



Online Safety Policy

Date: October 2023

Date ratified:	16/10/23
Author/Reviewer:	Ben Paxman
Date for Review:	October 2024

Totley Primary School Online Safety Policy

Policy Statement

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

User: refers to staff, governing body, school volunteers, children, 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: Children, all staff, governing body, parents

Aim

At Totley Primary School, we recognise that it is our responsibility to keep children safe.

Our Safeguarding and Online Safety policies outline how we keep children safe and ensure children leave Totley Primary School with the knowledge and understanding of how to keep themselves and others safe.

We use our values of ROAD as a driver:

Relationships - positive relationships provide a true sense of belonging for all of our staff community.

Outcomes - high expectations drive all children to aspire to achieve exceptional outcomes across and beyond.

Attitudes - through a culture of learning, children are lifelong, self-motivated learners with the resilience to embrace future challenges.

Development - nurture the personal growth of well-rounded and balanced citizens with a deep-rooted appreciation of British Values.

Policy Purpose

Safeguarding is everyone's responsibility. 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 at least annual basis, or in response to emerging needs, 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 child 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 safely 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. 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 who have access to and are users of school Information and Communication Technology (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 bullying or other Online Safeguarding incidents covered by this policy, which may take place out of school, but are 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 managed and how parents/carers are informed of inappropriate Online Safety behaviours that take place in and out of school.
- **Keeping Children Safe in Education (2023 update)** 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 2023 update**
- **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”. The Prevent Duty guidance is followed.

Contents

Teaching and Learning	6
Children with special educational needs (see also SEND policy)	6
Roles and Responsibilities	6
Governing Body	6
Headteacher and Senior Leaders	7
Designated Safeguarding Lead/Team	7
Online Safety Officer	8
IT Technical Support Staff	8
All Staff	9
All staff, Governors, workplace students and volunteers	10
Parents and Carers	10
Children of Totley Primary	11
Education	11
Children	11
Governors	12
All Staff (including Governors)	13
Parents/Carers	13
Use of digital and video images	13
Managing IT systems and access: Technical infrastructure and equipment	14
Communication Technologies	17
Responding to misuse	19
Social Networking	19
Google Classroom	20
Aims and Objectives	20
The Role of the Google Classroom - Admin:	20
The Role of the Google Classroom Teacher:	20
The Role of the Google Classroom pupil:	21
Feedback via messages	21
Feedback via live videos (Google Meets)	21
Appendix1 : Sexting	22
Appendix 2: Inappropriate Activity Flowchart (At a Glance)	25
Appendix 3: Response to an Incident of Concern	26

Teaching and Learning

Computing 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 Computing is an important tool in both the society we live in and in the process of teaching and learning. Children use computing tools to find, explore, analyse, exchange and present information responsibly, creatively and with discrimination. They learn how to employ computing skills 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 computing so that they can develop the skills, knowledge and understanding which enables them to use appropriate computing resources effectively as powerful tools for teaching & learning.

Children with special educational needs (see also SEND policy)

We believe that all children have the right to access 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 Computing Totley Primary School Computing Policy and computing curriculum for some children. We teach Computing to all children. Computing forms part of the National Curriculum to provide a broad and balanced education for all children. Through the teaching of 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, 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, screen printouts and access to technology for larger pieces of writing.

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 Computing 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 training 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 of children's lives. Therefore, the Designated Safeguarding Lead/Team will always be fully involved where online safety is concerned.

Please refer to the 2023 Safeguarding Policy for full contact details of the designated safeguarding team.

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 with the Data Protection Act 2018.
- They understand the risks and dangers regarding access to inappropriate online content and contact with adults and strangers.
- Any concerns about harmful content logged / reported by the school's firewall system are acted upon in a timely and appropriate manner
- 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.

