Tonacliffe Primary School

Online Safety Policy

September 2025

Contents

1. Developing and Reviewing of this Policy

This Online Safety Policy has been developed by Ruth Noble

Date policy created: September 2022 (approved by governors in September 2022)

Policy reviewed and updated: September 2025

This Online Safety policy review was approved by the Curriculum Committee on:	October 2025
The implementation of this Online Safety policy will be monitored by:	Joanne Heap (Headteacher and Lead DSL) Ruth Noble (Computing and Online Safety Lead and Deputy DSL) Charlotte Sutcliffe (Deputy Headteacher and Deputy DSL) Amy Griffiths (Deputy DSL)
Monitoring will take place at regular intervals:	Termly
The Governing Body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group	Three times a year during the Online Safety Group
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	September 2026
Should serious online safety incidents take place, the following external persons / agencies should be informed:	LCC Schools Safeguarding Officer: Victoria Wallace Local authority designated officers: Tim Booth / Shane Penn / Donna Green The police

This policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Cyber security policy
- Data protection policy
- Complaints procedure
- Acceptable use policy for parents
- Acceptable use policy for staff, governors and volunteers
- Acceptable use policy for visitors and contractors
- Ani-bullying policy
- Staff code of conduct

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity
- Surveys / questionnaires of
  - Pupils
  - Staff

2. Aims of this Policy

This policy aims to promote a whole school approach to online safety by:

- Setting out expectations for all Tonacliffe Primary School community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline).
- Helping safeguarding and senior leadership teams to have a better understanding and awareness of all elements of online safeguarding through effective collaboration and communication with technical colleagues (e.g. for filtering and monitoring), curriculum leads (e.g. PSHE) and beyond.
- Helping all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, regardless of device or platform, and that the same standards of behaviour apply online and offline.
- Facilitating the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online.
- Helping school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
  - for the protection and benefit of the children and young people in their care, and
  - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
  - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession.
- Establishing clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy).

3. Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, governors, volunteers and parents) who have access to and are users of the school digital technology systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such an extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other Online Safety incidents covered by the policy, which may take place outside of the school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate Online Safety behaviour that has taken place out of school.

4. Our Aim:

We aim to deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as mobile phones). We aim to have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.

Our school provides a diverse, balanced and relevant approach to the use of technology where all children are encouraged to maximise the benefits and opportunities that the technology has to offer. Children will learn in an environment where security measures are balanced appropriately with the need to learn effectively.

Following the school's Online Safety curriculum, the children will be equipped with the skills and knowledge to use technology appropriately and responsibly. The school's Online Safety curriculum will teach children how to recognise the risks associated with technology and how to deal with them, both within and outside the school environment. Our PSHE curriculum also has links to online safety which have been mapped out clearly to make sure the children are having plenty of support and teaching with some of the key areas of online safety.

We aim to help every pupil and adult to:

- Feel safe and confident when using new technologies.
- Know who to speak to when they feel unsafe.
- Know how to report any abusive behaviour.
- Know how to use the internet correctly, without misuse.
- Know what device is appropriate to use and when/where to use it.
- Identify a potential risk or situation from the onset.
- Stay in control and keep personal information private.

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

- **Content** – being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- **Contact** – being subjected to harmful online interaction with other users, such as child-to-child 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 behavior 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

- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam. If we feel our pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

5. Roles and Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

Our Online Safety Coordinators are Joanne Heap (DSL), Ruth Noble (Deputy DSL and Computing and Online Safety Lead), Charlotte Clutterbuck (Deputy Headteacher and Deputy DSL) and Amy Griffiths (Deputy DSL).

5.1 Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of this policy. A member of the governors has taken on the role of Safeguarding, which covers Online Safety. The governor who oversees online safety is Gareth Snook. The governor who oversees our filtering and monitoring provision is _ (to be elected at full governors in October 2025).

All governors will:

- Ensure they have read and understood this policy.
- Approve this policy and strategy and subsequently review its effectiveness.
- Undergo safeguarding and child protection training.
- Ensure that all staff also receive appropriate safeguarding and child protection (including online safety) training at induction and each academic year.
- Ensure that, where necessary, teaching about safeguarding, including online safety is adapted for the vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a ‘one size fits all’ approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may be more suitable.
- Appoint a filtering and monitoring governor to work with the DSL on the new filtering and monitoring standards.
- Have an overview of the filtering and monitoring provisions within our school.
- Have regular reviews with the online safety lead/DSL to discuss online safety.
- Support the school in encouraging parents and the wider community to become engaged in online safety activities.

The Governor for filtering and monitoring will:

- Have a clear overview of our filtering and monitoring provision.
- Have meetings with the Online Safety Lead.
- Be made aware of any updates or essential major changes to the provision.
- Review the monitoring/filtering check logs created by the online safety lead.
- Ensure that filtering and monitoring provision is reviewed and recorded, at least annually.
- Report to governors' meetings.

5.2 Headteacher

- The DSL should "take **lead responsibility** for safeguarding and child protection (**including online safety and understanding the filtering and monitoring** systems and processes in place). At Tonacliffe Primary School, the DSL/ Headteacher does this with the support of the Deputy DSL and Online Safety Lead. This ensures systems are robust.
- Hold the lead responsibility for online safety, within their safeguarding role.
- Fosters a culture of safeguarding where online safety is fully integrated into whole-school safeguarding.
- The Headteacher will ensure all staff undergo safeguarding and child protection training and updates (including online safety).
- The Headteacher and members of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The headteacher will receive regular monitoring reports from the Online Safety Lead.
- Liaises with the Local Authority/ relevant body.
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- Takes day to day responsibility for online safety issues.
- Ensures the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including remote systems are implemented according to child-safety first principles.
- Better understands, reviews and drives the rationale behind decisions in filtering and monitoring as per the new DfE standards – through regular liaison with the Online Safety Lead, technical colleagues and the DSL team – in particular understands what is blocked or allowed for who, when and how as per KCSIE.
- Works with the online safety lead to ensure that the filtering and monitoring provision is working, up to date and ensuring safety for our pupils.

