Totley Primary School

Online Safety Policy

Date Agreed:	Janurary 2020
Date Reviewed:	
Reviewed by:	Ben Paxman
Policy to be reviewed by:	July 2021

Totley Primary School Online Safety Policy

Policy Statement

For clarity, the online safety policy uses the following terms, unless otherwise stated:

User: refers to staff, governing body, school volunteers, students, and any other person working in or on behalf of the school, including contractors

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

School: Any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc

Wider School Community: Students, all staff, governing body, parents

Safeguarding is a serious matter; at Totley Primary School we use technology and the Internet throughout the curriculum. Online safeguarding, known as online safety, is an area that is constantly evolving and as such, this policy will be reviewed on an annual basis or in response to an online safety incident, whichever is sooner.

The primary purpose of this policy is:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and as low risk as possible is met
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school
- To encourage the use of technology as a means of supplementing and enhancing the learning and teaching experience.
- To present children with a wide range of opportunities and experiences to ensure they can successfully utilise their technological skills and knowledge in a variety of contexts.

This policy is available for anybody to read on the Totley Primary School website; upon review, all staff members will read and understand both the online safety policy and the Staff Acceptable Use Policy. A copy of the Students Acceptable Use Policy will be sent home and returned at the beginning of every year. Upon return of the completed Student Policy and acceptance of the terms and conditions, students will be permitted access to school technology including the Internet. The school approach to online safeguarding and its policy will be reinforced through the curriculum and programme of study. This policy applies to all members of the Totley Primary School community (including staff, Governors, pupils, volunteers, parents/carers and work place students) who have access to and are users of school ICT systems, both in and out of 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 applies to incidents of online bulling or other Online Safeguarding incidents covered by this policy, which may take place out of school. But is linked to membership of the school.
- **The Education Act 2011** gives the school the power to confiscate and search the contents of any mobile device if the Headteacher believes it contains any illegal content or material that could be used to bully or harass others.
- The school will identify in this policy and in the associated behaviour policy and anti-bullying policies, how incidents will be manage and how parents/carers are informed of inappropriate Online Safety behaviours that take place in and out of school.
- **Keeping Children Safe in Education** is a statutory guidance from the Department for Education issued under Section 175 of the Education Act 2002, the Education (Independent School Standards) Regulations 2014 and the Education (Non-Maintained Special Schools) Regulations 2011. Schools must have regard to it when carrying out their duties to safeguard and promote the welfare of children. The document contains information on what schools **should** do and sets legal duties with which schools **must** comply. It should be read alongside statutory guidance **Working Together to Safeguard Children 2015**
- **Counter-Terrorism and Security Act 2015** From July 1 2015, all schools are subject to a duty under Section 26 OF THE Counter-Terrorism and Security Act 2015, in the exercise of their functions, to have “due regard to the need to prevent people from being drawn into terrorism”

This policy has been developed by committee made up of:

- Headteacher and Senior Leaders
- Online Safety Officer
- Staff – including Teachers, Support Staff and Technical Staff
- Governors
- Parents/Carers

Consultation with the whole school community has taken place through a range of informal meetings across school.

Teaching and Learning

ICT prepares children to participate in a rapidly changing world in which work and other activities are increasingly transformed by access to varied and developing technology. We recognise that ICT is an important tool in both the society we live in and in the process of teaching and learning. Children use ICT tools to find, explore, analyse, exchange and present information responsibly, creatively and with discrimination. They learn how to employ ICT to enable rapid access to ideas and experiences from a wide range of sources.

Our vision is for all teachers and learners in our school to become confident users of ICT so that they can develop the skills, knowledge and understanding which enables them to use appropriate ICT resources effectively as powerful tools for teaching & learning.

Pupils with special educational needs (see also SEND policy)

We believe that all children have the right to access ICT and computing. In order to ensure that children with special educational needs achieve to the best of their ability, it may be necessary to adapt the delivery of the ICT Cheadle Primary School Computing and ICT Policy and computing curriculum for some pupils. We teach ICT and computing to all children, whatever their ability. ICT and computing forms part of the national curriculum to provide a broad and balanced education for all children. Through the teaching of ICT and computing we provide learning opportunities that enable all pupils to make progress. We do this by setting suitable learning challenges and responding to each child's different needs. Where appropriate ICT and computing can be used to support SEN children on a one to one basis where children receive additional support. Additionally, as part of our dyslexia friendly approach to teaching and learning, we will use adapted resources wherever possible such as visual timetables, different coloured backgrounds and screen printouts.

Roles and Responsibilities

Governing Body

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

- Review this policy at least annually and in response to any online safety incident to ensure that the policy is up to date, covers all aspects of technology use within school, to ensure online safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- Appoint one governor to have overall responsibility for the governance of ICT and online safety at the school who will:
  - Keep up to date with emerging risks and threats through technology use
  - Receive regular updates from the Headteacher in regards to training identified risks and any incidents.
  - Have regular meetings with the Online Safety Officer to monitor incidences and filtering in school to report back to Governors.

Headteacher and Senior Leaders

Reporting to the governing body, the Headteacher and Senior Leaders have overall responsibility for online safety within our school. The day-to-day management of this will be delegated to a member of staff, the Online safety officer, as indicated below.