The Headteacher, the Online Safety Officer, the Governing Body and the Trust IT Lead are responsible for ensuring that the latest DFE digital and technology standards are met, including those relating to filtering and monitoring, broadband and cyber security. They are fully aware of the vital role these play in protecting staff and pupils from potentially harmful and inappropriate online material, as well as protecting school systems from hacking, exploitation or attack.

Online Safety Officer

The day-to-day management of online safety is devolved to the Online Safety Officer and will involve professional dialogue and meetings when appropriate with the Designated Safeguarding Lead. **Please refer to the 2023 Safeguarding Policy for full contact details of the online safety officer.**

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, Trust 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 Trust IT Technical Support and the Headteacher.
- Make themselves aware of any reporting function with technical online safety measures, i.e. internet filtering reporting function; liaise with the Headteacher/DSL and responsible governor to decide what reports may be appropriate for viewing.

IT Technical Support Staff

Technical support staff are responsible for ensuring that:

- They are fully aware of their role and responsibilities at Totley Primary School.
- They understand, and contribute towards the school's Online Safeguarding policies and guidance.
- They understand and adhere to the staff Acceptable IT Use policy
- They 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 measures are 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.
- Any loaned devices have the same level of protection as in-school devices.

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 IT 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.
- Computers are locked when not in use and are mindful of screens in classrooms where sensitive information could be inadvertently displayed.
- Digital communications with parents or children, e.g. phones, email, social media are always made through school based systems where possible. If using a personal device is the only option, staff must disable Caller ID so that their personal number remains anonymous.
- Online Safety messages are embedded across learning activities across all areas of the curriculum
- Children are supervised and guided in school, when engaged with learning activities that involve online technology
- Remote working guidance is communicated clearly and promoted regularly, especially relating to online conduct and safety.

- Children are taught and are aware of research skills and some of the issues that relate such as copyright laws.

All staff, Governors, workplace 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:

- Adhere to the Acceptable Use of IT Policy
- 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.
- 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' evenings, and other communication such as letters, the school will keep parents up to date with new and emerging online safety risks and will involve parents in strategies to ensure that children 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.
- Ensure that any school devices loaned to be used at home are used for appropriate educational purposes.

Children of Totley Primary

As well as supporting their online safety in school through engaging and purposeful lessons across the curriculum, parents and children also have their own roles and responsibilities (which they are taught) 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

Children

Whilst regulation, technical solutions and filtering are very important, their use must be balanced with the education of pupils to take a safe and 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 the Personal Development curriculum (as part of the RSHE curriculum).
- 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.
- 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.

Governors should also regularly review the effectiveness of school filters and monitoring systems. They should ensure that the leadership team and relevant staff are:

- Aware of and understand the systems in place
- Manage them effectively
- Know how to escalate concerns when identified.

All Staff (including Governors)

Effective and continuous professional development for our staff is a key part of our practice. 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 Mercia Social Media Use policy.
- All staff will be regularly made aware of their individual responsibility for Online Safety and relevant staff to report to in case of concern or misuse.
- This Online Safety policy and its updates will be presented and discussed by staff during staff meetings or INSET days.
- The Online Safety Officer and Designated Safeguarding Lead/Team will provide advice, guidance and training as required as well as perform audits on staff Online Safety training needs.

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.

Totley Primary School will share information with parents / carers about

- What systems we have in place to filter and monitor online use
- What we are asking children to do online, including sites they will be asked to access
- Who from school (if anyone) their child is going to be interacting with online.

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 policies 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.
- Children 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 images. Staff will be aware of those pupils for whom 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.

Managing IT 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.

- KS2 children will have their own login and password for the school network 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.
- FS2 and KS1 children will have a generic class password as they will be monitored in small groups.
- All children have their own Google login details in order to access Google Classroom.
- 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 but use of memory sticks is avoided if at all possible.
- 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 and DSL receive daily Smoothwall notifications, including the immediate notification of potential concerns to support the checking, tracking and investigating of monitoring in regards to safe Internet access by pupils and staff. This will help inform and alert school of any safeguarding issues.
- If users discover a website with inappropriate content, it should be reported straight to the Safeguarding Team.
- The filtering and monitoring process will be regularly reviewed for its effectiveness.