5.3 Designated Safeguarding Leads

Details of the schools safeguarding lead and deputy leads are detailed within section 1 – developing and reviewing of the policy and within the school's child protection policy.

The DSL's take responsibility for online safety in school, in particular:

- Ensuring "an effective whole school approach to online safety" is fostered as per KCSIE.
- Supporting the Headteacher and Online Safety Lead in ensuring that staff understand this policy and that it is being implemented consistently throughout school.
- Working with the Headteacher, Online Safety Lead and other staff, as necessary, to address any online safety issues or incidents.
- Ensuring that online safety incidents are dealt with and are logged in line with school policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school policy.
- Supporting the Headteacher and Online Safety Lead with the monitoring and filtering provision in school and have an oversight of how this is managed.
- Reminding staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online safety and behaviour apply.
- Receive regular updates in online-safety issues and legislation, be aware of local and school trends – see safeblog.lgfl.net for examples or sign up to the LGfL safeguarding newsletter

Designated safeguarding leads should be trained in Online Safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- Sharing of personal data.
- Access to illegal/inappropriate materials.
- Inappropriate online contact with adults/strangers.
- Potential or actual incidents of grooming.
- Online Bullying.

5.4 Online Safety and Computing Lead:

Ruth Noble, the Online Safety and Computing Lead is also a member of the school's governing body and is a Deputy DSL in school and will follow the roles as described in those sections and has the following roles:

- Takes day to day responsibility for online safety and has a leading role in establishing and reviewing the school online safety policies/documents.
- Works closely on a day-to-day basis with the Designated Safeguarding Lead.
- Has a leading role in establishing and reviewing the school online safety policies/documents.
- Promote an awareness of and commitment to online safety education / awareness raising across the school and beyond.

- Liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff/governors/parents/carers/pupils.
- Collaborates with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use policies.
- Receives reports of online safety incidents and accesses this through CPOMs or Smoothwall and uses this to inform future online safety developments.
- Works with the headteacher and technical staff to ensure that the filtering and monitoring provision is working, up to date and ensuring safety for our pupils.
- Regularly uses the UKSIC test filtering tool to ensure the school's filtering is signed up to and blocking the relevant lists.
- Carries out tests and develop records of results, issues with or changes to the filtering and monitoring provision in school.
- Leads the Online Safety Group with governors to discuss current issues, reviews filtering and logs.
- Attends relevant meetings.
- Reports regularly to the Senior Leadership Team.
- Annually reviews the school's approach to online safety using the LGfL online safety audit.
- Oversees the delivery of the online safety curriculum.
- Works closely with the PSHE lead to monitor any over laps and ensures a complementary whole-school approach.
- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by pupils) with regard to the areas defined In Keeping Children Safe in Education:
    - content
    - contact
    - conduct
    - commerce

5.5 Technical Support:
The technical staff are responsible for ensuring:

- The school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required online safety technical requirements.
- That users may only access the networks and devices through a properly enforced password protection policy.
- Access to potentially dangerous sites and the downloading of potentially dangerous files is blocked.

- Collaborates with the Online Safety Lead/Headteacher to help them make strategic decisions around the safeguarding elements of technology.
- The use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the Headteacher or Online Safety Lead for investigation and action.
- Supports the Headteacher and Online Safety Lead with the setting up of the filtering and monitoring provision in school and works with the companies to make any changes where necessary.
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.

5.6 Teaching and Support Staff:

The teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices.
- They understand that online safety is a core part of safeguarding.
- They implement this policy consistently.
- They have read, understood and signed the Staff Acceptable Use Policy.
- They follow all relevant guidance and legislation including, for example, Keeping Children Safe in Education and UK GDPR regulations.
- They report any suspected misuse or problem to the Headteacher for investigation.
- They work with the Headteacher, Online Safety Lead and DSLs to ensure any online safety incidents are logged and dealt with appropriately in line with the school policy using CPOMs.
- They respond appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of ‘it could happen here’.
- They ensure all incidents of cyber-bullying are dealt with in line with the school behaviour policy and logged appropriately using CPOMs.
- All digital communications with pupils/parents/carers should be on a professional level and only carried out using official school systems (e.g. school email accounts).
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- Pupils understand and follow the acceptable use policies.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities with regards to these devices.
- Ensure pupils understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- In lessons where the internet use is pre-planned, pupils should be guided to sites checked suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

- Report to the online safety lead and headteacher any incidents where the filtering or monitoring may have not worked as expected.
- There is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc.
- They model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.
- They adhere to the school's technical security policy, with regard to the use of devices, systems and passwords and have an understanding of basic cybersecurity.
- They have a general understanding of how the pupils in their care use digital technologies out of school, in order to be aware of online safety issues that may develop from the use of those technologies
- Where staff use AI, they should only use school-approved AI services for work purposes which have been evaluated to comply with organisational security and oversight requirements.
- They are aware of the benefits and risks of the use of Artificial Intelligence (AI) services in school, being transparent in how they use these services, prioritising human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans, fact-checked and critically evaluated.

5.7 PSHE Lead

The PSHE curriculum lead's responsibilities are:

- As listed in the 'teaching and support staff' section, plus:
- To embed consent, mental wellbeing, healthy relationships and staying safe online as well as raising awareness of the risks and challenges from recent trends in self-generative artificial intelligence, financial extortion and sharing intimate pictures online into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives."
- To work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSE.
- To note that an PSHE/RSE policy should be included on the school website.
- To work closely with the Computing subject leader to monitor overlap and ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach

5.8 Pupils

- Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

- Should know what to do if they or someone they know feels vulnerable when using online technology.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to membership of the school.
- Should avoid plagiarism and uphold copyright regulations, taking care when using Artificial Intelligence (AI) services to protect the intellectual property of themselves and others and checking the accuracy of content accessed through AI services.

5.9 Parents and Carers

Parents play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parent's evenings/newsletters/school website.