The Headteacher and Senior Leaders will ensure that:

- Online safety training throughout the school is planned and up to date and appropriate to the recipient
- The designated online safety officer has had appropriate CPD in order to undertake the day to day duties
- Ensure that there is a mechanism in place to allow for monitoring and support of those in school carrying out the internal Online Safety role. This provision provides a safety net and also supports those colleagues who take on these important monitoring roles.
- The Headteacher and Senior Leaders will ensure everyone is aware of procedures to be followed in the event of an Online Safety incident.
- All online safety incidents are reported and dealt with promptly and appropriately.

Designated Safeguarding Lead/Team

Online Safety is becoming an increasing part in children's lives and is just one part of a whole child. Therefore, the Designated Safeguarding Lead/Team will always be fully involved where online safety is concerned.

The Designated Safeguarding Lead/Team will ensure that:

- They understand the issues surrounding the sharing of personal or sensitive information and to ensure that personal data is protected in accordance to the Data Protection Act 1998.
- They understand the risks and dangers regarding access to inappropriate online content and contact with adults and strangers.
- They are aware of potential or actual incidents involving the grooming of children and young people in relation to sexual exploitation, radicalisation and extremism.
- They are aware that the use of social media, online bullying and online gaming can be used for this purpose.

Online Safety Officer

The day-to-day of online safety is devolved to the Online Safety Officer and will involve professional dialogue and meetings when appropriate with the Designated Safeguarding Lead. The online safety officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarising themselves with the latest research and available resources for school and home use thus ensuring that the school policy and approaches are up to date.
- Ensure this policy is systematically reviewed regularly and bring any matters to the attention of the Headteacher and Senior Leaders.
- To promote an awareness and commitment to Online Safety through the life of the school.
- To communicate regularly with the school technical staff, designated Online Safety governor and the Headteacher and Senior Leaders.
- Advise the Headteacher, Senior Leaders and governing body on all online safety matters.
- Have regular contact and meetings with the Safeguarding team.

- Engage and organise engagement with parents and the school community on online safety matters at school and home.
- Liaise with the Local Authority, IT technical support and other agencies as required.
- Be included in CPOMS reports involving Online Safety concerns which ensures a running record of incident logs.
- Ensure any technical online safety measures in school (e.g. Internet filtering software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.
- Make themselves aware of any reporting function with technical online safety measures, i.e. internet filtering reporting function; liaise with the Headteacher and responsible governor to decide what reports may be appropriate for viewing.

ICT Technical Support Staff

Technical support staff are responsible for ensuring that:

- They are fully aware of their role and responsibilities at Totley Primary School.
- To understand, contribute and help towards the school's Online Safeguarding policies and guidance.
- Understand and adhere to the staff Acceptable Use policy
- To develop and maintain an awareness of current Online Safeguarding issues, legislation and guidance relevant to their work.
- The IT infrastructure is secure; this will include at the minimum:
  - Anti-virus is fit for purpose, up to date and applied to all capable devices
  - Windows (and any other operating systems) updates are regularly monitored and devices updated as appropriate
  - Any online safety technical solutions such as Internet filtering are operating correctly
  - Filtering levels are applied correctly and according to the age of the user; that categories of use are discussed and agreed with the Online Safety Officer and Headteacher and Senior Leaders.
  - Ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.

All Staff

Staff are to ensure that:

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

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

All staff, Governors, work place students and volunteers

This section applies to any adult, but those particularly working with children and young people (paid or unpaid) within Totley Primary. It is to ensure that every person is aware how their online behaviour may affect their own safety and reputation and that of the school. Communications between adults and children, young people and other adults should be transparent and take place with clear boundaries, no matter what method of communication. This does include the wider use of technology such as mobile phones, texting, social media, digital cameras, emails, videos, web-cams and blogs.

When using digital communication, staff, governors and volunteers should:

- Only make contact with children for professional reasons and in accordance with the policies and professional guidance from school.
- Not share their personal information with a child including email, phone number or other personal contact details.
- Not request or respond to any personal information for the child other than that which may be appropriate as part of the professional role, or if the child is in immediate risk of harm.
- Not send or accept friend requests from any children on social networks.
- Not send or accept friend requests from any parent or carer on social networks unless personal circumstances differ from the usual professional relationship e.g. relative or school friend. Professional judgement by the Headteacher and Senior Leaders will be used if there are any uncertainties. (see Model Social Media Policy for Teaching and Support Staff in Schools 2012 for further advise).
- Understand that all communications are transparent and open to scrutiny.
- Be aware that online communication is open to misinterpretation.
- Ensure that personal social networking profiles and details are not shared with children or parents to make every effort to keep personal and professional lives separate.
- Do not post anything that could bring the school into disrepute.
- Be aware of the sanctions that may be applied for breaches of policy related to professional conduct.

Parents and Carers

Parents play the most important role in the development of their children; as such, the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents evening, school letters and school tweets, the school will keep parents up to date with new and emerging online safety risks and will involve parents in strategies to ensure that students are empowered.

