

A partnership approach to online safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home internet use or highlighting online safety at other well attended events e.g. parent evenings and sports days.

Parents will be requested to read online safety information as part of the Home School Agreement.

Parents will be encouraged to read the school's AUP for pupils and discuss its implications with their children.

Information and guidance for parents on online safety will be made available to parents in a variety of formats. Parents will be encouraged to role model positive behaviour for their children online.

7. Managing Information Systems

7.1 Managing personal data online

Personal data will be recorded, processed, transferred and made available according to the UK-GDPR and Data Protection Act 1998.

Full information regarding the school's approach to data protection and information governance can be found in our Information Security Policy.

7.2 Security and Management of Information Systems

We take appropriate steps to ensure the security of our information systems. The security of the school information systems and users will be reviewed regularly. Virus protection will be updated regularly.

Personal data sent over the internet or taken off site (such as via portable media storage) will be encrypted or accessed via appropriate secure remote access systems.

Portable media may not be used without specific permission followed by an anti-virus /malware scan.

Unapproved software will not be allowed in work areas or attached to email.

Files held on the school's network will be regularly checked.

ICT Support will review system capacity regularly.

The appropriate use of user logins and passwords to access the school network will be enforced for all but the youngest users.

All users are expected to log off or lock their screens/devices if systems are unattended.
The school will log and record internet use on all school owned devices.

Password Policy

All members of staff will have their own unique username and private passwords to access school systems. Members of staff are responsible for keeping their password private.

From Year 2, all learners are provided with their own unique username and private passwords to access our systems; learners are responsible for keeping their password private

All users will be informed not to share passwords or information with others and not to login as another user at any time.

Staff and pupils must always keep their password private and must not share it with others or leave it where others can find it.

School systems require staff to use STRONG passwords for access into our system.

7.3 Filtering and Monitoring Decisions

7.3.1 Decision making

The governors and leaders have ensured that our school has age and ability appropriate filtering and monitoring in place, to limit learners' exposure to online risks

Our internet access strategy will be dependent on the need and requirements of our community and will therefore be designed to suit the age and curriculum requirements of our pupils, with advice from technical, educational and safeguarding staff.

The school uses educational filtered secure broadband connectivity which is appropriate to the age and requirement of our pupils.

The school will ensure that age and ability appropriate filtering is in place whilst using school devices and systems to try and prevent staff and pupils from being accidentally or deliberately exposed to unsuitable content.

The school will have a clear procedure for reporting breaches of filtering which all members of the school community will be made aware of.

Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the SLT.

All changes to the school filtering policy will be logged and recorded.

All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.

7.3.2 Filtering

Education broadband connectivity is provided through Schools Broadband.

The school uses Netsweeper filtering system which blocks sites that fall into categories such as pornography, racial hatred, extremism, gaming, sites of an illegal nature, etc.

The school filtering system will block all sites on the Internet Watch Foundation (IWF).

We work with the network support provider to ensure that our filtering system is continually reviewed.

Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, police or CEOP immediately.

If staff or learners discover unsuitable sites they will be required to:

- turn off the screen and report the concern immediately to a member of staff.
- the member of staff will report the concern (including the URL of the site if possible) to the DSL and / technical staff
- parents / carers will be informed of filtering breaches involving their child

7.3.3. Monitoring

We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by physical monitoring (supervision), monitoring internet and web access (reviewing log file information) and use of technology monitoring services (real time alerts to the Headteacher of inappropriate or safeguarding related content.

If a concern is identified via monitoring approaches we will report to DSL and technical staff who will respond in line with the child protection policy.

All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

7.4 Management of applications (apps) used to record children's progress

We use Educater to track learner progress and share appropriate information with parents and carers.

The Headteacher is ultimately responsible for the security of any data or images held of children. As such they will ensure that the use of tracking systems is appropriately risk assessed prior to use and that they are used in accordance with the UK General Data Protection Regulations (GDPR) and Data Protection legislation.