The school will take every opportunity to help parents and carers understand these issues through:

- publishing the school Online Safety Policy on the school website.
- providing them with a copy of the pupils' acceptable use agreement.
- publish information about appropriate use of social media relating to posts concerning the school.
- seeking their permissions concerning digital images, cloud services etc.
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents must ensure their child has read, understood and agreed to the terms on the acceptable use of the school's ICT systems and internet.

Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events.
- Access to the Online Safety section of the school's website.

This has been done by sending out a parent's acceptable use policy for them to read and sign.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

6. Professional Standards

There is an expectation that professional standards will be applied to online safety as in other aspects of school life i.e.

- There is a consistent emphasis on the central importance of literacy, numeracy, digital competence and digital resilience. Pupils will be supported in gaining skills across all areas of the curriculum and every opportunity will be taken to extend pupils' skills and competence.
- There is a willingness to develop and apply new techniques to suit the purposes of intended learning in a structured and considered approach and to learn from the experience, while taking care to avoid risks that may be attached to the adoption of developing technologies e.g. Artificial Intelligence (AI) tools.
- Staff are able to reflect on their practice, individually and collectively, against agreed standards of effective practice and affirm and celebrate their successes
- Policies and protocols are in place for the use of online communication technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms.
- Where necessary, Generative AI is used to monitor staff communications, it will be balanced with respect for privacy and transparency about what is being monitored and why.

7. Policy

The school Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard pupils in the digital world
- describes how the school will help prepare pupils to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related acceptable use agreements
- is made available to staff at induction and through normal communication channels within staff handbooks, the school website and safeguarding training

- is published on the school website.

7.1 Acceptable Use

The school has defined what it regards as acceptable/unacceptable use and this is shown in the tables below.

The Online Safety Policy and acceptable use agreements define acceptable use at the school. The acceptable use agreements will be communicated/re-enforced through:

- staff induction and handbook
- posters/notices around where technology is used
- communication with parents/carers
- school website.

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Any illegal activity for example:** • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering School will refer to guidance about dealing with self-generated images/sexting – UKSIC					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)					**X**
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)			X	X	
	Promotion of any kind of discrimination				X	
	Using school systems to run a private business				X	

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the school				X	
	Infringing copyright and intellectual property (including through the use of AI services)				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

	Staff and other adults				Pupils			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission/awareness
Online gaming	X				X			
Online shopping/commerce			X					X E.G DT Research
File sharing		X			X			
Social media **Staff* - Unless for the use of texting during lunch or breaks	X *				X			
Messaging/chat			X		X			
Entertainment streaming e.g. Netflix, Disney+			X		X			
Use of video broadcasting, e.g. YouTube, Twitch, TikTok			X		X			
Mobile phones may be brought to school **Staff phones not kept in classrooms – lockers are provided.* *Children's phones are kept in the baskets near the school office and not in school bags.*		X						X
Use of mobile phones for learning at school	X		X		X			
Use of mobile phones in social time at school			X		X			

Taking photos on mobile phones/cameras **Staff can use school iPads/cameras/tablets to take appropriate photos following the policy guidelines.*			X		X			
Use of other personal devices, e.g. tablets, gaming devices	X				X			
Use of personal e-mail in school, or on school network/wi-fi			X		X			
Use of school e-mail for personal e-mails			X		X			
Use of AI services that have not been approved by the school	X				X			

When using communication technologies, the school considers the following as good practice:

- when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school.
- any digital communication between staff and pupils or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. Personal e-mail addresses, text messaging or social media must not be used for these communications.
- staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community
- users should immediately report to a nominated person – in accordance with the school policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school e-mail addresses should be used to identify members of staff and pupils.

8. Reporting and Responding

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

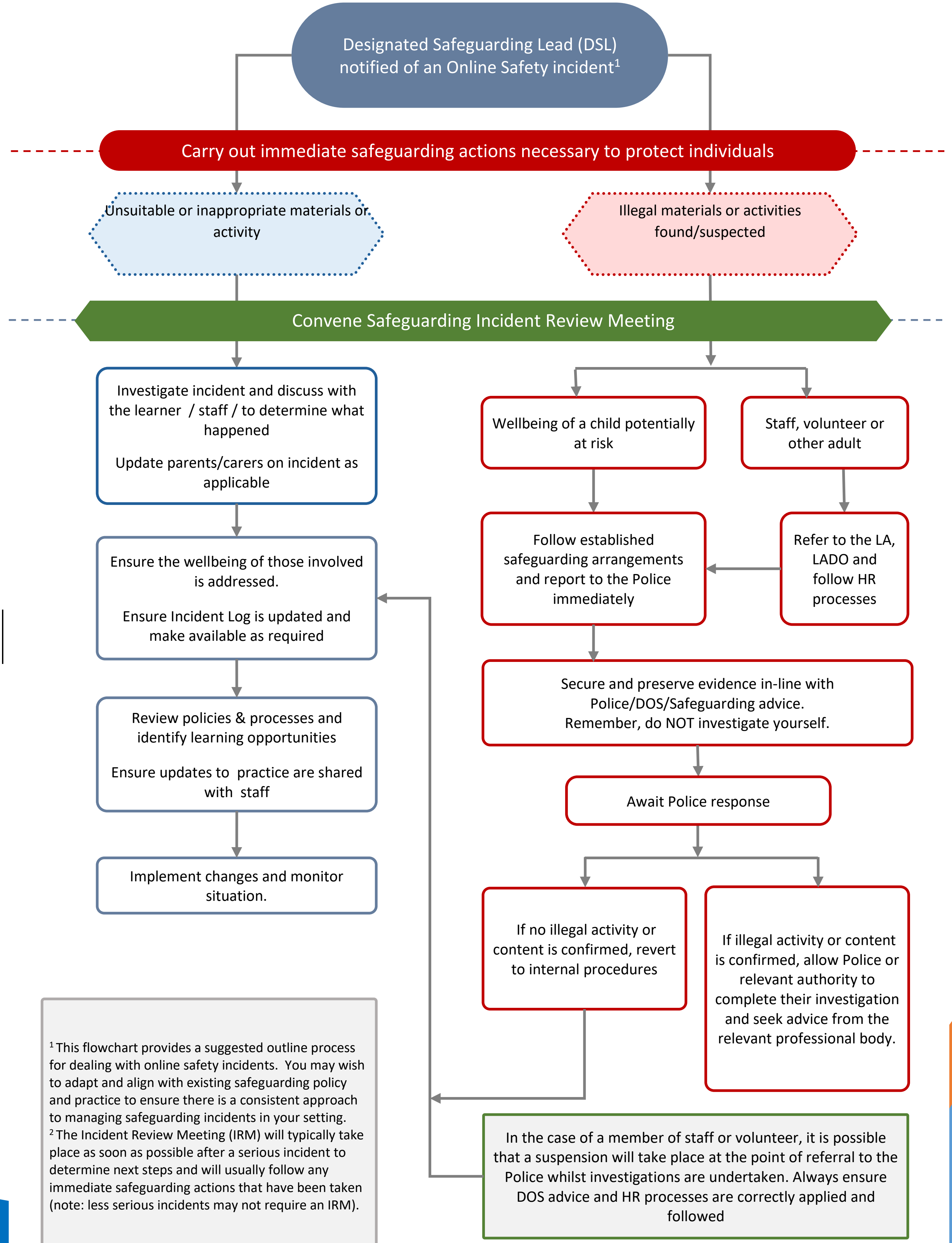
- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- all members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm (see flowchart and user actions chart in the appendix), the incident must be escalated through the agreed school safeguarding procedures, this may include
    - Non-consensual images
    - Self-generated images
    - Terrorism/extremism
    - Hate crime/ Abuse
    - Fraud and extortion
    - Harassment/stalking
    - Child Sexual Abuse Material (CSAM)
    - Child Sexual Exploitation Grooming
    - Extreme Pornography
    - Sale of illegal materials/substances
    - Cyber or hacking offences under the Computer Misuse Act
    - Copyright theft or piracy

- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority
- where AI is used to support monitoring and incident reporting, human oversight is maintained to interpret nuances and context that AI might miss
- where there is no suspected illegal activity, devices may be checked using the following procedures:
    - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
    - conduct the procedure using a designated device that will not be used by pupils and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.

- ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form
- once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
  - internal response or discipline procedures
  - involvement by local authority / MAT (as relevant)
  - police involvement and/or action

- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents should be logged
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
  - the Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with
  - staff, through regular briefings
  - pupils, through assemblies/lessons
  - parents/carers, through newsletters, school social media, website
  - governors, through regular safeguarding updates
  - local authority/external agencies, as relevant

The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.



Designated Safeguarding Lead (DSL) notified of an Online Safety incident[1]

Carry out immediate safeguarding actions necessary to protect individuals

Unsuitable or inappropriate materials or activity

Illegal materials or activities found/suspected

Convene Safeguarding Incident Review Meeting

Investigate incident and discuss with the learner / staff / to determine what happened

Update parents/carers on incident as applicable

Ensure the wellbeing of those involved is addressed.

Ensure Incident Log is updated and make available as required

Review policies & processes and identify learning opportunities

Ensure updates to practice are shared with staff

Implement changes and monitor situation.

Wellbeing of a child potentially at risk

Staff, volunteer or other adult

Follow established safeguarding arrangements and report to the Police immediately

Refer to the LA, LADO and follow HR processes

Secure and preserve evidence in-line with Police/DOS/Safeguarding advice. Remember, do NOT investigate yourself.

Await Police response

If no illegal activity or content is confirmed, revert to internal procedures

If illegal activity or content is confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body.

In the case of a member of staff or volunteer, it is possible that a suspension will take place at the point of referral to the Police whilst investigations are undertaken. Always ensure DOS advice and HR processes are correctly applied and followed

[1] This flowchart provides a suggested outline process for dealing with online safety incidents. You may wish to adapt and align with existing safeguarding policy and practice to ensure there is a consistent approach to managing safeguarding incidents in your setting.

[2] The Incident Review Meeting (IRM) will typically take place as soon as possible after a serious incident to determine next steps and will usually follow any immediate safeguarding actions that have been taken (note: less serious incidents may not require an IRM).

School actions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

Responding to Learner Actions

Incidents	Refer to class teacher	Refer to Online Safety lead/DSL	Refer to Headteacher/Deputy	Refer to Police/Social Work	Refer to local authority technical support for advice/action	Inform parents/carers	Remove device/ network/internet access	Issue a warning	Further sanction, in line with behaviour policy
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on User Actions on unsuitable/inappropriate activities).		X	X	X					
Attempting to access or accessing the school network, using another user's account (staff or learner) or allowing others to access school network by sharing username and passwords	X	X	X	X	X	X	X	X	X
Corrupting or destroying the data of other users.	X	X	X		X	X		X	X
Sending an e-mail, text or message that is regarded as		X	X			X		X	X

offensive, harassment or of a bullying nature									
Unauthorised downloading or uploading of files or use of file sharing.	X	X	X		X	X		X	X
Using proxy sites or other means to subvert the school's filtering system.	X	X	X	X	X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident.	X	X	X	X	X	X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material.	X	X	X	X	X	X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.	X	X	X		X	X	X	X	X
Unauthorised use of digital devices (including taking images)	X	X	X			X	X	X	X
Unauthorised use of online services	X	X	X		X	X	X	X	X
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.	X	X	X		X	X	X	X	X
Continued infringements of the above, following	X	X	X		X	X	X		X

previous warnings or sanctions.									