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.
- The message that passwords should not be disclosed is made clear to staff and children
- 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 by the Trust IT team.
- 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

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 2018 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 safekeeping 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	At certain times	With permission	Not allowed
Mobile phones in school		*					*	
Use phones in lessons		*						*
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 reasons				*				*
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. Any new service will be risk assessed by both the online safety officer and Headteacher, before being permitted.

- Gmail – used by staff to email
- Twitter – used by the school as a broadcasting service
- Vimeo – a closed area to upload videos.

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.

Google Classroom

Aims and Objectives

Google Classroom is an online platform service which has the capabilities for 2-way communication between teachers and children, including the sharing and uploading of work and providing feedback. This platform is a closed network and will be used for the sharing of regular homework, as well as remote learning, should this be a necessity for any reason.

With the use of Google Classroom, Totley Primary School will:

- Safely set work which runs alongside learning in the classroom to ensure fluidity and meaningfulness of learning.
- Provide every opportunity for children to complete work.
- Allow pupils to receive feedback safely.
- Promote pupils' learning.

The Role of the Google Classroom - Admin:

The Google Classroom Admin has access to all classrooms set up on Google Classroom, and can provide comments, feedback and advice to all. This is a vital role, especially as the platform is being established, or with new users, to provide support for teachers, children, parents and carers.

The Role of the Google Classroom Teacher:

The running of Google Classroom will be the responsibility of the class teacher/year group team and will involve:

- Uploading work onto Google Classroom for the children.
- Providing appropriate feedback in the form of online feedback messages (see private message section), and also live lesson feedback sessions if applicable (see live lesson feedback section).
- Using this information to make formative assessment decisions on their class and individuals
- Promoting a positive learning environment.

No photos sent on Google Classroom will be downloaded onto personal devices.

The Role of the Google Classroom pupil:

The following rules, if followed, will minimise any risks and will ensure that you will stay safe whilst using. These messages will be reinforced in class, and during use.

1. Keep your log in details safe and private.
2. Use correct English when typing messages.
3. Comment and reply on the 'stream'. It's polite to respond!
4. If you don't get feedback straight away, your teacher might be busy, do be patient.
5. If you see anything that shouldn't be on your screen, do tell your teacher or parents immediately.
6. Try to show off your best work/writing and maintain the expected standard of work that would be expected in class (e.g. presentation, layout...)

Feedback via messages

Teaching staff have the capability of providing feedback to uploaded work. This is done via the 'private messaging' option in the bottom corner submitted work in the form of positive praise, encouragement or advice for next time.

This is a 2-way communication with the teacher and child account. All feedback comments are advised to be done within the working day, and not after hours.

Feedback via live videos (Google Meets)

In the unusual event of remote learning being a necessity, teaching staff also have the capability of providing live feedback, which can support children's mental well-being as well as their progress.

- Parental permission will be sought before inviting a child to a live feedback session (for those who do not give permission, private messaging feedback will be maintained).
- A planned, scheduled timetable of manageable live feedback will be created by the class teacher to ensure purposeful and manageable sessions, if this is necessary.
- Both parties will ensure the session takes place in a suitable area e.g. quiet space, suitable background.

Appendix1 : Sexting

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

Step 1 - Disclosure by a child

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

The child 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 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 need immediate support and/or protection?
- Are there other children 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 / person whose image has been distributed. Instead rely on the description by the young person, secure the device and contact the Police.

Never...