- To help and support the school in promoting Online Safeguarding

- To read, understand and promote the school’s Online Safety policy and the pupil Acceptable Use policy with their children.
- Take responsibility for learning about the benefits as well as the risks of using the Internet and other technologies that their children use in school and at home.
- Take responsibility for their own awareness and learning in relation to the opportunities as well as risks posed by new and emerging technology.
- To discuss Online Safety concerns with their children and promote an open communication at home about content, websites and apps they are using as well as apply appropriate parental controls and ensure they behave safely and responsibly when using technology.
- Model safe and responsible behaviours in their own use of technology and social media.
- Consult with school if they have any concerns about their child’s use of the Internet and digital technology.
- Agree and sign the home-school agreement which clearly sets out the use of photographic and video images outside of school (see Appendix)

Children of Totley Primary

As well as supporting their online safety in school through engaging and purposeful lessons across the curriculum, children also have their own roles and responsibilities to ensure they are safe.

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

Education

Pupils

Whilst regulation, technical solution and filtering are very important, their use must be balanced with the education of pupil to take a safe a responsible approach and make informed decisions online. The education of pupils Online Safety is therefore an essential part of the school’s Online Safety provisions. Children and young people need the help and support to recognise and mitigate risks to build their own resilience online. Online Safety will be part of a broad and balanced curriculum and staff will reinforce Online Safety messages. The Online Safety curriculum should be broad, relevant and provide progression across the year groups. This will be provided by:

- A planned Online Safety curriculum will be provided as part of a Computing curriculum and will regularly be met during relevant and meaningful PSHE and SRE lessons.
- Key Online Safety messages will be taught in all lessons when appropriate and will also be reinforced as part of a planned programme of assemblies including Safer Internet Day.

- Pupils will be taught in all lessons to be critically aware of materials and content they access online and explore the validity and accuracy of information as well as respect and acknowledge sources of information in respect to copyright laws.
- We will raise relevant Online Safety messages when and where suitable opportunities arise within any lesson which include:
  - the need to protect personal information
  - consider consequences their actions may have on themselves and others
  - check validity of information and acknowledge sources
- Internet use will be planned in advance to ensure to check it is age appropriate and adds to the impact and education of the lesson
- Pupils will be taught how to use a range of age appropriate online tools in a safe and effective way.
- We will remind pupils of their Acceptable Use policy which they will sign and will be displayed throughout school where user logins are used.
- Staff will model safe and responsible use of technology during lessons
- In lessons where Internet research is planned, it is best practice that pupils are guided to sites pre-checked for their suitability. However, it is recognised that as they progress through school, the amount of websites required and also topic of search required may make this unmanageable. It is therefore suggested that reminders of what to do when researching e.g. using key words such as 'kids' may provide better results.
- In lessons where the Internet or electronic devices are used more freely, pupils are reminded of the Acceptable Use policy and the steps to take in terms of their Online Safety and what to do if they come across inappropriate content.
- Staff are vigilant and monitor the use by regularly checking screens.
- Pupils will be regularly reminded about how to report Online Safety concerns either at school, at home with a parent or carer but also by organisations such as ChildLine or CEOP.

Governors

Governors should take part in Online Safety training and awareness sessions, especially those who are involved in the overseeing of the Online Safety at Totley Primary School. This can be done by:

- Attendance of training provided by the Local Authority/ National Governors Association or other relevant organisations
- Participation in school training or information sessions for teachers or parents.

All Staff (including Governors)

It is essential that the education of our staff is always developing. All staff receive Online Safety training and understand their responsibilities as outlined in this policy. Training will be offered by:

- Receiving regular information and Online Safety training through annual updates or as required with new developments.
- All new staff will have access to the Online Safety information as part of induction and will fully understand the Acceptable Use policy.
- All staff will be regularly made aware of their individual responsibility for Online Safety and relevant staff to report to in case of concern or misuse.
- This Online Safety policy and its updates will be presented and discussed by staff during staff meetings or INEST days.

- The Online Safety Officer and Designated Safeguarding Lead/Team will provide advice, guidance and training as required as well as perform audits on staff Online Safety training needs.

Parents/Carers

Parents and Carers are at the forefront of a child's life and play a crucial role in ensuring children understand the need to use the Internet and devices in a safe and responsible way. Many people have a limited understanding of the Online Safety risks and issues, yet it is essential they are involved in this area of education for children. Parents and Carers may underestimate just how often children come across potentially harmful and inappropriate material on the Internet and may be unsure how to respond. The school will therefore seek to provide as much information and regular updates to help the awareness across the Totley community by:

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

Use of digital and video images

The development of digital imaging technologies has created significant benefits to teaching and learning, allowing staff and pupils instant use of images that they have uploaded themselves or downloaded from the Internet. However, everyone needs to be aware of potential risks associated with sharing images and with posting digital images on the Internet. Those images may remain available on the Internet forever and may cause harm or embarrassment to individuals in the short or long term. Totley Primary School will inform and educate users about these risks and their legal responsibilities and will implement policies to reduce the likelihood of the potential harm.