Responding to Staff Actions

Incidents	Refer to line manager	Refer to Headteacher/ Deputy Headteacher	Refer to local authority/MAT/HR	Refer to Police	Refer to LA / Technical Support Staff for action re filtering, etc.	Issue a warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)		X	X	X		X	X	X
Actions which breach data protection or network / cyber-security rules.	X	X	X	X	X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X	X	X	X	X	X

Using proxy sites or other means to subvert the school's filtering system.	X	X	X	X	X	X	X	X
Unauthorised downloading or uploading of files or file sharing	X	X			X	X	X	X
Breaching copyright/ intellectual property or licensing regulations (including through the use of AI systems)	X	X	X		X	X	X	X
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.	X	X	X		X	X	X	X
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X	X	X	X	X
Using personal e-mail/social networking/messaging to carry out digital communications with pupils and parents/carers	X	X	X	X	X	X	X	X
Inappropriate personal use of the digital technologies e.g. social media / personal e-mail	X	X	X	X	X	X	X	X
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner	X	X	X		X	X	X	X
Actions which could compromise the staff member's professional standing	X	X	X		X	X	X	X

Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.	X	X	X	X	X	X	X	X
Failing to report incidents whether caused by deliberate or accidental actions	X	X	X	X		X	X	X
Continued infringements of the above, following previous warnings or sanctions.		X	X			X	X	X

9. The Use of Artificial Intelligence (AI) systems in School

See separate AI Policy

10. Education and training

10.1 Education - Pupils

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways. The education of pupils in online safety / digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

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 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 same 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 sort 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.

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

Online safety is a focus in all areas of the curriculum and staff make sure they reinforce online safety messages across the curriculum. The online safety curriculum is broad, relevant and provides progression, with opportunities for creative activities and is provided in the following ways:

- A planned online safety curriculum for all year groups is provided as part of Computing and PSHE and other lessons and should be regularly revisited and reinforced and is matched against a national agreed framework using Project Evolve.
- Lessons are matched to need; are age-related and build on prior learning.
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Pupils need and progress are addressed through effective planning and assessment.
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc.
- It incorporates/makes use of relevant national initiatives and opportunities e.g. *Safer Internet Day* and *Anti-bullying week*.
- The programme is accessible to pupils at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- Pupils are taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information (including where the information is gained from Artificial Intelligence services).
- Pupils are taught to acknowledge the source of information used and to respect copyright / intellectual property when using material accessed on the internet and particularly through the use of Artificial Intelligence services.

- Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.
- Pupils are helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school.
- The online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.
- Pupils are supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Where pupils are allowed to freely search the internet, staff should be vigilant in supervising the pupils and monitoring the content of the websites / tools (including AI systems) the pupils visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

10.2 Education - Parents and Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will seek to provide information and awareness to parents and carers through:

- regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes
- regular opportunities for engagement with parents/carers on online safety issues through awareness workshops / parent/carer evenings etc
- the pupils – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by pupils leading sessions at parent/carer evenings.
- letters, newsletters, website, learning platform,
- high profile events / campaigns e.g. Safer Internet Day
- reference to the relevant web sites/publications, e.g. SWGfL; *www.saferinternet.org.uk/; www.childnet.com/parents-and-carers* (see Appendix for further links/resources).
- Sharing good practice with other schools in clusters and or the local authority/MAT
- Sharing information through the use of our Online Safety Hub.

10.3 Education and Training – Staff/Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

All staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- a planned programme of formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced.
- An Online safety questionnaire to be completed annually for all staff to look at training needs.
- the training will be an integral part of the school's annual safeguarding, data protection and cyber-security training for all staff.
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.
- The Online Safety Lead will provide advice / guidance / training to individuals as required.
- 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 can all contain an online element.

10.4 Education and Training – Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/online safety/health and safety/safeguarding. This may be offered in several ways such as:

- attendance at training provided by the local authority/MAT or other relevant organisation (e.g., SWGfL)
- participation in school training / information sessions for staff or parents

A higher level of training will be made available to (at least) the Online Safety Governor. This will include:

- Cyber-security training (at least at a basic level)
- Training to allow the governor to understand the school's filtering and monitoring provision, in order that they can participate in the required checks and reviews.

11. Cyber-bullying

11.1 Definition

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

11.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences may be.

Teachers are encouraged and supported to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, online safety lessons and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, it's impact and ways to support pupils, as part of safeguarding training.

The school also sends information on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident or cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained. All staff are aware that they must not view or forward illegal images of children. The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

11.3 Examining electronic devices

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

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

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

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

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

School staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes and online element.

Any searching of pupils will be carried out in line with:

- The DfE's guidance on screening, searching and confiscation.
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

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

12. Use of Microsoft Teams

Microsoft Teams is used within school for many reasons:

- As a form of meetings with companies, staff and parents.
- To use the assignments tool for the setting of homework for children.

When using Microsoft Teams, all staff will follow the Online Safety Policy. Staff will:

- Make sure that no personal information or identification is shown in the background of the video call.
- Ensure private and confidential video calls are held in private rooms with no children present.
- Teach the children how to be safe when using Microsoft Teams.
- Provide clear rules and expectations to the children and parents in using Microsoft Teams for assignments and homework.

13. Technical

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

13.1 Filtering and Monitoring.

The school filtering and monitoring provision is agreed by senior leaders, governors and the IT Service Provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL (Joanne Heap) and Online Safety Lead (Ruth Noble) has lead responsibility for safeguarding and online safety and the IT service provider (Convene IT alongside Smoothwall and Forinet) will have technical responsibility.

The filtering and monitoring provision is reviewed annually by the Online Safety Lead, senior leaders, the Designated Safeguarding Lead and a governor with the involvement of the IT Service Provider.

Checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of the Online Safety lead and the Designated Safeguarding Lead, in particular when a safeguarding risk is identified, there is a change in working practice, e.g. remote access or BYOD or new technology is introduced e.g. using SWGfL Test Filtering.

13.2 Filtering

At Tonacliffe Primary School:

- The Online Safety Lead (Ruth Noble) and DSL (Joanne Heap) are responsible for ensuring these standards are met. Roles and responsibilities of staff and third parties, for example, in-house or third-party IT support are clearly defined.
- Web filtering is provided by Fortinet on the school site.