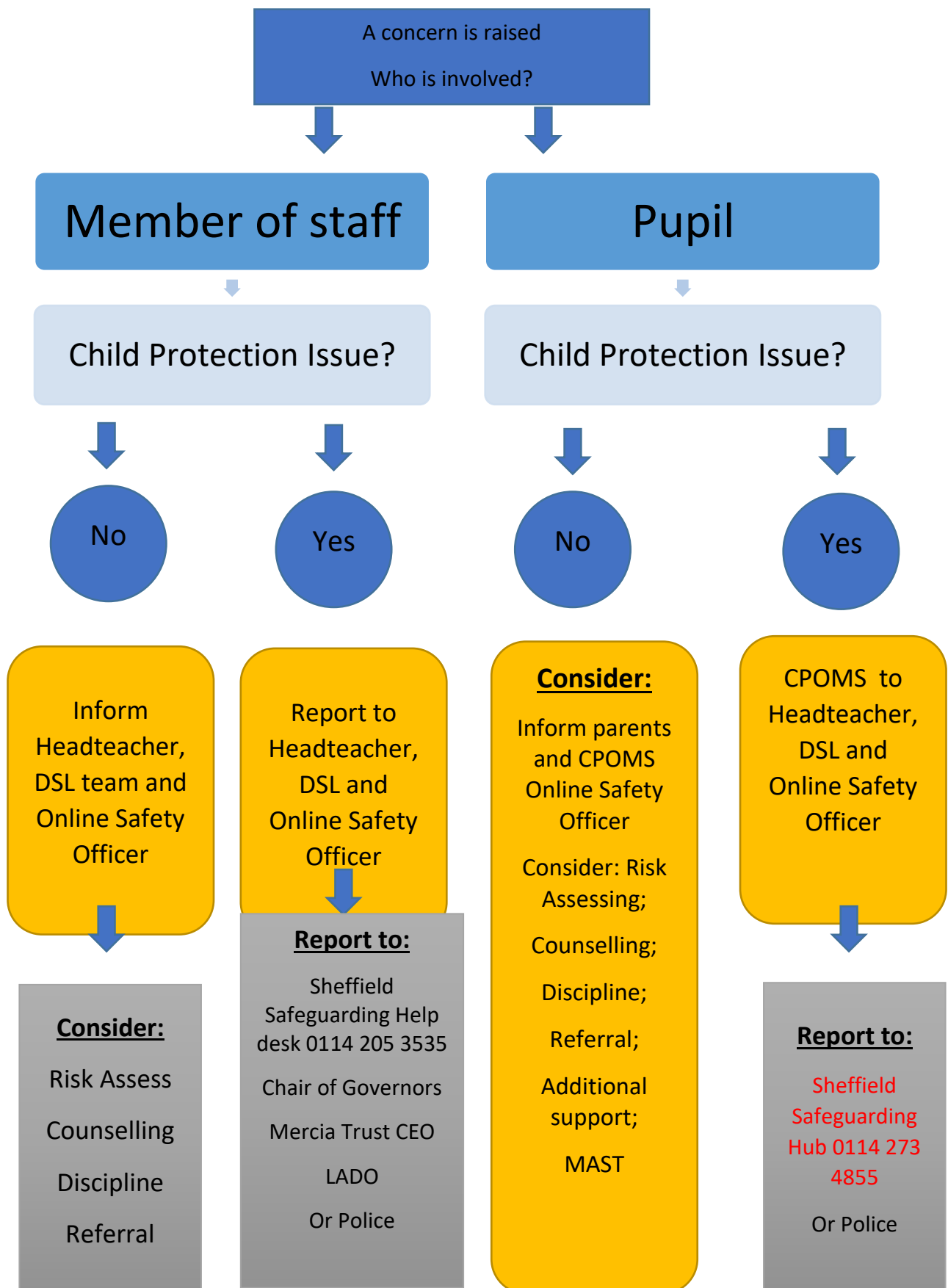
- Search a mobile device even in response to an allegation or disclosure if this is likely to cause additional stress to the child /young person UNLESS there is clear evidence to suggest not to do so would impede a police inquiry.
- Print out any material for evidence
- Move any material from one storage 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 2: Inappropriate Activity Flowchart (At a Glance)



Appendix 3: Response to an Incident of Concern