To safeguard learner's data:

- Only school issued devices will be used for apps that record and store learners' personal details, attainment or photographs.
- Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store learners' personal details, attainment or images.
- Devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
- All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
- Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.
- Only school issued devices will be used for apps that record and store children's personal details, attainment or photographs.
- Devices will be appropriately encrypted if taken off site to prevent a data security breach in the event of loss or theft.
- Staff and parents/carers will be advised on safety measures to protect all members of the community such as using strong passwords, logging out of systems etc.

8. Responding to Online Incidents and Concerns

All members of the school community will be informed about the procedure for reporting online safety (e-Safety) concerns (such as breaches of filtering, cyber bullying, illegal content etc.).

The DSL will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded. The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with thresholds and procedures.

Complaints about internet misuse will be dealt with under the school's complaints procedure. Complaints about online bullying will be dealt with under the school's anti-bullying policy and procedure. Any complaint about staff misuse will be referred to the Headteacher.

Any allegations against a member of staff's online conduct will be discussed with the Local Authority Designated Officer (LADO).

Pupils, parents and staff will be informed of the school's complaints procedure. Staff will be informed of the complaints and whistleblowing procedure.

All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.

All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

The school will manage online safety incidents in accordance with the school discipline/behaviour policy where appropriate. The school will inform parents/carers of any incidents of concerns as and when required.

After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes as required.

Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Education Safeguarding Team or South Yorkshire Police via 999 if there is immediate danger or risk of harm.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to South Yorkshire Police.

If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Education Safeguarding Team.

If an incident of concern needs to be passed beyond the school, then the concern will be escalated to the Education Safeguarding Team to communicate to other schools.

Parents and children will need to work in partnership with the school to resolve issues.

8.1 Concerns about pupil welfare

The DSL (or deputy) will be informed of any online safety incidents involving safeguarding or child protection concerns.

The DSL (or deputy) will record these issues in line with our child protection policy.

The DSL (or deputy) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Barnsley Safeguarding Children Partnership thresholds and procedures.

We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.

8.2 Staff misuse

Any complaint about staff misuse will be referred to the headteacher, in accordance with the Allegations against staff policy.

Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).

Appropriate action will be taken in accordance with our staff behaviour policy/code of conduct.

9. Procedures for Responding to Specific Online Incidents or Concerns

9.1 Online Sexual Violence and Sexual Harassment between children

Our school has accessed and understood "Sexual violence and sexual harassment between children in schools and colleges" (2018) guidance and part 5 of 'Keeping children safe in education' 2023.

We recognise that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.

Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our child protection and anti-bullying policies.

We recognise that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.

We also recognise the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

We will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE.

We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.

We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.

If made aware of online sexual violence and sexual harassment, we will:

- Immediately notify the DSL (or deputy) and act in accordance with our child protection and anti- bullying policies.
- If content is contained on learners' electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
- Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
- Implement appropriate sanctions in accordance with our behaviour policy.
- Inform parents and carers, if appropriate, about the incident and how it is being managed.
- If appropriate, make a referral to partner agencies, such as Children's Social Work Service and/or the Police.
- If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
- If a criminal offence has been committed, the DSL (or deputy) will discuss this with South Yorkshire Police first to ensure that investigations are not compromised.
- Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate

9.2 Responding to concerns regarding Youth produced sexual imagery (or "Sexting")

The school recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy). We will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people'

The school will ensure that all members of the community are made aware of the social, psychological and criminal consequences of sharing, possessing and creating indecent images of children (known as "sexting").

The school will implement preventative approaches via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.