- Changes can be made by Ruth Noble (Online Safety Lead and Deputy DSL), Joanne Heap, (Headteacher and DSL) and any other member of Convene IT Staff, when spoken to by Ruth Noble or Joanne Heap.
- Overall responsibility is held by the DSL's Joanne Heap and Ruth Noble.
- Technical support and advice, setup and configuration are from Convene IT.
- An annual review is carried out as part of the online safety audit.
- The school manages access to content across its systems for all users and on all devices using the school's internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.
- Illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated.
- There are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective. These are acted upon in a timely manner, within clearly established procedures.
- There is a clear process in place to deal with, and log, requests/approvals for filtering changes.
- Filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.
- There are regular checks of the effectiveness of the filtering systems. Checks are undertaken across a range of devices at least termly and the results recorded and analysed to inform and improve provision. The DSL and Governor are involved in the process and aware of the findings.
- Devices that are provided by the school have school-based filtering applied irrespective of their location.
- The school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/children, etc.)
- Younger learners will use child friendly/age-appropriate search engines e.g. *SWGfL Swiggle*.
- Access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

If necessary, the school will seek advice from, and report issues to, the SWGfL *Report Harmful Content* site.

13.3 Monitoring

The school has monitoring systems in place, agreed by senior leaders and technical staff, to protect the school, systems and users. The school uses Smoothwall monitoring solutions to monitor the use of computers and laptops owned by the school. Smoothwall monitor provides a real-time, digital monitoring solution that flags incidents as they happen. It monitors keystrokes and informs the Headteacher, Online Safety Lead and DSLs about incidents, providing detailed reports and screenshots when users try to view or type harmful content. The incidents are analysed for indication of risk to a student such as cyber-bullying, suicide, violence or inappropriate use of school resources. The Headteacher and Online Safety Lead and DSLs will be informed via the Smoothwall portal, weekly reports and through notification with the integration of Smoothwall and CPOMS.

- The school monitors all network use across all its devices and services.
- Monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that monitoring is in place.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.
- The monitoring provision is reviewed at least once every academic year and updated in response to changes in technology and patterns of online safety incidents and behaviours. The review should be conducted by members of the senior leadership team, the designated safeguarding lead, and technical staff. It will also involve the responsible governor. The results of the review will be recorded and reported as relevant.
- Devices that are provided by the school have school-based monitoring applied irrespective of their location.
- Monitoring enables alerts to be matched to users and devices.

13.4 Technical security

The school technical systems will be managed in ways that ensure that the school meets recommended standards in the DfE Technical Standards for Schools and Colleges. The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- Responsibility for technical security resides with SLT who may delegate activities to identified roles e.g. the Online Safety Lead and technical staff.
- Users can only access data to which they have right of access.
- Access to personal data is securely controlled in line with the school's personal data policy.
- System logs are maintained and reviewed to monitor user activity.
- There is effective guidance and training for users.
- There are regular reviews and audits of the safety and security of school computer systems, including filtering and monitoring provision.

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling is securely located and physical access restricted.

- There are rigorous and verified back-up routines, including keeping of network separated copies off site or in the cloud.
- Appropriate security measures (including updates) are in place to protect the servers, firewalls, switches, routers, wireless systems, workstations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data, including operating systems.
- The school's infrastructure and individual workstations are protected by up-to-date software to protect against malicious threats from viruses, worms, trojans etc.
- All users have clearly defined access rights to school technical systems and devices.
- All users are provided with a username and secure password by Convene IT, who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and passwords. Users must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Mobile device security and management procedures are in place.
- an appropriate system is in place for users to report any actual/potential technical incident to the SLT/DSL/Online Safety Lead (OSL).
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by Fortinet. Content lists are regularly updated and internet use is logged and monitored.
- Regular checks will be used to make sure our filtering is up to date and blocking the relevant lists using the UKSIC test filtering tool.
- Internet filtering / monitoring ensures that children are safe from terrorist and extremist material when accessing the internet.
- The school provides enhanced / differentiated user-level filtering.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreement is in place regarding the extent of personal use that users (staff / pupils) are allowed on school devices that may be used out of school.

The Headteacher, Online Safety lead, DSL and school staff log behaviour and safeguarding issues related to online safety. The Headteacher, Online Safety Lead and DSL will investigate and manage the issues related and log actions. These will be logged through the Child Protection Online Management System (CPOMS).

13.5 Passwords

A safe and secure username/password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and learning platform

Policy Statements:

- The password procedures reflect NCSC and DfE advice/guidance.
- The use of passwords is reduced wherever possible, for example, using Multi-Factor Authentication (MFA) or (Single Sign On) SSO.
- School networks and system will be protected by secure passwords.
- Passwords are encrypted by the system to prevent theft.
- Passwords do not expire and the use of password managers is encouraged.
- Passwords are immediately changed in the event of a suspected or confirmed compromise.
- No default passwords are in use. All passwords provided "out of the box" are changed to a unique password by the IT Service Provider.
- A copy of administrator passwords is kept by the IT providers or on a password protected document only accessible by the Online Safety Lead/Headteacher.
- All users (adults and learners) have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Passwords must not be shared with anyone.

13.6 Mobile Technologies

Mobile technology devices are school owned. Pupils' personal mobile devices are not allowed to be used in school – see personal electronic devices policy. All users should understand that the primary purpose of the use of mobile devices in a school context is educational and that the school will not be held responsible for personal devices in school.

The school acceptable use agreements for staff, learners, parents, and carers outline the expectations around the use of mobile technologies.

The school allows:

	School devices			**Personal devices**		
	School owned for individual use	School owned for multiple users	Authorised device[1]	Student owned	Staff owned	Visitor owned
Allowed in school	**Yes**	**Yes**	**Yes**	No*	Yes	Yes
Full network access	Yes	Yes	Yes	No	No	No
Internet only	Yes	Yes	Yes	No	No	Yes**
Any network access	Yes	Yes	Yes	No	No	No

*children personal devices are collected and handed in at the office.