- When using digital images, staff will inform and educate pupils about the risks and current laws associated with the taking, sharing, use, publication and distribution of images. In particular, they should recognise the risks attached to publishing inappropriate images on the Internet or distributing through mobile technology.
- Staff are allowed to take digital images and videos of pupils to support educational aims or promote celebration and achievements but must follow polices concerning the sharing and publication of these images. Images should be taken on school equipment and not personal devices.
  - In the case of the School Twitter account and the Headteacher, a risk assessment and professional judgement has been made.
- Care must be taken when taking digital and video images that pupils are appropriately dressed and are not participating in activities that may bring that individual or school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on websites or elsewhere will be selected carefully and will comply with good practice on the use of such image. Staff will be aware of those pupils who publication of images may put them at risk.
- Written permission from parents and carers will be obtained before publishing onto the school website or elsewhere.

For further details, please refer to the Totley Primary School 'Digital Image Policy'.

Managing ICT systems and access: Technical infrastructure and equipment

Totley Primary School is responsible for ensuring that the infrastructure and network is as safe and secure as is reasonably possible and that the policies and procedures approved within this policy are implemented and meet recommended technical requirement.

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, mobile devices etc from accidental or malicious attempts which might threaten the security of school systems and data.
- Hardware and infrastructure is protected by active, up to date virus software
- Technical support will hold regular reviews and updates to ensure the safety and security of technical systems
- Technical support have remote access to school system and the Headteacher is the only other staff member who has the administrator password.
- School will agree which users should and should not have Internet access if required and appropriate levels of access and supervision is in place through school.
- Children will have their own log in and password to help enable monitoring of children's Internet access at school. They will be kept safe and be in line with the pupil Acceptable Use policy.
- Staff members will access the Internet using an individual ID and password login which they keep secure. They will ensure they log out after use and not allow pupils to access the Internet through the login. They will abide by the staff Acceptable Use policy.
- An appropriate system is in place for users to report any actual or potential technical incident or support.
- Professional judgement is used when using CD's, DVD's and memory sticks on school devices e.g. for educational purposes, show homework etc.
- Personal data cannot be sent over the Internet or taken off school site unless safely encrypted or otherwise secured e.g. encrypted emails, encrypted memory sticks, secure remote access.

Filtering and Monitoring

- The school uses a filtered Internet service which is provided by Smoothwall. Smoothwall ensures the block of extremist content and protect against radicalisation in compliance with Prevent Duty, Counter-Terrorism and Security Act 2015.
- This Internet provision will include filtering appropriate to the age and maturity of the pupils by creating Archive Directories for staff and pupils. This will allow the school to be proactive regarding the nature of content which can be viewed on site.
- Technical support will work closely with the Online Safety Officer in regards to Archive Directories staff and pupils. Creating these directories (including staff, year groups and SEN/DA) will support the monitoring of pupil's Internet access and enable the Online Safety Officer to receive alerts and reports for specific children or groups of children when necessary.
- The Online Safety Officer has access to Smoothwall's monitoring system to support the checking, tracking and investigating of monitoring in regards to Internet access by pupils. This will help inform and alert school of any safeguarding issues.
- If users discover a website with inappropriate content, it should be reported straight to the Safeguarding Team.
- The filtering and monitoring process will be regularly reviewed for its effectiveness.

Passwords

Passwords are an important aspect of computer security with poorly chosen passwords resulting in the compromise of documents and data. From this, as well as providing a more informed monitoring system, it is important that all staff and children are aware of the importance of passwords, the complexity of creating one and the implications of sharing them.

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

Management of assets

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

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

Data Protection (ask about a Senior Information Risk Officer SIRO and Data Protection Officer DPO)

Totley Primary has access to a wide range of personal data, held digitally and on paper records. Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than necessary
- Secure
- Only transferred to others with adequate protection

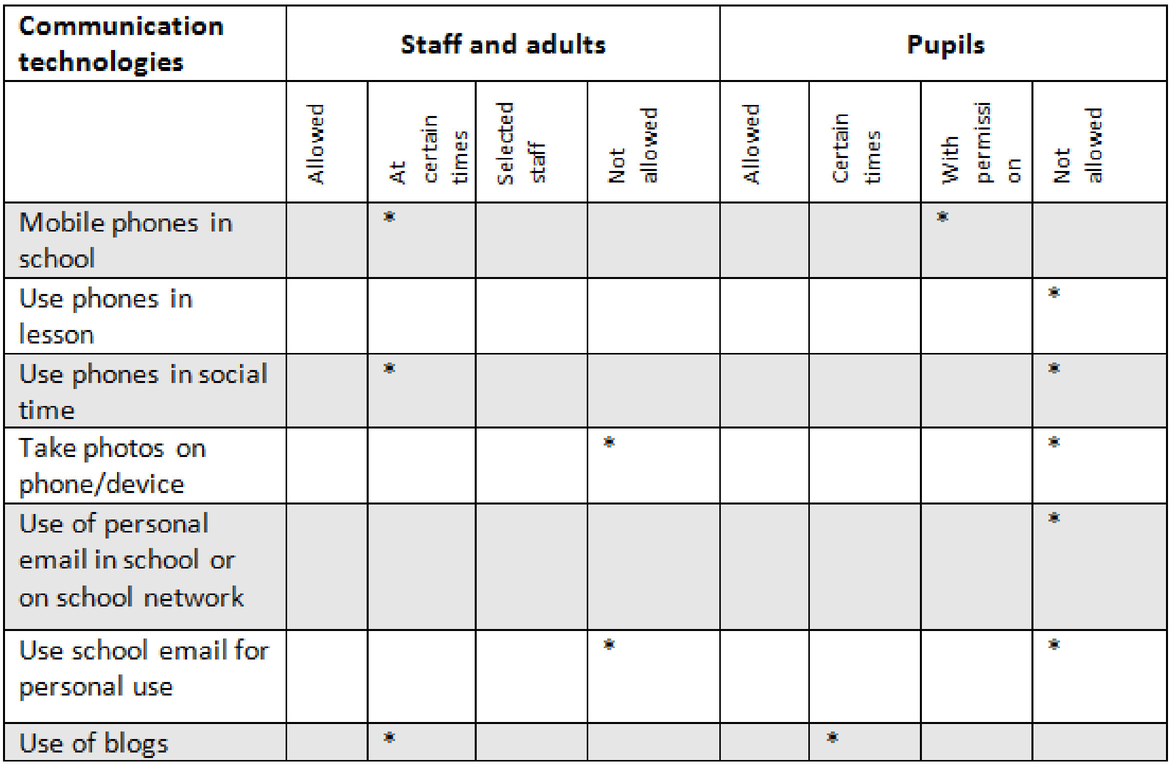
The school will:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Use personal data only on secure, password protected computers and devices and ensure they are properly logged off after use.