If the school are made aware of incident involving youth produced sexual imagery /indecent images of a child the school will:

- Act in accordance with the school's child protection and safeguarding policy and the relevant Barnsley Safeguarding Children Partnership procedures.
- Immediately notify the DSL.
- Store the device securely.
- Carry out a risk assessment in relation to the children(s) involved.
- Consider the vulnerabilities of children(s) involved (including carrying out relevant checks with other agencies)
- Make a referral to children's social care and/or the police (as needed/appropriate).
- Put the necessary safeguards in place for children e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
- Inform parents/carers about the incident and how it is being managed.
- Implement appropriate sanctions in accordance with the school's behaviour policy but taking care not to further traumatise victims where possible.
- Review the handling of any incidents to ensure that the school is implementing best practice and the SLT will review and update any management procedures where necessary.
- The school will not view the image unless there is a clear need or reason to do so.
- The school will not send, share or save indecent images of children and will not allow or request children to do so.
- If an indecent image has been taken or shared on the school network or devices then the school will take action to block access to all users and isolate the image.
- The school will need to involve or consult the police if images are considered to be illegal.
- The school will take action regarding indecent images, regardless of the use of school equipment or personal equipment, both on and off the premises.
- The school will follow the guidance (including the decision making flow chart and risk assessment template) as set out in "'Sexting' in schools: advice and support around self-generated images. What to do and how to handle it".
- The school will ensure that all members of the community are aware of sources of support

9.3 Responding to concerns regarding Online Child Sexual Abuse and Exploitation

The school will ensure that all members of the community are made aware of online child sexual abuse, including exploitation and grooming including the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.

The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.

The school views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the DSL.

If the school is unclear if a criminal offence has been committed then the DSL will obtain advice immediately through the Education Safeguarding Team and/or South Yorkshire Police.

If the school are made aware of incident involving online child sexual abuse of a child then the school will:

- Act in accordance with the school's child protection and safeguarding policy and the relevant Barnsley Safeguarding Children Partnership procedures.
- Immediately notify the DSL.
- Store any devices involved securely.
- Immediately inform South Yorkshire Police via 101 (using 999 if a child is at immediate risk) or alternatively to CEOP by using the Click CEOP report form: http://www.ceop.police.uk/safetycentre/
- Where appropriate the school will involve and empower children to report concerns regarding online child sexual abuse
- Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
- Make a referral to children's social care (if needed/appropriate).
- Put the necessary safeguards in place for pupil(s) e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
- Inform parents/carers about the incident and how it is being managed.
- Review the handling of any incidents to ensure that the school is implementing best practice and the school SLT will review and update any management procedures where necessary.

The school will take action regarding online child sexual abuse regardless of the use of school equipment or personal equipment, both on and off the school premises.

The school will ensure that all members of the community are aware of sources of support regarding online child sexual abuse.

If pupils at other schools are believed to have been targeted then the school will seek support from the Education Safeguarding Team to enable other schools to take appropriate action to safeguarding their community.

The school will ensure that the Click CEOP report button is visible and available to pupils and other members of the school community, for example including the CEOP report button the school website homepage and on intranet systems.

9.4 Responding to concerns regarding Indecent Images of Children (IIOC)

The school will ensure that all members of the community are made aware of the criminal nature of Indecent Images of Children (IIOC) including the possible consequences.

The school will take action regarding of Indecent Images of Children (IIOC) regardless of the use of school equipment or personal equipment, both on and off the premises.

The school will take action to prevent access accidental access to of IIOC for example using an Internet Service provider (ISP) which subscribes to the Internet Watch Foundation (IWF) block list, implementing appropriate web filtering, implementing firewalls and anti-spam software.

If the school is unclear if a criminal offence has been committed then the DSL will obtain advice immediately through the Education Safeguarding Team and/or South Yorkshire Police.

If the school are made aware of IIOC then the school will:

- Act in accordance with the school's child protection and safeguarding policy and the relevant Barnsley Safeguarding Children Partnership's procedures.
- Immediately notify the school DSL.
- Store any devices involved securely.
- Immediately inform appropriate organisations e.g. the IWF, South Yorkshire Police via 101 (using 999 if a child is at immediate risk) and/or the LADO (if there is an allegation against a member of staff).

If the school are made aware that a member of staff or a pupil has been inadvertently exposed to IIOC whilst using the internet then the school will:

- Ensure that the DSL is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the IWF via www.iwf.org.uk .
- Ensure that any copies that exist of the image, for example in emails, are deleted.
-

If the school are made aware that IIOC have been found on the school's electronic devices then the school will:

- Ensure that the DSL is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the IWF via www.iwf.org.uk .
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
- Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.

If the school are made aware that a member of staff is found in possession of indecent images of children on their electronic device provided by the school, then the school will:

- Ensure that the DSL is informed or another member of staff in accordance with the school whistleblowing procedure.
- Contact the police regarding the images and quarantine any devices involved until police advice has been sought.
- Inform the LADO and other relevant organisations in accordance with the school's managing allegations policy.

- Follow the appropriate school policies regarding conduct.

9.5 Responding to concerns regarding radicalisation or extremism online

The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering is in place which takes into account the needs of pupils

When concerns are noted by staff that a child may be at risk of radicalisation online then the DSL will be informed immediately and action will be taken in line with the school safeguarding policy.

If we are concerned that a member of staff may be at risk of radicalisation online, the Head teacher will be informed immediately, and action will be taken in line with the Safeguarding and child protection policies and Allegations against staff policy.

9.6 Responding to concerns regarding cyber bullying

Cyber bullying, along with all other forms of bullying, of any member of the school community will not be tolerated. Full details are set out in the school policies regarding anti-bullying and behaviour.

All incidents of online bullying reported will be recorded. There are clear procedures in place to investigate incidents or allegations and support anyone in the school community affected by online bullying.

If the school is unclear if a criminal offence has been committed then the DSL will obtain advice immediately through the Education Safeguarding Team and/or South Yorkshire Police.

Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.

The school will take steps to identify the bully where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

Pupils, staff and parents/carers will be required to work with the school to support the approach to cyber bullying and the school's e-Safety ethos.

Sanctions for those involved in online or cyber bullying may include:

- Those involved will be asked to remove any material deemed to be inappropriate or offensive.
- A service provider may be contacted to remove content if those involved refuse to or are unable to delete content.
- Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the school's anti-bullying, behaviour policy or AUP.
- Parent/carers of pupils involved in online bullying will be informed.
- The police will be contacted if a criminal offence is suspected.

9.7 Online Hate

Online hate content, directed towards or posted by, specific members of the community will not be tolerated and will be responded to in line with existing policies, including anti-bullying and behaviour.

All members of the community will be advised to report online hate in accordance with relevant policies and procedures.

The Police will be contacted if a criminal offence is suspected.

If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through the Education Safeguarding Team and/or Barnsley Police.

Appendix E
Online Safety (e-Safety) Contacts and References

National Links and Resources

Action Fraud: www.actionfraud.police.uk

BBC WebWise: www.bbc.co.uk/webwise

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

ChildLine: www.childline.org.uk

Childnet: www.childnet.com

Get Safe Online: www.getsafeonline.org

Internet Matters: www.internetmatters.org

Internet Watch Foundation (IWF): www.iwf.org.uk

Lucy Faithfull Foundation: www.lucyfaithfull.org

Know the Net: www.knowthenet.org.uk

Net Aware: www.net-aware.org.uk

NSPCC: www.nspcc.org.uk/onlinesafety

Parent Port: www.parentport.org.uk

Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

The Marie Collins Foundation: http://www.mariecollinsfoundation.org.uk/

Think U Know: www.thinkuknow.co.uk

Virtual Global Taskforce: www.virtualglobaltaskforce.com

UK Safer Internet Centre: www.saferinternet.org.uk

360 Safe Self-Review tool for schools: https://360safe.org.uk/

Online Compass (Self review tool for other settings):http://www.onlinecompass.org