**this is dependent on situation e.g Ofsted/LA advisor/Out of hours care.

When on site, all staff must:

- Make sure their personal devices are kept in certain areas – unless leaving the school premises. The headteacher and office staff keep their phones within locked draws in their office. All other staff must keep their personal devices/mobile phones in the staffroom.
- If staff are waiting for important calls such as doctor appointments, mechanics and health calls, phones can be left within the school office.
- Not take their phone out of the given areas within the school day.
- Phones must be left on silent unless left in the office for important and urgent calls.
- Only use their mobile phones within dedicated breaks within working hours, unless on PPA or agreed situations with the Headteacher.

[1] Authorised device – purchased by the learner/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

The school caretaker will have his work phone on his person throughout the day. This phone has no access to the internet or a camera.

Supply staff will be informed of the school rules in relation to personal mobile devices. If they bring their phone onto the premises, they must keep their phone in the staffroom or the school office.

Any visitors to school will be informed of the school rules in relation to personal mobile device. They will not be able to use their personal devices when children are present (contractors completing on site works, for example, PAT testing may need phones for work purposes) unless agreed otherwise by SLT.

People and companies that let the school premises will follow their own policies and procedures.

Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL or headteacher of any breaches of the policy.

14. Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet.

The Online Safety Lead will inform and educate users about risks involved with the use of digital and video images and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognize the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes.
- Permission from parents or carers will be obtained before photographs of pupils are published on the school website, school social media page or local press.
- In accordance with guidance from the Information Commissioner’s Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone’s privacy and in some cases protection, parents are informed that these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.

- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images are only to be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care is taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- The school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.
- Images will be securely stored in line with the school retention policy.

15. Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

For more information regarding data protection and GDPR, please refer to our school's GDPR policy.

Staff must ensure that they:

- 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 other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- The data must be encrypted and password protected.
- The device must be password protected.
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

To help protect personal data within the school office, school children will not be allowed to enter the office.

16. Email

The use of email is an essential means of communication for staff. We recognise that pupils need to understand how to style an email in relation to their age and good network etiquette.

In our school, the following statements reflect our practice in the use of email:

- The school gives all staff their own email account to use for all school business as a work-based tool. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- The school requires a standard disclaimer to be attached to all email correspondence.
- All emails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.
- When logging onto emails off the school premises and using personal devices, a two-factor verification has been set up.

Staff must:

- Inform the Online Safety Lead and the Headteacher if they receive an offensive email.
- Treat incoming email should be treated as suspicious and attachments not open unless the author is known.
- Not use staff email for personal advertising.
- Check emails regularly.
- Log into and out of their emails every time they have accessed them.

17. Social media

Social media (including all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:

- Ensuring that personal information is not published.
- Education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues.
- Clear reporting guidance, including responsibilities, procedures, and sanctions.
- Guidance for learners, parents/carers.

When official school social media accounts are established or used, there is:

- A process for approval by senior leaders.
- Clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff.
- A code of behaviour for users of the accounts.
- Systems for reporting and dealing with abuse and misuse.
- Understanding of how incidents may be dealt with under school disciplinary procedures.

17.1 Expectations

- The expectations regarding safe and responsible use of social media applies to all members of the Tonacliffe school community.
- The term social media include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.
- All members of the Tonacliffe school community are expected to engage in social media in a positive, safe and responsible manner.
    - All members of the Tonacliffe school community 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.
- Concerns regarding the online conduct of any member of the Tonacliffe school community on social media, should be reported to the DSL and will be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.

17.2 Staff personal use of social media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of the 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 our code of conduct/behaviour policy and policy on social networking sites and other forms of social media as part of the acceptable use policy.

- They must not use their social media accounts for personal use during working hours.
- Staff must familiarise themselves with the site's 'privacy settings' in order to ensure that information is not automatically shared with a wider audience than intended.
- They do not conduct or portray themselves in a manner which may
  - Bring the school into disrepute;
  - Lead to valid parental complaints;
  - Be deemed as derogatory towards the school and/or its employees;
  - Be deemed as derogatory towards pupils and/or parents and carers;
  - Bring into question their appropriateness to work with children and young people.
- Staff must notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online to ensure that their social media is compatible with their professional role and is in accordance with our policies and the wider professional and legal framework.
- All members of staff are encouraged not to identify themselves as employees of Tonacliffe on their personal social networking accounts; this is to prevent information on these sites from being linked with the setting, and to safeguard the privacy of staff members.
- Staff must make sure there is no reference made in social media to learners, parents/carers or school staff.
- Staff must not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school.
- Staff should make sure security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.

Communicating with pupils and parents and carers

- All members of the staff are advised not to communicate with or add as ‘friends’ any current or past pupils via any personal social media sites, applications or profiles.
    - Any pre-existing relationships or exceptions may compromise this, will be discussed with DSL or headteacher.
- Staff will not use personal social media accounts to contact pupils or parents.
- Any communication from current or past pupils received on personal social media accounts will be reported to the DSL or headteacher.

17.3 Monitoring of public social media

- As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school.
- The school should effectively respond to social media comments made by others according to a defined policy or process.
- When parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

17.4 Pupils use of social media

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

- We are aware that many popular social media sites state that they are not for children under the age of 13, therefore we will not create accounts specifically for pupils.
- Pupils are advised not to place personal photos on any social networking site. They are taught to consider how public the information is and consider using private areas. Advice is given regarding the background detail in a photograph which could identify the pupil or his/her location.
- Pupils are advised on the security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils are encouraged to invite known friends only and deny access to others by making profiles private.
- Pupils are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Pupils are advised to use nicknames and avatars when using social networking sites.
- Pupils are taught about how to keep personal information safe when using online services.
- Pupils are taught to never give out personal details of any kind which might identify them and/or their location.

18. The school website

The school website will contain a page outlining the school's online safety messages so that the children and parents and carers can use this information when online and outside of the school environment.