- Transfer data using encrypted and secure devices.
- On portable devices including laptops and memory sticks:
  - They must be password protected and encrypted
  - They must have approved virus and malware checking software
- Users should be vigilant when accessing sensitive information on screen and ensure that no one else, who may be unauthorised, can read the information.
- All information on school servers shall be accessed through allocated logins with file permission allocated and assessed on a need-to-know privilege basis.
- Staff will not leave printed personal or sensitive information within public areas of school
- All communications involving sensitive information (e.g. email, post) is appropriately secure. Users should be aware that email communication can be monitored.
- All devices with personal information will be secure and not left in cars or unsecure locations.

Communication Technologies

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



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

Please note that mobile devices for children are handed to teachers at the start of every day and given back at the end of the school day.

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

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

Responding to misuse

It is hoped that all members of staff and members of the school community will be responsible users of ICT. However, there may be times where infringements of the policy occur through carelessness or very rarely, deliberate use. If any of the above deemed ‘unacceptable’ or ‘illegal’, then it will be dealt with through usual disciplinary procedure.

Social Networking

There are many social networking services available and Totley Primary School is fully supportive of social network sites as a tool to engage and collaborate with learners and to engage with parents and the wider school community. The following social networking sites are permitted for use within Totley Primary and have been appropriately risk assessed by the Online Safety Officer, if other networks are wished to be used. Any new service will be risk assessed by both the online safety officer and Headteacher, before being permitted.

- Gmail – used by staff to email
- Blogging – currently trialling class blog in Y5. Areas of school website also used as blog for all year groups (see appendix for policy)
- Twitter – used by the school as a broadcasting service
- Staff Blog – a closed blog for staff to share CPD
- Vimeo – a closed area to upload videos to be converted to QR codes

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

'Appendix Sexting'

Steps to take in the case of a sexting incident in school

Step 1 - Disclosure by a student

Sexting disclosures should follow the normal safeguarding practices and protocols (see the schools Safeguarding Policy).

The child/student is likely to be very distressed especially if the image has been circulated widely and if they don't know who has shared it, seen it or where it has ended up. They will need pastoral support during the disclosure and after the event. They may even need immediate protection or a referral to police or social services; parents should be informed as soon as possible (police advice permitting).

The following questions will help decide upon the best course of action:

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

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

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

Step 2- Searching a device – what are the rules?

Please refer to the school's Search and Confiscation Policy which is based on the most current legislation: The 2011 Education Act.

The policy allows for a device to be examined, confiscated and securely stored if there is reason to believe it contains indecent images or extreme pornography. When searching a mobile device the following conditions should apply:

- The action is in accordance with the school's policies regarding Safeguarding and Searching and Confiscation.
- The search is conducted either by the head teacher or a person authorised by them (or Deputy Head or Designated Safeguarding Lead) and one other person but only search the device if it is necessary

- The search should normally be conducted by a member of the same gender as the person being searched. However if the image being searched for is likely to be of a different gender to the person 'in possession' then the device should only be viewed by a member of the same gender as the person whose image it is.
- If any illegal images of a young person are found the head teacher or Designated Safeguarding Lead (DSL) will discuss this with the Police

The Association of Chief Police Officers (ACPO) advise that as a general rule it will almost always be proportionate to refer any incident involving 'aggravated' sharing of images to the Police, whereas purely 'experimental' conduct may proportionately dealt with without such referral, most particularly if it involves the young person sharing images of themselves.

'Experimental conduct' commonly refers to that shared between two individuals (e.g. girlfriend and boyfriend) with no intention to publish the images further. Coercion is not a feature of such conduct, neither are requests for images sent from one person to multiple other young persons.

Any conduct involving, or possibly involving, the knowledge or participation of adults should always be referred to the police.

If an 'experimental' incident is not referred to the Police, the reasons for this should be recorded in the school's 'Safeguarding Incidents Log'.

Always put the young person first. Do not search the device if this will cause additional stress to the child/student/person whose image has been distributed. Instead rely on the description by the young person, secure the device and contact the Police.

Never…

- Search a mobile device even in response to an allegation or disclosure if this is likely to cause additional stress to the child/student/young person UNLESS there is clear evidence to suggest not to do so would impede a police inquiry.
- Print out any material for evidence
- Move any material from one storage device to another

Always…

- Inform and involve the Designated Safeguarding Lead so they are able to take any necessary strategic decisions.
- Record the incident. The Designated Safeguarding Lead will employ a systematic approach to the recording of all safeguarding issues
- Act in accordance with school safeguarding search and confiscation policies and procedures

If there is an indecent image of a child on a website or a social networking site then the Designated Safeguarding Lead will report the image to the site hosting it. Under normal circumstances the team would follow the reporting procedures on the respective website; however, in the case of a sexting incident involving a child or young person where it may be felt that they may be at risk of abuse then the DSL will report the incident directly to CEOP www.ceop.police.uk/ceop-report, so that law enforcement can make an assessment, expedite the case with the relevant provider and ensure that appropriate action is taken to safeguard the child.

Appendix 'Class Blog trial'

Aims and Objectives

Whilst blogging has been around for 10+ years, more and more schools are now giving their pupils a voice and an audience through blogging. These are mainly in the form of class blogs but can also be in the form of project blogs or individual pupil blogs. Whilst there are many blogging platforms, Wordpress (edublogs) is the most popular for educational needs. This policy will outline the safe management of setting up and running a blogging platform. A successful blog can:

→ Safely give your pupils a wider audience for their learning.

→ Encourage reluctant learners to participate and succeed

→ Allow pupils to receive feedback safely from many different people

→ Allow your pupils to peer assess each other's learning

→ Encourage parental engagement

→ Promote your pupils' learning across the globe

Online Safety

Blogging involves pupils working on a blog whilst in school and also at home. To be able to post, pupils need to log into the blog either using an individual sign in or a class sign in. The advantages of individual sign in is that this gives more ownership to each pupil. Most blog platforms allow accounts to have different permissions. Subscriber is the lowest level that allows a user to post. A subscriber can submit a post for review, however, this will need to be authorised by the admin before it appears on the blog. The 'Subscriber' permission level is recommended for Primary/Elementary School. Any other permission level above that of 'Contributor' will allow posts to be viewable as soon as the pupil clicks 'Submit'.

The class teachers are 'administrators'. They are fully in charge of the blog and screen everything that is submitted for posting.

Each pupil will eventually have a unique log in has been told to keep this private, with only the class teacher (administrator of the blog) having record of the log in details. If a pupil or parent thinks their log in needs changing, this can be done in the 'profile' setting on the dashboard. Parents and pupils are to contact the named admin should this need clarifying.

Blog Rules:

Using a blog safely is the most important thing about being a blogger. The following rules, if followed, will minimise any risks and will ensure that you will stay safe whilst blogging.

Don'ts:

1. Never give away any personal information about your location or identity.
2. Don't post pictures of yourself without specific permission from your teacher or parents.
3. Never give out your log in details to anyone.
4. Don't use text language in your posts
5. Never use someone's name in a comment, use their initials.

Do's:

1. If you receive a comment, it is polite to respond, say thank you and reply to a question if they have left one.
2. Comment on other people's posts too. Blogging is about commenting and posting!
3. If your post doesn't appear straight away, your teacher might be busy, do be patient.
4. Try to post about things that your audience would like to read.
5. If you see anything that shouldn't be on your screen, do tell your teacher or parents immediately.
6. Do visit other class blogs regularly to read and comment. This helps people come back to your blog.
7. Try to show off your best work/writing whilst blogging and use the tips people suggest to you to improve.
8. Remember, your username is your screen name (intitaltps e.g. mctps) and include key words specific to your post.

The Role of the Blog Admin/Teacher:

The blog admin is the class teacher. This responsibility as gatekeeper is key to ensuring safety for the pupils using the blog. The following guidelines should be followed if a successful flowing blog is to be achieved:

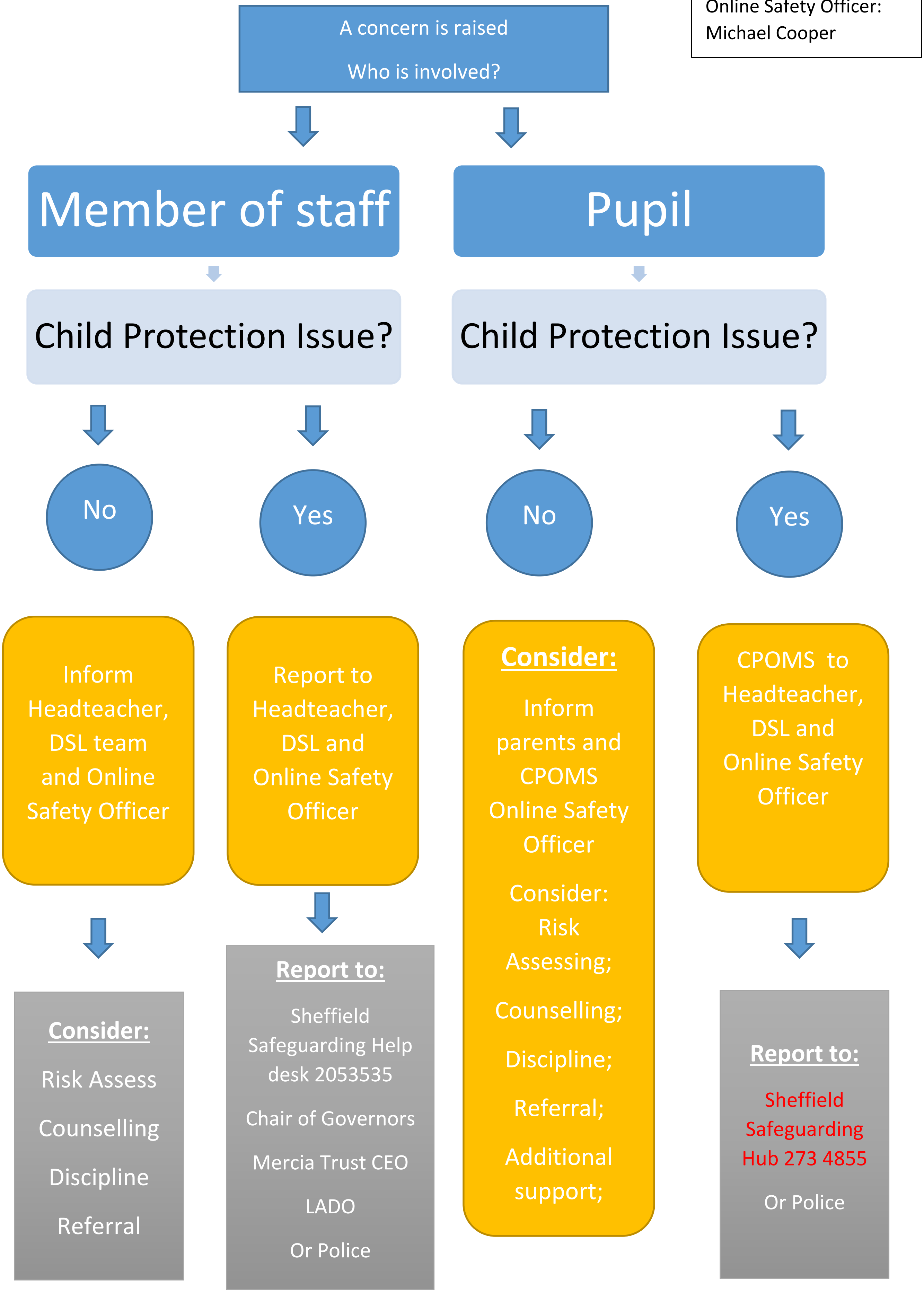
1. Visit the blog regularly. It is better to visit short and often than catching up once a week. Your bloggers will appreciate comments and posts being approved quickly!
2. If you use a shared computer, log out at the end of each session.
3. Promote the links on the class blog to the parents and the wider community. Twitter is a great way to promote a blog.
4. A blog can take a while to gather momentum and an audience. Be patient... the audience will come!
5. Your users will need to log in. For a quick solution, you can have one Username and Password for your class to get posts on the blog. However, for older pupils of 7+ they are more than capable of having their own log in.
6. The safest permission setting for your blogger is 'Subscriber'. This will allow them to log in and post but the blog admin will need to approve each post.
7. Mention the blog in assemblies and have it on display at parent evenings or school events, a blogging culture will soon be established!
8. Make sure each blog looks different in your school. This will help keep the interest high for the pupils from year to year.

Visit other blogs regularly and promote these to your class through links on your blog. What goes around comes around with blogging and strong loyal communities will form quickly.

Designated Safeguarding Team: Ben Paxman, Chris Atkinson, Coralie Corrin

Online Safety Officer: Michael Cooper

Inappropriate Activity Flowchart (At a Glance)



A concern is raised

Who is involved?

Member of staff

Child Protection Issue?

No

Inform Headteacher, DSL team and Online Safety Officer

Consider:

Risk Assess

Counselling

Discipline

Referral

Yes

Report to Headteacher, DSL and Online Safety Officer

Report to:

Sheffield Safeguarding Help desk 2053535

Chair of Governors

Mercia Trust CEO

LADO

Or Police

Pupil

Child Protection Issue?

No

Consider:

Inform parents and CPOMS Online Safety Officer

Consider: Risk Assessing;

Counselling;

Discipline;

Referral;

Additional support;

Yes

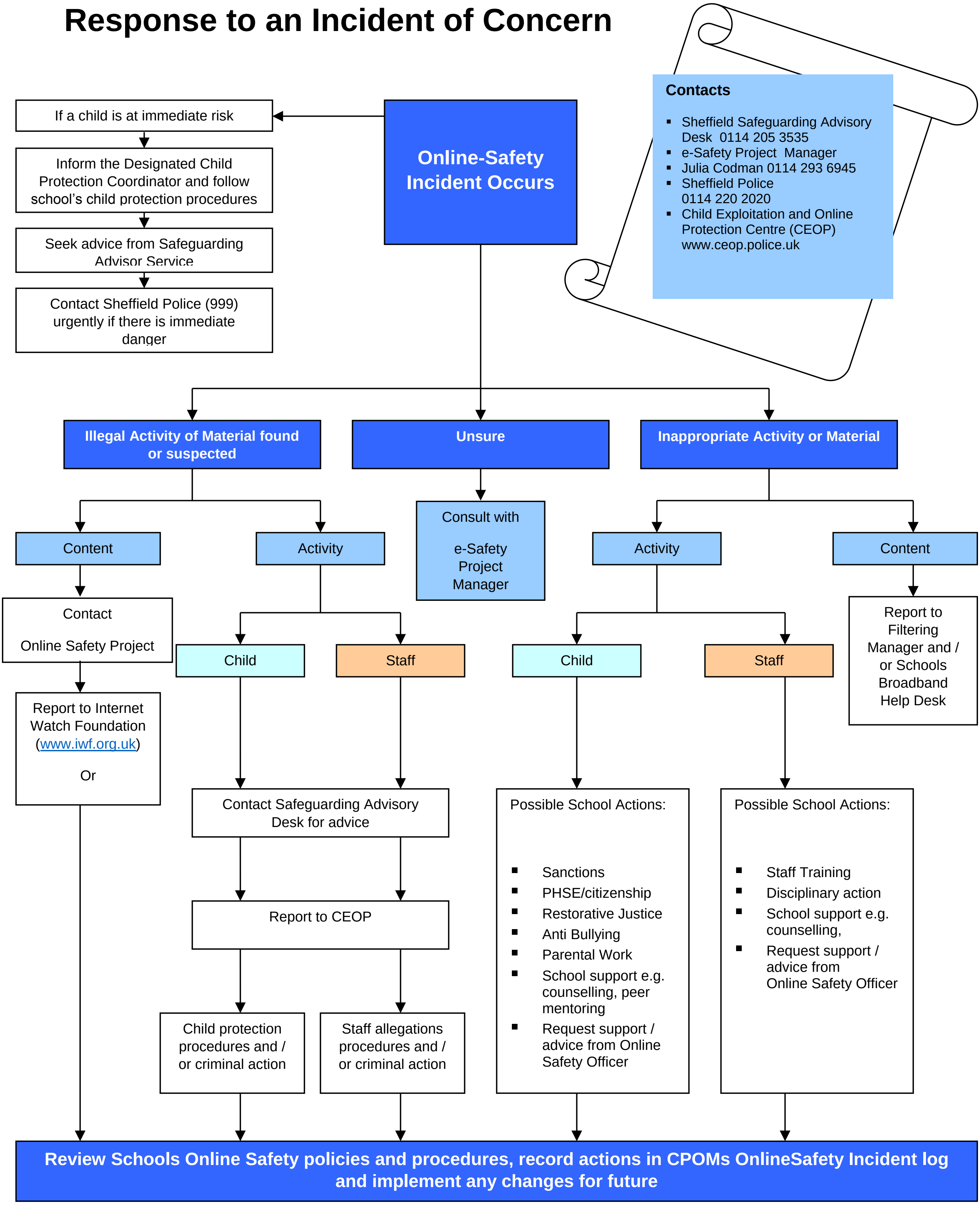
CPOMS to Headteacher, DSL and Online Safety Officer

Report to:

Sheffield Safeguarding Hub 273 4855

Or Police

Response to an Incident of Concern



Contacts

- Sheffield Safeguarding Advisory Desk 0114 205 3535
- e-Safety Project Manager
- Julia Codman 0114 293 6945
- Sheffield Police 0114 220 2020
- Child Exploitation and Online Protection Centre (CEOP) www.ceop.police.uk

Online-Safety Incident Occurs

If a child is at immediate risk

Inform the Designated Child Protection Coordinator and follow school's child protection procedures

Seek advice from Safeguarding Advisor Service

Contact Sheffield Police (999) urgently if there is immediate danger

Illegal Activity of Material found or suspected

Content

Contact

Online Safety Project

Report to Internet Watch Foundation (www.iwf.org.uk)

Or

Activity

Child

Staff

Contact Safeguarding Advisory Desk for advice

Report to CEOP

Child protection procedures and / or criminal action

Staff allegations procedures and / or criminal action

Unsure

Consult with

e-Safety Project Manager

Inappropriate Activity or Material

Activity

Child

Possible School Actions:

- Sanctions
- PHSE/citizenship
- Restorative Justice
- Anti Bullying
- Parental Work
- School support e.g. counselling, peer mentoring
- Request support / advice from Online Safety Officer

Staff

Possible School Actions:

- Staff Training
- Disciplinary action
- School support e.g. counselling,
- Request support / advice from Online Safety Officer

Content

Report to Filtering Manager and / or Schools Broadband Help Desk

Review Schools Online Safety policies and procedures, record actions in CPOMs OnlineSafety Incident log and implement any changes for future