Pipworth Community Primary School

Online Safety and Social Media policy

Date Adopted:	March 2018
Reviewed:	September 2025
To be reviewed by:	Maria Jackson-Brown
Policy to be reviewed by:	September 2026

W:\StaffShare\POLICIES\Well being policies

Our vision is for all pupils to achieve their best outcomes through a creative, inclusive and engaging curriculum, enabling them to become lifelong learners.

Contents Page

1. Aims

At Pipworth Community Primary School online safety is embedded throughout school life as we use technology and the Internet as part of the curriculum. We take all opportunities to talk with pupils and families about their online behaviours and use of technologies. The primary purpose of this policy is:

- To empower the whole school community with the knowledge to stay safe and keep risk as low as possible is met
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school
- To encourage the use of technology as a means of supplementing and enhancing the learning and teaching experience
- To present children with a range of opportunities and experiences that enable them to utilise their technological skills and knowledge.
- To establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

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

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

2. Legislation and Guidance

Dfee guidance states that whilst the breadth of issues classified within online safety is considerable and ever-evolving, they can be categorised into four areas of risk; **content, contact, conduct and commerce**.

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

- Generative Artificial Intelligence in education
- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

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

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

The schools online policy will operate in conjunction with the National Curriculum computing programmes of study and other policies, including Safeguarding and Child Protection policy, Behaviour and Data Protection policy.

3. Roles and responsibilities

3.1 Governing Body

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

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is Paul Stead.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND).

3.2 Headteacher and Senior Leaders

The Headteacher, supported by the Senior Leadership team, is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 Designated Safeguarding Lead/Team

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

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

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents and promote an awareness and commitment to Online Safety through the life of the school.
- Keeping up to date with the latest risks to children whilst using technology; familiarising themselves with the latest research and available resources for school and home use
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are dealt with appropriately in line with this policy, including responding in a timely manner to alerts from the filtering and monitoring system installed by Ekte (the school's ICT manager)
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services when necessary to ensure any technical online safety measures in school (e.g. Internet filtering software) are fit for purpose
- Providing regular reports on online safety in school to the headteacher and/or governing board

3.4 All Staff and volunteers

Staff are to ensure that:

- They understand, contribute and promote the school's Online Safety guidance and policy.
- They understand and adhere to the staff Acceptable Use and Social Media policy.
- All details within this policy are understood. If anything is not understood, it should be brought to the attention of the Headteacher and Senior Leaders.
- Any online safety incident, suspected misuse or problem is reported to the DSL / Online Safety Officer and Headteacher, and it is logged on CPOMS
- To develop and maintain an awareness of current Online Safeguarding issues and guidance such as sexting, bullying, radicalisation and extremism, online exploitation etc.
- They model safe and responsible behaviours on their own use of technology and maintain a professional level of conduct in their personal use at all times.
- Sensitive and personal data is kept secure at all times by using approved and encrypted data storage and by transferring data through secure communication systems.

- Digital communications with parents or children are NEVER through personal devices e.g. phones, email, social media and always through school based systems
- Online Safety messages are embedded across learning activities across all areas of the curriculum
- Children are supervised and guided when engaged with learning activities that involve online technology.
- Children are aware of research skills and some of the issues that relate such as copyright laws.

3.5 Parents and Carers

Parents play the most important role in the development of their children; as such, 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 are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- To help and support the school in promoting Online Safety
- To read, understand and promote the school's Online Safety policy and the pupil Acceptable Use policy with their children.
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet
- Take responsibility for learning about the benefits as well as the risks of using the Internet and other technologies that their children use in school and at home.
- Take responsibility for their own awareness and learning in relation to the opportunities as well as risks posed by new and emerging technology.
- To discuss Online Safety concerns with their children and promote an open communication at home about content, websites and apps they are using as well as apply appropriate parental controls and ensure they behave safely and responsibly when using technology.
- Model safe and responsible behaviours in their own use of technology and social media.
- Consult with school if they have any concerns about their child's use of the Internet and digital technology.
- Agree and sign the home-school agreement which clearly sets out the use of photographic and video images outside of school.

3.6 Visitors and members of the community

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

3.7 Children of Pipworth Primary

Children also have their own roles and responsibilities to ensure they are safe online and it is expected that they:

- Read and understand the pupil Acceptable Use policy
- Know and understand school policies relating to mobile phones, digital cameras and other personal devices.
- Know and understand the school policy relating to online bullying.
- Take responsibility for learning about the benefits and risks of using the Internet and other technologies at home and at school.
- Be aware of research skills and the legal issues regarding electronic content such as copyright laws.
- Take responsibility in each other's safe and responsible use of technology at school and at home and judging potential risks such as online bullying or inappropriate content or contact.
- To understand what actions to take if they feel worried, uncomfortable and vulnerable or at risk while using technology in school or at home at any time but also if this is happening to someone else.
- To discuss Online Safety issues with family, friends and teachers in an honest and open way.
- Report to a trusted adult any concerns that they have about their own, or other people's online behaviour.

3.8 ICT Technical Support Staff

Ekte Technical Services are contracted by Pipworth Community Primary School to be responsible for ensuring that the infrastructure and network is as safe and secure as is reasonably possible and that the procedures within this policy are implemented.

The ICT staff are responsible for:

- Making opportunities a reality so that pupils can explore all aspects of technology safely, enabling staff to encourage innovation and maximise benefits for education
- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly to block of extremist content and protect against radicalisation in compliance with Prevent Duty, Counter-Terrorism and Security Act 2015.
- Conducting a full security check and monitoring the school's ICT systems on a regular basis- termly
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Responding to staff requests for IT support in a timely manner through the agreed online 'help desk'
- Ensuring that any online safety incidents are dealt with appropriately in line with this policy
- Providing regular updates to the headteacher, the DSL / Online Safety Coordinator and school's Computing curriculum lead
- Ensuring there is an appropriate system in place for users to report any actual or potential technical incident or support.

4. Technical Infrastructure - working the headteacher and school Governors, Ekte will ensure the following

- Technical support staff will have remote access to school system and the Headteacher is the only other staff member who has the administrator password.
- Access provided, in agreement with school, which users should be able to access different folders on the school server
- In agreement with school, which users should and should not have Internet access if required
- Upper KS2 children will have their own log in and password to help enable monitoring of children's Internet access at school. They will be kept safe and be in line with the pupil Acceptable Use policy.
- Staff members will access the Internet using an individual ID and password login which they keep secure. They will ensure they log out after use and not allow pupils to access the Internet through the login. They will abide by the staff Acceptable Use policy.
- Professional judgement is used when using CD's, DVD's and memory sticks on school devices e.g. for educational purposes, show homework etc.
- Personal data cannot be sent over the Internet or taken off school site unless safely encrypted or otherwise secured e.g. encrypted emails, encrypted memory sticks, secure remote access.
- All new technology is risk assessed by Etke as part of the set up process for school use.

4.1 Filtering and Monitoring

- This Internet provision will include filtering appropriate to the age and maturity of the pupils by creating Archive Directories for staff and pupils.
- Technical support will work closely with the Online Safety Officer in regards to Archive Directories staff and pupils. Creating these directories (including staff and year groups) will support the monitoring of pupil's Internet access and enable the safeguarding lead officer to receive alerts and reports for specific children or groups of children when necessary.
- The safeguarding lead has access to Ekte's monitoring system to support the checking, tracking and investigating of monitoring in regards to Internet access by pupils and staff. This will help inform and

alert school of any safeguarding issues. If users discover a website with inappropriate content, it should be reported straight to the Safeguarding Team.

- The filtering and monitoring process will be regularly reviewed for its effectiveness.
- All staff have agreed and signed to acknowledge monitoring by 'Iboss', this is monitored regularly or when alerts signal potentially activity of concern. This will be carried out by the Safeguarding lead and the headteacher, who will formulate and check the reports of activity in each domain filtered by Ekte. The DSL and HT will investigate any activity of concern.

4.2 Antivirus

Antivirus software is installed on all computers and is used to scan local disks, email and network files for malicious software.

- Staff are to immediately alert Ekte to the presence of a virus or other malicious program (providing as much information about messages (if any) displayed) after they have:
    - Stop using the computer immediately
    - Disconnect it from the network by shutting it down and remove any portable media from the computers' sockets.

In addition staff and pupils should not:

- Attempt to interfere with or stop the Anti-Virus software on your computer
- Attempt to introduce virus code, spam software or other malicious code
- Use removable media such as portable hard drives or memory sticks without first scanning them

The anti-virus systems are updated frequently. If a computer is not connected to the network or home Internet for some time, please ensure the IT Support Department scan the contents before you attempt to use it on the network.

4.3 Passwords

Poorly chosen passwords result in the compromise of documents and data so it is important that all staff and children are aware of the importance of passwords, the complexity of creating one and the implications of sharing them.

- Staff members have their own ID and password to access the school system which they do not share.
- Staff have their own work Gmail accounts with their own created passwords which are kept safe and not shared.
- All staff have a responsibility to keep their login details safe and secure.
- KS1 and lower KS2 children have a generic pupil login and staff monitor the screens of the pupils in class.
- Pupils in upper KS2 (Y5 and Y6) have their own login and password which they keep safe and secure in line with the pupil Acceptable Use policy.
- Passwords will be changed if there is a suspicion of compromise for anyone on school site.
- Only disclose passwords to technical support when necessary and never to anyone else.
- All access to school information and data will be controlled via username and password.
- The school maintains a log of all accesses by users and their activities while using the system.

5. Risks related to life online

We recognise that ICT is an important tool in both the society we live in and in the process of teaching and learning. Our vision is for all teachers and learners in our school to become confident users of ICT so that they can develop the skills, knowledge and understanding which enables them to use appropriate ICT resources effectively as powerful tools for teaching and learning. We aim to support children use ICT tools to find, explore, analyse, exchange and present information responsibly, creatively and with discrimination.

5.1 Generative Artificial Intelligence (AI)

Generative Artificial Intelligence (AI) is the defining technology of our age, and it is evolving at incredible speed. This technology has the potential to benefit the economy and meet societal challenges. This is not new, and we already use AI in everyday life for:

- email spam filtering
- media recommendation systems
- navigation apps
- online chatbots

Advances in technology mean that we can now use these tools to produce AI-generated content. This creates opportunities and challenges for the education sector.

It is widely accepted that we currently have limited evidence on the impact of AI use in education on learners' development, the relationship of AI use and educational outcomes, and the safety implications of children and young people using this technology in the classroom. We will continue to follow Government guidance and updates to support pupils to use AI safely, responsibly and effectively.

We do know that content produced by generative AI could be:

- inaccurate
- inappropriate or unsafe
- biased
- taken out of context
- taken without permission (intellectual property infringement)
- out of date or unreliable
- low quality

This is because generative AI:

- returns results based on its training dataset, which may not be specific to our curriculum
- stores and learns from input data
- may not provide results that are comparable with a human-designed resource
- can generate believable content, including credible scam emails
- can provide instructions for illegal or harmful activities
- can produce nonsensical, inaccurate or false information presented as fact, known as hallucination

It is accepted that Generative AI tools can make certain written tasks quicker and easier, but it cannot replace the judgement and deep subject knowledge of a human expert. Staff will use their professional judgement when using these tools to check for appropriateness and accuracy. The quality and content of any final documents will remain the responsibility of the staff member who produced it, regardless of the source of the tools or resources used. Staff who use AI must be aware of the limitations and risks of this technology and use it safely and effectively to deliver excellent education.

Pupils will be taught the additional risks online related to generative AI content such as: being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation and conspiracy theories.

5.2 Searching a device – what are the rules?

In line with legislation in the 2011 Education Act, this policy allows for a device to be examined, confiscated and securely stored if there is reason to believe it contains indecent images or extreme pornography. When searching a mobile device the following conditions should apply:

- The search will be conducted either by the head teacher or a person authorised by them (or Deputy Head or Designated Safeguarding Lead) and one other person only if it is necessary.

- The search will be conducted by a member of the same gender as the person being searched. However if the image being searched for is likely to be of a different gender to the person 'in possession' then the device should only be viewed by a member of the same gender as the person whose image it is.

When working with our school community to minimalise online risks we include the following areas: contact, content, conduct and commerce

5.3 Cyber-bullying

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

Any bullying through digital medium, including:

- Trolling
- Posting private photos
- Gathering information to misuse

Impact of bullying:

- Emotional suffering
- Feeling trapped
- Changes to behaviour in the real world

Cyber bullying is not acceptable in this school. Pupils should feel safe and secure while at school and in the privacy of their own homes. Technology offers opportunities to learn, communicate, collaborate and be entertained in a virtual world. At Pipworth, we educate the pupils to recognise, judge and manage risks in the cyber world. AUP (acceptable use policy) is agreed and followed by all pupils. Internet safety is taught through the curriculum, small group sessions and studied during Online Safety week.

Any reports of cyber bullying are reported to the head teacher and recorded on CPOMS. SLT will deal with the incident using SLT procedures (see anti-bullying policy). Outside agencies, such as South Yorkshire Police, may also be involved depending upon the severity of the case.

To help prevent cyber-bullying

- Pupils are taught to understand what it is and what to do if they become aware of it happening to them or others
- Pupils are taught how they can report any incidents, including where they are a witness rather than the victim.
- Cyber-bullying is actively discussed with pupils explicitly and though other curriculum subjects such as PSHE, explaining the reasons why it occurs, the forms it may take and what the consequences can be.
- All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.
- Information on cyber-bullying is shared with parents/carers, including:
  - Signs of cyber bullying
  - How to report it
  - How they can support children who may be affected.

Dealing with incidents of online bullying/inappropriate online behaviour

Any incidents of cyber-bullying will be addressed following the processes set out in the school Anti-bullying policy.

If illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained and the DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable. They will also work with external services if it is deemed necessary to do so.

The school's Anti-Bullying Policy sets out the processes and sanctions regarding any type of bullying by a child on the school roll.

The Governing Body understands that, "There are circumstances in which police involvement is appropriate. These include where postings have a racist element or where violence is threatened or encouraged." Furthermore, "Laws of defamation and privacy still apply to the web and it is unlawful for statements to be written…which:

- Expose (*an individual*) to hatred, ridicule or contempt;
- Cause (*an individual*) to be shunned or avoided;
- Lower (*an individual's*) standing in the estimation of right-thinking members of society; or
- disparage (*an individual in their*) business, trade, office or profession." (National Association of Head teachers).

5.4 Unsafe communications

Staff will following the principles and procedures set out in 'sexting' when responding to unsafe online communications and pupils will be taught about the risks related to unsafe online communications, as follows:

- Sexting

  Sending or receiving of naked images is considered to be a new form of flirting for young people.

  - It is illegal to have naked photographs of an under 18 on a phone (even if the phone owner is under 18 too)
  - It is illegal to share images of under 18s
  - There is an immediate loss on control of an image that is sent digitally
  - It can cause embarrassment
  - It can lead to bullying and black mailing

  If any illegal images of a young person are found the head teacher or Designated Safeguarding Lead (DSL) will discuss this with the Association of Chief Police Officers (ACPO), using the following general rule 'experimental' or 'aggravated' conduct.

  - **'Experimental conduct'** commonly refers to that shared between two individuals (e.g. girlfriend and boyfriend) with no intention to publish the images further. Coercion is not a feature of such conduct, neither are requests for images sent from one person to multiple other young persons.
  - **'Aggravated conduct'** refers to incidents involving additional criminal or abusive elements beyond the creation, sending or possession of sexual images. This may include the involvement of adults, for example soliciting sexual images from children and young people, or other illegal adult involvement. It may also involve criminal or abusive behaviour by minors such as sexual abuse, extortion, deception or threats; malicious conduct arising from interpersonal conflicts; or creation or sending.

  Any suspicion of 'aggravated conduct' should always be referred to the police.

If you are made aware of an image NEVER view, download or share the image (it is illegal).

- If you see the image by accident, you must report this to the DSL.
- Do search a device to see the image UNLESS there is clear evidence to suggest not to do so would impede a police inquiry
- Do not ask for the image to be deleted
- Do not move the image to another device or storage system
- Do not print the image
- Do not ask them to share information / describe the image (this is for the DSL to do)
- Do not share information about the image with other staff, parents, the person it involves or their parents

- Explain clearly to the young person the process (as stated above in your role) and report to the DSL

Always…

- Inform and involve the DSL so they are able to take any necessary strategic decisions.
- Record the incident.
- Act in accordance with school's s search and confiscation procedures

The DSL may ask the following questions to help decide upon the best course of action:

- Is the child/student disclosing about themselves receiving an image, sending an image or sharing an image?
- What sort of image is it? Is it potentially illegal or is it inappropriate?
- Are the school child protection and safeguarding policies and practices being followed?
- How widely has the image been shared and is the device in their possession?
- Is it a school device or a personal device?
- Does the child/student need immediate support and/or protection?
- Are there other children/students and/or young people involved?
- Do they know where the image has ended up or how many times it was shared?

A referral to the police and/or social care will be made if any of the following are a feature:

- There was an adult involved
- There was coercion or blackmail
- The images were extreme or violent
- The child involved had already been identified as vulnerable or is under 13
- There is an immediate risk of harm

If there is an indecent image of a child on a website or a social networking site then the DSL will:

- Report the image to the site hosting it, follow the reporting procedures on the respective website
- In the case of a sexting incident involving a child or young person at risk of abuse, then the DSL will report the incident directly to CEOP www.ceop.police.uk/ceop-report so that law enforcement can make an assessment, expedite the case with the relevant provider and ensure that appropriate action is taken to safeguard the child.

- Live streaming

  Most social media platforms have this feature which increases the risk to:
  - Online grooming
  - Sexual exploitation

  Screenshots and recordings can be made without the users consent

- Radicalisation

  This can occur through social media and promotes extremist views:
  - Exploits vulnerable people
  - Uses social media (happens in real time)
  - Refer to PREVENT Duty (2015)

- Online relationships

  Not all people are bad on line but there are risks:
  - People pretending to be someone else
  - People giving harmful advice
  - Children becoming at risk of abuse or exploitation

- Fake profiles

  Intention to trick or deceive (catfishes):
  - Lure to offline
  - Lure to transfer / gift money
  - Request sexual images

  Staff should learn to spot fake profiles:
  - Lack of interaction
  - Lack of mutual friends
  - Too good to be true

- Online grooming

  Intention to abuse or exploit.
  - The internet is a popular tool to access and groom
  - Groomers use psychological tricks to isolate victims from friends and family
  - Groomers target vulnerable people
  - Grooming starts online and moves offline

- Child Sexual Exploitation

  Can be online through power / tricks to children:
  - Starts online and moves to offline
  - Black mailing or threats
  - Sexual abuse, often leading to long term behaviours such as drugs, self-harm, alcohol

  Signs
  - Acquisition of money, clothes, mobile phones etc
  - Gang association and/or isolation from peers
  - Exclusion or unexplained absences from school
  - Persistently going missing or returning late
  - Excessive texts, phone calls, multiple handsets
  - Returning home under the influence of drugs or alcohol
  - Inappropriate sexualised behaviour or sexually transmitted infections for age
  - Evidence or suspicions of physical or sexual assault, unexplained injuries
  - Relationships with controlling or significantly older individuals or groups
  - Concerning use of internet/other social media
  - Increasing secretiveness around behaviours
  - Self-harm or significant changes in emotional well-being
  - Decline in academic results & performance

5.5 Managing online information

- Online reputation

  This is your digital footprint, how we portray yourself online and how we are perceived by others, based on what is seen. Everyone needs to know the dangers of negative behaviours:
  - Affect the present and the future (employers can see)
  - Makes people vulnerable to exploitation / grooming **by over sharing information**
  - Identify theft

- Fake news and hoaxes

  False or exaggerated information to intentionally misled others. This can also be tricks / stunts that are staged to mislead and can be dangerous to children.
  - Embarrassing if believed and then discovered to be false
  - Affects how things are perceived off line (this can be damaging)

- Personal data

  Search engines and online platforms farm personal data (cookies).
  - GDPR protects us of misuse but if we are not careful, anyone can gain access to your personal data
  - Web cookies
  - Targeted marketing (information is sold to companies)

- Targeted advertising and pop-ups

  Form of digital marketing aiming at specific adverts based on what YOU have previously searched.
  - Contextual
  - Geo-targeting
  - Re-targeting
  - Web-cookies build a profile of you, depending what you have viewed online will affect what adverts you view in the future
  - Hard to recognise difference between real and fake ads / scam ads

- Dark web

  Needs dedicated software referred to as Tor (it is not illegal use the Dark Web but it gives access to illegal activities).
  - Criminal activity
  - Illegal content (drugs, weapons etc.)
  - Terrorists and paedophiles have anonymity

- Age inappropriate content

  All apps have age ratings but are easily accessible. Think about filters
  - It is impossible to filter everything
  - Sexual and violent content is easily accessed
  - General lack of age verification
  - You need to be aware of what children are accessing online

- Online fraud

  This can be financial, data or identity which can affect offline life.
  - Pop-ups, scams
  - Stolen identify - children's identities are used to carry put fraudulent acts.

5.6 Effects on health, wellbeing and lifestyle

- Online Vs offline identify

  Social Media enables people to portray themselves differently to their offline self.
  Social Media influences image, lifestyle, consumer decisions – basically everything!
  - It promotes unrealistic images using editing tools
  - It creates unhealthy ideals, leading to people questioning themselves
  - Impacts on self-esteem and body confidence
  - Social Media Influencers are paid to influence!

It is important to educate young people about online/ offline identities and fake identifies. Young people need to learn that Social Media Influences do not portray a realistic view of the world and trying to imitate their lifestyle or image may not be healthy.

- Social media and mental health

Children and young people (CYP) are constantly connected which has pros and cons. Always being visible leads to modern pressures linked to Social Media platforms.

- FOMO (Fear Of Missing Out) -> increase usage and increase anxiety
- Self-esteem and body confidence
- Cyber-bullying
- Many Social Media platforms (and some forms of texting) allows the sender to see the message has been opened – if there is not an immediate response, it is considered to be 'aired' and this has consequences for the offline relationship / friendship

- Device addiction

Technology companies use design techniques to increase time online as this increases revenues.

- 2018 WHO defined 'Gaming Disorder' as a pattern of persistent or recurrent **gaming** behaviour so severe that it takes "precedence over other life interests"
- CYP are at risk as their brains are still growing alongside using technology which is engineered to require constant engagement leading:
- Sleep disruption
- Changes in attitude and behaviour
- Neglect of school work
- Lack of focus and concentration
- Plus physical health impacts such as dry eyes, poor posture and lack of physical activity

- Online challenges / viral challenges

These spread and gather pace rapidly with varying levels of risk, often requiring the CYP to share photographic evidence.

- FOMO (Fear Of Missing Out)
- CYP feel social pressure as can gain 'likes' on Social Media platforms
- Can go too far, causing harm

It is not always appropriate to specifically address the dangers of a Viral Challenge in school as this may lead other pupils to the challenge that would have not been interested before. School will alwya follow advice from Sheffield Safeguarding Hub.

- Online gambling

Gambling by anyone of any age can be a problem. Many online games for children have ways of collecting tokens that can be converted for items/ cheats, some real cash. This is training a 'gambling mind' from a young age, as one day the token become real pounds!

- Loot boxes in games increase gambling habits
- Skin gambling encourages gamers to use items gained in games a currency for betting, this can be outside the game on unregulated websites
- There can be a long term impact on mental health and habits at a young age

6. Online safety education and training

In addition to regulation and filtering, pupils are educated to make informed decisions and take a safe a responsible approach to life online. The education of pupils Online Safety is therefore an essential part of the school's Online Safety provisions and the messages that staff give to pupils about keeping safe online.

The Online Safety curriculum is broad and relevant, providing progression across the year groups as it delivered:

- As part of a Computing curriculum and though other curriculum subjects such PSHE and SRE.
- Through key Online Safety messages being taught in all lessons when appropriate as well as being reinforced as part of a planned programme of assemblies including Safer Internet Day.

- By encouraging pupils to be critically aware of materials and content they access online and explore the validity and accuracy of information as well as respect and acknowledge sources of information in respect to copyright laws in all lessons.
- Using suitable opportunities in lessons to raise relevant Online Safety messages which include:
    - The need to protect personal information
    - Considering the consequences their actions on themselves and others
    - Checking the validity of information and acknowledge sources
- Through lessons planned in advance to ensure to check it is age appropriate and adds to the impact and education of the lesson
- To teach pupils how to use a range of age appropriate online tools in a safe and effective way.
- Reminding pupils of their Acceptable Use Policy which they have signed
- By staff modelling safe and responsible use of technology during lessons
- Pupils being guided through Internet research so that they access sites that have been pre-checked for their suitability. (It is recognised that as pupils progress through school, the amount of websites required and also topic of search required may make this unmanageable. It is therefore suggested that reminders of what to do when researching e.g. using key words such as 'kids' may provide better results.)
- By supporting pupils to recognise inappropriate content and the steps to take in terms of their Online Safety.
- By staff being vigilant and regularly checking screens to monitor pupil the use.
- Regularly reminding pupils about how to report Online Safety concerns either at school, at home with a parent or carer but also by organisations such as ChildLine or CEOP.

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

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

Pupils in **Key Stage 2** will be taught to:

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

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

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

Pupils with special educational needs (see also SEND policy)

In order to ensure that children with special educational needs achieve to the best of their ability, it may be necessary to adapt the delivery of the computing and online safety curriculum for some pupils. Where appropriate ICT maybe used to support pupils with SEND to enable them to access the curriculum or engage with programmes that promote their individual progress, such as My Lexia, a personal laptop for recording skills. All access to ICT is monitored by the class teacher,

6.1 Educating parents/carers about online safety

Parents and Carers play a crucial role in ensuring children understand the need to use the Internet and devices in a safe and responsible way. Due to the fast paced changes in how children access and utilise online websites, gaming and social media platforms, we recognise that many people have a limited understanding of the Online Safety risks and issues. Parents and Carers may underestimate just how often children come across potentially harmful and inappropriate material on the Internet and may be unsure how to respond. The school will therefore seek to provide as much information and regular updates to help the awareness across the Pipworth community by:

- Curriculum activities
- High profile events such as Safer Internet Day
- Parent/Carer evenings or sessions
- Letters, newsletters or reference to relevant websites and publications.

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

6.2 Training and educating staff and Governors about online safety

All staff and Governors will receive Online Safety training and understand their responsibilities as outlined in this policy. Training will be offered by:

- Receiving regular information and Online Safety training through annual updates or as required with new developments.
- All new staff will have access to the Online Safety information as part of induction and will fully understand the Acceptable Use policy.
- All staff will be regularly made aware of their individual responsibility for Online Safety and relevant staff to report to in case of concern or misuse.
- This Online Safety policy and its updates will be presented and discussed by staff during staff meetings or INSET days.
- The Online Safety Officer and Designated Safeguarding Lead/Team will provide advice, guidance and training as required as well as perform audits on staff Online Safety training needs.

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

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

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

7. Use of digital and video images

Developments in digital technologies has created significant benefits to teaching and learning, allowing staff and pupils instant use of images that they have uploaded themselves or downloaded from the Internet.

Pupils need to be taught about the potential risks associated with sharing images on the Internet that may cause harm or embarrassment to individuals in the short or long term. Pipworth Primary School will inform

and educate users about these risks and their legal responsibilities and will implement policies to reduce the likelihood of the potential harm.

- Pupils will be educated about the risks and current laws associated with the taking, sharing, use, publication and distribution of images. In particular the risks attached to publishing inappropriate images on the Internet or distributing through mobile technology.
- Images taken by staff will be taken on school equipment (not personal devices) for use on school accounts (Instagram and Facebook) and the school website.
- Digital images and videos of pupils taken to support educational aims, or promote celebration and achievements, will be selected carefully and will comply with good practice ensuring that pupils are always appropriately dressed and are not participating in activities that may bring that individual or school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Permission from parents and carers is obtained before publishing onto the school website or elsewhere and staff will be aware of those pupils who publication of images may not be used.

8. Data Protection (Data Protection Officer DPO)

The **General Data Protection Regulation** (**GDPR 2018)** is a regulation intended to strengthen and unify data protection for all individuals within the European Union (EU) and aims primarily to give control back to citizens and residents over their personal data.

Pipworth Primary continues to review all data protection and internet-safety elements to ensure we remain current with this and other data related directives or orders. The school will:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Use personal data only on secure, password protected computers and devices and ensure they are properly logged off after use.
- Transfer data using encrypted and secure devices.
- All information on school servers shall be accessed through allocated logins with file permission allocated and assessed on a need-to-know privilege basis.
- Staff will not leave printed personal or sensitive information within public areas of school
- All communications involving sensitive information (e.g. email, post) is appropriately secure. Users should be aware that email communication can be monitored.

On portable devices including laptops and memory sticks:

- They must be password protected and encrypted
- They must have approved virus and malware checking software
- Users should be vigilant when accessing sensitive information on screen and ensure that no one else, who may be unauthorised, can read the information.
- All devices with personal information will be secure and not left in cars or unsecure locations.

9. Social media

Social media sites play an important role in the lives of many people, including children. We recognise that social networking can bring many benefits, but there are also potential risks.

Definition - Social media is a broad term for any kind of online platform which enables people to directly interact with each other. It allows people to share information, ideas and views. Examples of social media include blogs, Facebook, LinkedIn, Twitter, Google+, Instagram, Myspace, Flickr and YouTube.

Acceptable use - Employees should be aware that content uploaded to social media is not private. Even if you restrict it to 'friends', there is still capacity for it to be re-posted or distributed beyond the intended recipients. Therefore, employees using social media should conduct themselves with professionalism and respect.

All members of the school community should bear in mind that information that they share through social media and networks, even if it is on private spaces, is still subject to copyright, General Data Protection

Regulation (2018) and Freedom of Information Act (2014), the Safeguarding Vulnerable Groups Act 2006, the Human Rights Act (1998) and UK libel and defamation laws (2013).

- Good practice is encouraged at all times (with regard to both personal and professional use of social media) to protect the school and its employees, and to promote the effective use of social media as part of the school activities and minimise the risks that can impact on the wellbeing of staff, pupils and the reputation of the school.
- Regardless of whether the social media is accessed using the school's IT facilities and equipment, or equipment belonging to members of staff, all personal communications via social media accounts that are likely to have a negative impact on professional standards or the school's reputation are within the scope of this policy.
- This policy is applicable to all individuals working at all levels and grades, including full-time and part-time employees, fixed-term employees and agency workers.

9.1 Statutory requirements

All adults working with children have a responsibility to maintain public confidence in their ability to safeguard the welfare and best interests of children. It is therefore expected that they will adopt high standards of personal conduct in order to maintain the confidence and respect of their colleagues, children, and public in general and all those with whom they work.

Adults in contact with children should therefore understand and be aware that safe practice also involves using judgement and integrity about behaviours in places other than the work setting. The guidance contained in this policy is an attempt to identify what behaviours are expected of school staff who work with children. Anyone whose practice deviates from this document and/or their professional or employment-related code of conduct may bring into question their suitability to work with children and young people and may result in disciplinary action being taken against them.

School staff should always maintain appropriate professional boundaries and avoid behaviour, during their use of the internet and other communication technologies, which might be misinterpreted by others. They should report and record any incident with this potential.

9.2 The use of social networking sites within school

There are many social networking services available and Pipworth Primary School is fully supportive of social network sites as a tool to engage and collaborate with learners and to engage with parents and the wider school community.

The following social networking sites are permitted for use within Pipworth Primary and have been appropriately risk assessed by the Online Safety Officer, if other networks are wished to be used. Any new service will be risk assessed by both the online safety officer and Head teacher, before being permitted.

- Gmail – used by staff to email
- Instagram and Piptac (Facebook)

Notice and take down policy – Should it come to the school's attention that there is a resource which has been inadvertently uploaded and the school does not have copyright permission to use it, it will be removed within one working day.

The school's Acceptable Use of the Internet Policy (AUP) outlines the rules for using IT in school and these rules therefore apply to use of social networking sites. Such sites should not be used or accessed in school unless under the direction of a teacher and for a purpose clearly apparent from the learning objective of the relevant learning experience. If social media sites are used then staff should carry out a risk assessment to determine which tools are appropriate. Parents will give permission for children to access these sites in school.

9.3 Inappropriate use of social media by a pupil

Mobile devices for children are handed to teachers at the start of every day and given back at the end of the school day.

In terms of private use of social networking sites by a child it is generally understood that children under the age of 13 are not permitted to be registered for, for example, Facebook and Instagram accounts.

Following a report of inappropriate use of social media, the senior manager will conduct a prompt investigation.

- If it is found that a pupil purposely submitted the material to the website, that pupil will be disciplined in line with the school's behaviour policy.
- Senior Leaders, where appropriate, will approach the website hosts to ensure the material is either amended or removed as a matter of urgency, i.e. within 24 hours. If the website requires the individual who is complaining to do so personally, the school will give their full support and assistance.
- Checks will be carried out to ensure that the requested amendments or removals are made. If the website(s) does not co-operate, the senior manager will contact the internet service provider (ISP) as the ISP has the ability to block access to certain sites and, in exceptional circumstances, can close down a website.
- If the material is threatening and/or intimidating directly to a member of staff, senior management will, with the member of staff's consent, report the matter to the police.
- The member of staff will be offered full support and appropriate stress counselling.

9.4 Comments posted by parents/carers on social media sites

In the case of inappropriate use of social networking by parents/carers, the Governing Body will contact the parent asking them to remove such comments and seek redress through the appropriate channels such as the Complaints Policy.

- Parents/carers are required to sign an Acceptable Use agreement when their child is admitted to school
- Parents/carers will be made aware of their responsibilities regarding their use of social media via this policy (in particular when their child joins the school), the school website, letter and school newsletters.
- Parents/carers are reminded at school events that photography and filming is not permitted
- Parents/carers are asked not to post images (photos and videos) of pupils other than their own children on social media sites unless they have the permission of parents/carers of other children pictured
- Parents/carers are asked to raise queries, concerns or complaints directly with the school rather than posting them on social media
- Parents/carers should not post malicious or fictitious comments on social media sites about any member of the school community
- Posts and comments on any school led social media platform will be filtered and monitored by staff

9.5 Use of social networking by staff in a personal capacity

It is important for all staff to protect their professional reputation by ensuring that they use their personal accounts in an appropriate manner. Guidelines are issued to staff:

- Staff must **never** add pupils as 'friends' into their personal accounts (including past pupils under 16)
- Staff should not use any information in an attempt to locate or meet a child
- Staff are **strongly advised** not to add parents as 'friends' into their personal accounts
- Staff **must not** post comments about the school, pupils, parents or colleagues including members of the Governing Body
- Staff must not use social networking sites within lesson times (for personal use)
- Staff should enable all privacy settings when using social media
- Staff should only use social networking in a way that does not conflict with the current National Teacher's Standards and code of conduct

- Staff should review and adjust their privacy settings to give them the appropriate level of privacy and confidentiality
- Staff should read and comply with 'Guidance for Safer Working Practice for Adults who Work with Children and Young People'
- Staff must be responsible for their words and actions in an online environment and never upload any content to social media sites that:
  - is confidential to the school or its staff
  - amounts to bullying, unlawful discrimination, harassment or victimisation
  - brings the school into disrepute, undermining the reputation of the school and/or individuals
  - contains lewd, sexually explicit, threatening or similarly inappropriate or offensive comments, images or video clips
  - is defamatory or knowingly false
  - breaches copyright or is unlawful in anyway

Inappropriate use by staff should be referred to the Head teacher in the first instance; this may lead to disciplinary action.

Protection of Personal Information

- Staff should not give their personal e-mail addresses to children or parents. All communication must be sent electronically using a school e-mail address (this can be via enquiries@ or a year group email).
- Staff should keep their personal phone numbers private and not use their own mobile phones to contact children or parents in a professional capacity.
- Staff should never share their work log-ins or passwords with other people.
- Staff are advised to understand who is allowed to view the content on their pages of the sites they use and how to restrict access to certain groups of people.

The Senior Leadership Team are responsible for:

- Addressing any concerns and/or questions employees may have on the use of social media
- Operating within the boundaries of this policy and ensuring that all staff understand the standards

Breaches of this policy by staff

- Any member of staff suspected of committing a breach of this policy (or if complaints are received about unacceptable use of social networking that has potentially breached this policy) will be investigated in accordance with the school's disciplinary procedure.
- The member of staff will be expected to co-operate with the school's investigation which may involve:
  - handing over relevant passwords and login details
  - printing a copy or obtaining a screenshot of the alleged unacceptable content
  - Determining that the responsibility or source of the content was in fact the member of staff.
- The seriousness of the breach will be considered including the nature of the content, how long the content remained visible on the social media site, the potential for recirculation by others and the impact on the school or the individuals concerned.
- Staff should be aware that actions online can be in breach of the harassment/IT/equality policies and any online breaches of these policies may also be treated as conduct issues in accordance with the disciplinary procedure.
- If the outcome of an investigation leads to disciplinary action, the consequences will be dealt with in accordance with the appropriate procedures. Serious breaches could result in the dismissal of the employee.
- Where conduct is considered to be unlawful, the school will report the matter to the police and other external agencies.

10. Acceptable Use

New technologies have become integral to the lives of children and young people in today's society, both within schools/academies and in their lives outside school. The internet and other digital information and

communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school/academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

11. Reporting safeguarding concerns

We must be guided by our legal obligations under the Children Act when making decisions about the level of response. Knowledge of the family should also be taken into account.

- Any content or online activity which raises a safeguarding concern must be reported to the Designated Safeguarding Lead.
    - Write down, with the date and time, (including the year), what you have noticed or are concerned about (this should also be logged on CPOMS).
    - Pass on information **immediately** to the DSL so that the concern can be discussed and appropriate decisions taken as to what to do.
    - If a child discloses to you, the dialogue must be written down as accurately as possible, straight away.

All staff must be aware that the well-being and safety of a child are our first concerns, and a child in distress should be comforted (as is our usual practice.) It is not appropriate however to tell lies to a child in the effort to provide comfort, nor to tell the child that everything will be alright because it may not be.

- Before a referral is made to Social Care, school will discuss with parents/carers the concern that has been raised, and if appropriate the action to consult with Social Care.
- The DSL or deputy DSL will ring the duty social worker at the Sheffield Safeguarding Hub for advice where necessary (Tel: 2734855).
- In cases where it may cause harm to the child or other family members, a consultation with Social Care can be carried out before parents/carers are informed.
- Following any consultation, school will be asked to informed parents/carers that a referral to Social Care.
- Only in extreme cases where the risk of harm is significant will Social Care take action without parents/carers being informed first.
- School will always follow the guidance of the Social Worker as to when parents should be informed if Child Protection procedures are to be instigated.

The DSL or deputy DSL will be responsible for completing a referral to Multi-Agency Complex Case Panel (MACCP) and attending a Strategy Meeting upon the request of Social Care.

If the DSL is out of school, concerns that may arise must be taken to the Deputy DSL, who will respond according to the above procedures. If they too are out of school staff should use the line management.

Disclosures can be difficult and upsetting for staff to handle. Staff should share their feelings / worries with the DSL.

11.1 Responding to incidents that affect the professional reputation of staff

- With regard to personal safeguarding, you should report any harassment or abuse you receive online while using your work accounts.
- Staff should never engage with cyberbullying incidents that they are the victim of.
- If in the course of your employment with this school/trust, you discover a website containing inaccurate, inappropriate or inflammatory written material relating to you, or images of you which have been taken and/or which are being used without your permission, you should immediately report this to a senior manager at your school.
- Staff should keep any records of the abuse such as text, emails, voicemail, website or social media. If appropriate, screen prints of messages or web pages could be taken and the time, date and address of site should be recorded.

12. Monitoring and review

- The Senior Leadership Team has the right to monitor or record communications that are sent or received from within the school's network.
- This policy will be reviewed on a yearly basis and, in accordance with the following, on an as-and-when-required basis:
    - Legislative changes
    - Good practice guidance
    - Case law
    - Significant incidents reported.

This policy runs alongside the Staff and Volunteers Acceptable User Agreement. All members of staff are asked to sign this policy, to record that they have read and understood the contents. By doing so, members of staff are confirming the acceptance of this policy.

Pupils are asked to sign the Acceptable Use Agreement annually as part of Online Safety week.

13. Appendix

13.1 Management of assets

All schools have both hardware and software assets on site for both teaching and learning and also administrative purposes. This all comes at a cost and therefore needs to be controlled and documented accordingly.

- Details of all school-owned hardware and software is recorded in an inventory on purchase.
- All redundant electrical resources will be disposed of through an authorised agency, including a written receipt of the item and destruction of any personal data if applicable.
- Disposal of any ICT equipment will conform to the Waste Electrical and Electronic Equipment Regulations 2006 and 2007.

The disposal of Computers and other ICT Equipment

- The security of any data that may remain on computers or other ICT Equipment is taken very seriously. All redundant ICT equipment that may have held sensitive data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We only use authorised companies who will supply a written guarantee that this will happen and provide a certificate of authenticity and proof once the data has been securely erased.
- Any data that contains information such as student records, personnel information or financial information is securely erased in addition and prior to being sent for secure disposal.
- The IT Technical Support Department maintains a comprehensive inventory of all ICT equipment including a record of disposal. This includes:
- Date item disposed
- Authorisation for disposal.

13.2 Remote/Blended Education, for example, Google Meet or Zoom

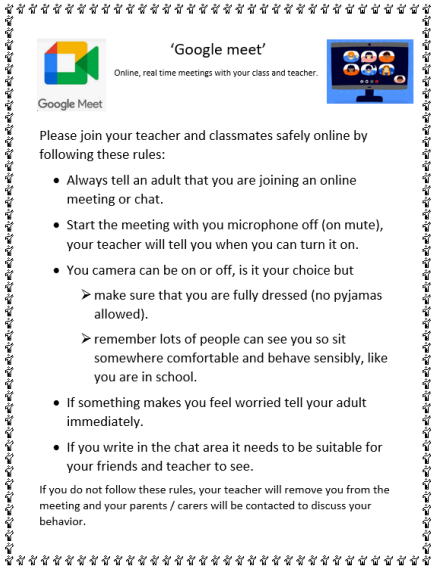
- All teachers share our Meet Rules Policy/ children's guidance with their class prior to a Meet taking place. (See appendix)

- Teachers run Meets from a private location (either at home or in school).

- Recording (either video or photograph) of a Meet is not allowed by teachers or pupils.

- Teachers are aware of how to remove an individual from a Meet if acceptable use guidelines are not followed.

-All pupils must leave the meet before the teachers does so not pupils are not left unattended on the internet.



13.3 Communication Technologies

A rapidly changing area of technology which has huge opportunities to enhance school learning, can also have implications on children's safety. Below is an agreed table relating to the usage of communication technology on school site. Breach of these may be seen as a breach of the Acceptable Use policy.

Communication technologies	Staff and adults				Pupils			
	Allowed	At certain times	Selected staff	Not allowed	Allowed	Certain times	With permission	Not allowed
Mobile phones in school		*					*	
Use phones in lesson								*
Use phones in social time		*						*
Take photos on phone/device				*				*
Use of personal email in school or on school network								*
Use school email for personal use				*				*
Use of blogs		*				*		

The following table displays how appropriate certain activities are using school devices both on site and outside of school:

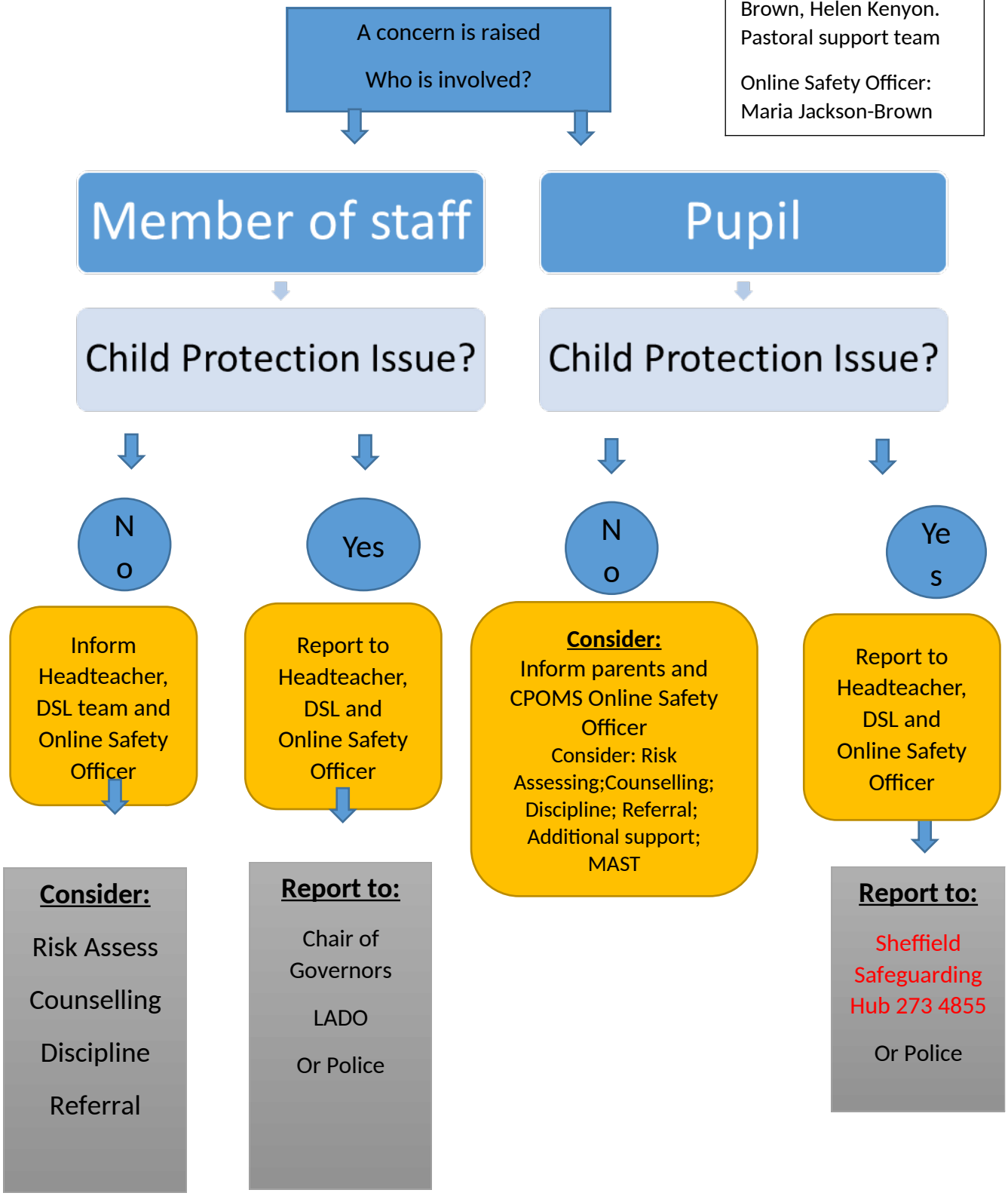
	A	CT	SS	U	U and illegal
Child sexual abuse images- The making, production or distribution of indecent images of children. Contrary to Protection of Children Act 1978					
Grooming, incitement, arrangement or facilitation of sexual acts against children. Contrary to Sexual Offences Act 2003					
Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise obscene nature) Contrary to Criminal Justice and Immigration Act 2008					
Criminally racist material in UK – stir up religious hatred (or sexual orientation) Contrary to Public Order Act 1986 and Radicalisation or extremism. Contrary to Counter Terrorism Act 2015					
Pornography					
Promotion of any kind of discrimination					
Threatening behaviour, including promotion of physical violence or mental harm					
Any other information which may bring offense to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute					
Using school systems to run a private business					
Using systems, apps, websites or other mechanisms to bypass the school filtering and monitoring system					
Infringing copyright					
Revealing or publishing confidential material or data					
Creating or propagating computer viruses or other harmful files					
Unfair usage (downloading/upload large files that hinders use for others)					
Gaming (educational)					
Gaming (non-educational)					
Online gambling					
Online shopping					
Use of social media					
Use of messaging and messaging apps					
Use of video broadcast e.g. YouTube					

A- Allowed CT- at certain times SS- selected staff U- unacceptable

13.4. **Inappropriate Activity Flowchart (At a Glance)**

Designated Safeguarding Team: Maria Jackson-Brown, Helen Kenyon. Pastoral support team

Online Safety Officer: Maria Jackson-Brown



13.5 Response to an Incident of Concern