- Staff are aware of the guidance associated with the use of digital media and personal information on the school website and this is included in the Acceptable Use Policy.
- Staff or pupil personal contact information will not be published. The contact details given online are that of the school office.
- Photographs that include pupils will be selected carefully so that individual pupils whose parents have not been given consent are not in photos online.
- Pupil's full names will not be used anywhere on a school website or other online space in association with photographs.
- Permission from parents or carers will be obtained when they start school before photographs are published on the school website.

19. Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, learners; parents/carers and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors
- parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
- the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

20. Responding to Online Safety incidents and concerns

Illegal offences

Any suspected illegal material or activity will be brought to the immediate attention of the headteacher who will refer this to the external authorities, e.g. Police, CEOP etc.

Inappropriate use

The school will deal with incidents that involve inappropriate use. Incidents will be dealt with quickly and actions will be proportionate to the offence.

- All staff are aware of the different types of online safety incidents and how to respond appropriately.
- All incidents and concerns will be logged on CPOMS, our online safeguarding system.
- We require staff, parents, carers and pupils to work in partnership to resolve online safety issues.
- After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- Parents, carers or external agencies will be involved when necessary.

21. Staff Misuse

- Any complaint about staff misuse will be referred to the headteacher in accordance with the allegations policy.
- Any allegations regarding a member of staff's online conduct will result in following the procedure outlined in our Child Protection Policy and the PANS Lancashire procedures and 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.

22. Procedures for responding to specific online incidents or concerns.

22.1 Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Tonacliffe.
- Full details of how we will respond to cyberbullying are set out in our anti-bullying policy.

22.2 Online hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Tonacliffe 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 will obtain advice through the Multi agency safeguarding hub or the Lancashire Police.

22.3 Online radicalisation and extremism

- We will take all reasonable precautions to ensure that pupils and staff are safe from terrorist and extremist material when accessing the internet on site.
- If we are concerned that a child or parent/carer may be at risk of radicalization online, the DSL will be informed immediately, and action will be taken in line with our child protection policy.
- If we are concerned that a member of staff may be at risk of radicalization online, the headteacher will be informed immediately, and action will be taken in line with the child protection and allegations polices.

22.4 Indecent images of children (IIOC)

- Tonacliffe will ensure that all members of the community are made aware of the possible consequences of accessing indecent images of children.
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- We will seek to prevent accidental access of IIOC by using internet filtering, firewalls and anti-spam software.
- If we are unclear if a criminal offence has been committed the DSL will obtain advice immediately through Lancashire Police and/or LSCB.
- If made aware of IIOC, we will:
  - Act in accordance with our child protection policy and the relevant Lancashire Safeguarding Child Board procedures.
  - Store any devices involved securely.
  - Immediately inform appropriate organisations, such as the Internet Watch Foundation, Lancashire Police or the LADO.
- If made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children, we will:
  - Ensure the DSL is informed.
  - Ensure that the URLs which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk

    - Ensure that any copies that exist of the image, for example in emails, are deleted.
    - Report concerns, as appropriate to parents and carers.
- If made aware that indecent images of children have been found on the setting provided devices, we will:
    - Ensure that the DSL is informed.
    - Ensure that the URLs which contain the suspect images are reported to the Internet Watch Foundation 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 and Children's Social Work Service (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.
    - Report concerns, as appropriate to parents and carers.
- If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:
    - Ensure that the headteacher is informed in line with our managing allegations against staff policy.
    - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.
    - Quarantine any devices until police advice has been sought.

22.5 Online sexual violence and sexual harassment between children (child-on-child abuse).

The school recognizes that child-on-child abuse can take place online.

Examples include the following:

- Non-consenual sharing of sexual images and videos
- Sexualised cyberbullying
- Online coercion and threats
- Unwanted sexual comments and messages on social media
- Online sexual exploitation

The school responds to all concerns regarding online child-on-child abuse, whether or not the incident took place on the school premises or using school owned equipment.

Concerns regarding online child-on-child abuse are reported to the DSL who will investigate the matter in line with the Child Protection and Safeguarding Policy.

22.6 Online child sexual abuse and exploitation

Through the online safety curriculum, pupils are taught about how to recognise online and abuse and where they can go for support if they experience it.

The schools responds to concerns regarding online abuse and exploitation, whether or not it took place on the school premises or using school-owned equipment.

All concerns relating to online abuse and exploitation, including child sexual abuse and exploitation and criminal exploitation, are reported to the DSL and dealt with in line with the Child Protection and Safeguarding Policy.

23. Useful link for Education Settings

Lancashire support and guidance for educational settings

LSCB:

http://www.lancashiresafeguarding.org.uk/

General Enquiries:

Telephone: 01772 536954

Email: children.cypsafeguarding@lancashire.gov.uk

Twitter: https://twitter.com/LancsSguarding

Concerns about a child should be reported on Lancashire 0300 123 6720 or out of hours 0300 123 6722 (8pm-8am); or Rochdale 0300 303 0440 or out of hours 0300 303 8875. (Monday 11am-11.30am Monday-Friday 5.30pm-8.30am. Anytime weekends and bank holidays.)

Lancashire Schools' ICT Centre can provide advice on dealing with social media issues (telephone: 01772 532626 or email: AskICT@btlancashire.co.uk). In addition, the Professionals Online Safety Helpline (POSH) is able to support colleagues with issues such as protecting their professional identity and online harassment by parents.

In the event of a serious incident, schools should contact the Schools Safeguarding Officer, Tammy Twang, 01772 531196, CYPsafeeduc@lancashire.gov.uk.

General advice and guidance on dealing with incidents can be obtained through the Schools' ICT Centre.

Lancashire Police

https://www.lancashire.police.uk/ or https://www.lancashire.police.uk/help-advice/online-safety

In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Lancashire Police via 101.

National Links and Resources for Educational Settings

- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Internet matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
- Childline: www.childline.org.uk
- Net Aware: www.net-aware.og.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
- Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk

National Links and Resources for Parents/carers

- Action Fraud: www.actionfraud.police.uk
- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation: www.iwf.org.uk
- NSPCC: www.nspcc.org.uk/onlinesafety
- Childline: www.childline.org.uk
- Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk