FREMINGTON PRIMARY SCHOOL

ONLINE SAFETY POLICY

Date Adopted: October 2023
Author/owner: Tarka Learning Partnership Board of Directors
Anticipated Review: October 2024

Background/Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound (Please refer to Guidance for Safe Working Practice for the Protection of Children and Staff in Education Settings). A school online safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the Head Teacher and Governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this online safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies)., Guidance for Safe Working Practice for the Protection of Children and Staff in Education Settings

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The online safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Development / Monitoring / Review of this Policy

This online safety policy has been developed by Kate Fairbrother following discussion with the whole school community has taken place through the following:

- Staff meetings
- School website / newsletters

Development / Monitoring / Review

The implementation of this online safety policy will be monitored by the:	Leader for IT and Computing & Designated Safeguarding Lead
Monitoring will take place at regular intervals:	Termly
The Online safety Policy will be reviewed bi-annually or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	September 2023
Should serious online safety incidents take place, the following external persons / agencies should be informed:	*lightspeed filtering/ LADO/police*

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Lightspeed systems monitoring logs of internet activity (including sites visited)

Scope of the Policy

This policy applies to all members of the school community (including staff, ITE students, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school digital communication systems, both in and out of school.

The Education and Inspections Act 2006 empowers Head Teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other online safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

Roles and Responsibilities

Head Teacher and Senior Leaders:

- The Head Teacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the ~~L~~eader for IT and Computing and the Desiganted Sfaeguarding Lead.
- The Head Teacher are responsible for ensuring that the Leader for IT, the DSL and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant
- The Head Teacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. Monitoring TalkStraight records and reports to be shared responsibility between HT and DSL.
- The Senior Leadership Team will receive regular (daily) monitoring reports from the school filtering and monitoring system (TalkStraight) and have an agenda item each week related to safeguarding.

- The Head Teacher and another member of the Senior Leadership Team (DSL) should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (See flow chart on dealing with online safety incidents – "Responding to incidents of misuse" and relevant Local Authority HR / disciplinary procedures)
- The Head Teacher will determine who will deal with any investigations, actions and sanctions following an online safety incident.

Leader for IT and Computing

- leads online safety across the school
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the relevant bodies
- liaises with school ICT technical staff
- receives reports of online safety incidents through the senior leadership team and uses them to inform future online safety developments
- attends relevant meetings / committee of Governors
- reports regularly to Senior Leadership Team

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school online safety Policy and practices
- they report any suspected misuse or problem to the Head Teacher for investigation / action / sanction
- all digital communications with pupils should be on a professional level and only carried out using official school systems
- Online safety issues are embedded in all aspects of the curriculum and other pupils understand and follow the school online safety and acceptable use policy
- pupils have a good understanding of research skills and know the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead

- should be trained in online safety issues and be aware of the potential for serious child protection issues to arise from:
    - sharing of personal data
    - access to illegal / inappropriate materials
    - inappropriate on-line contact with adults / strangers
    - potential or actual incidents of grooming
    - cyber-bullying

Students / pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile devices and digital cameras. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through induction meetings, parents' evenings, newsletters, letters, website / VLE and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- mobile phone use within the school areas
- access to parents' sections of the school website

Policy Statements

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety programme is provided as part of Computing / PHSE / other lessons and is regularly revisited. Key online safety messages are reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils should be taught in lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils should be helped to understand and encouraged to adopt safe and responsible use both within and outside school
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- In lessons where internet use is pre-planned, it is best practice that students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students / pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

Education – parents / carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters and website information
- Reference / signposting as relevant

Education & Training – Staff

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

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.
- The Leader for IT and Computing will receive regular updates through attendance at training sessions and by reviewing guidance documents released by relevant organisations.
- This Online safety policy and its updates will be presented to and discussed by staff in staff meetings.
- The Leader for IT and Computing will provide advice / guidance / training to individuals as required.

Technical – infrastructure / equipment, filtering and monitoring

The school and Trust (TLP) will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- School ICT systems will be managed in ways that ensure that the school meets the online safety technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems**.** Details of the access rights available to groups of users will be recorded by the IT Technician (Aprox) and will be reviewed, at least annually, by their manager.
- Pupils will all log on using an individual username and password.
- The ICT Technician is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Users will be made responsible for the security of their username and password must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Any filtering issues should be reported immediately.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. Requests from staff for sites to be removed from the filtered list will be considered by the IT Technician and the Headteacher.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. Including keeping staff up to date with training of what to do in case of a threat.

- ITE students, supply teachers and visitors to the school will be able to use a guest log on to allow them access to the school system.
- Personal use of laptops at home is not permitted. They are to be used for school use only when taken away from the school premises.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement, and through training.
- Any member of staff wishing to add software to any school machines must first seek the permission of the Leader for IT and Computing or IT Technician
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks) by users on school devices. Removable media devises will be phased out in the near future.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data can not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (See School Personal Data Handling Policy below) This includes using initials rather than names in emails, the use of the Egress secure email system for named pupils, as well as encrypting iPads / devices to take them off site.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with sharing images and with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website / social media / local press.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can be published without the permission of the student / pupil and parents or carers as long as it does not contain the name of the child.

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- on the TLP web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas

- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)
- on the school assessment software (Class DoJo, Bromcom)

Data Protection

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 is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

- All personal data will be fairly obtained and held in accordance with the Data Protection Policy

- It has a Data Protection Policy (available on request from school)

- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)

- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)

- Risk assessments are carried out

- It has clear and understood arrangements for the security, storage and transfer of personal data

- Data subjects have rights of access and there are clear procedures for this to be obtained

- There are clear and understood policies and routines for the deletion and disposal of data

- There is a policy for reporting, logging, managing and recovering from information risk incidents

- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties

- There are clear policies about the use of cloud storage / cloud computing which ensure that such data transfer / storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

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

- the data must be encrypted and password protected
- the device must be password protected

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

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	√							√ * Kept in School Office if permitted
Use of mobile phones in lessons (NO PHOTOGRAPHS)		√ Offsite trips- for contact with school)						√
Use of mobile phones in teachers' social time away from classrooms	√ Staff room and office areas only							√
Taking photos on personal mobile phones or other camera devices				√				√
Use of other mobile devices e.g. tablets, gaming devices.				√				√
Use of school email for personal emails			√					√
Use of messaging apps		√						√
Use of social media				√				√
Use of blogs		√					√	

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

- The official school email service may be regarded as safe and secure and is monitored.
- Users should be aware that email communications may be monitored

- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of and communication that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such communication
- Any digital communication between staff and students / pupils or parents / carers must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media – Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

Personal Use:

- Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to proactively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and those users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

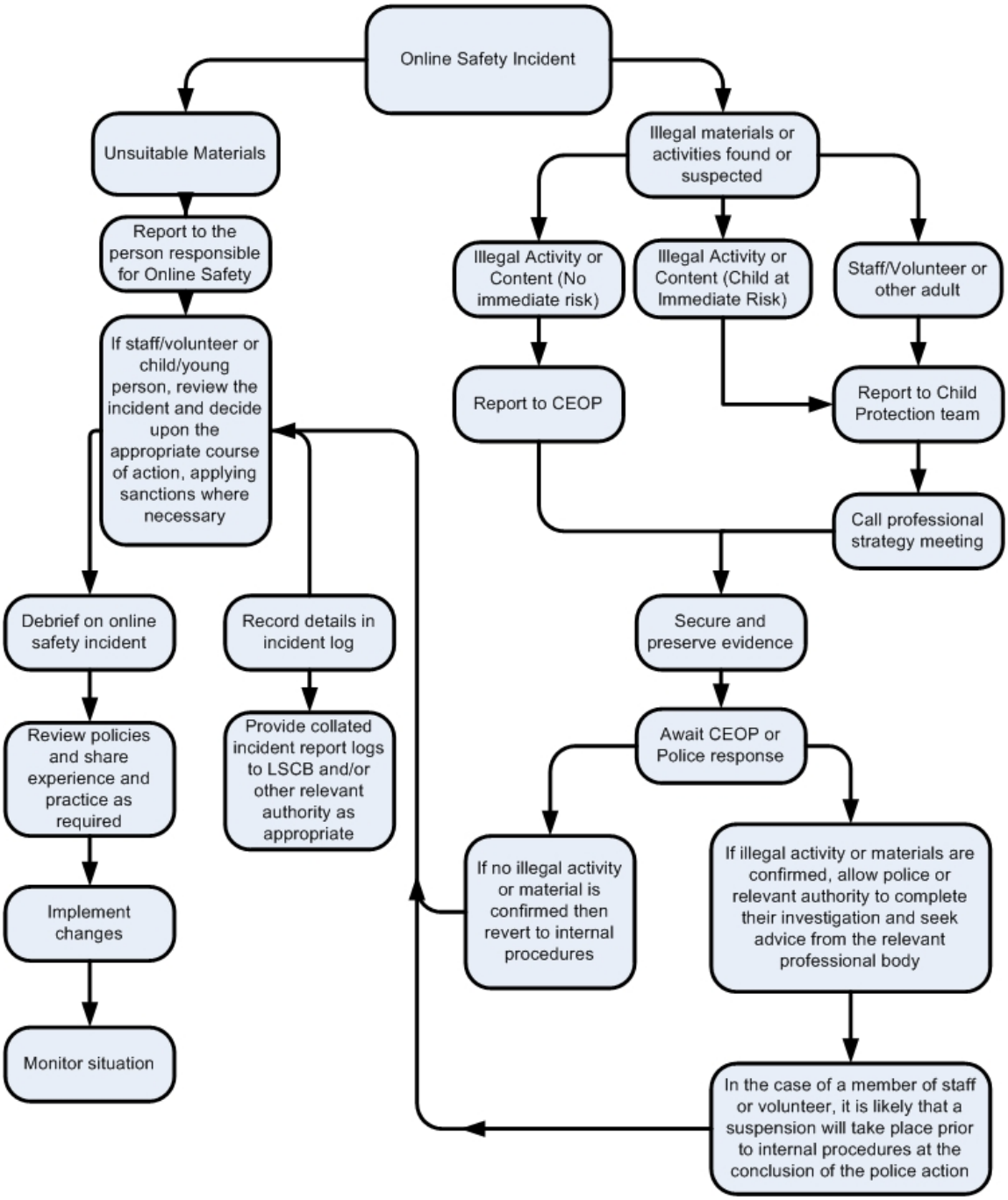
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child sexual abuse images - The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**					√
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					√
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					√
	Criminally racist material in UK - to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					√
	Pornography				√	
	promotion of any kind of discrimination				√	
	Promotion of racial or religious hatred				√	
	Threatening behaviour, including promotion of physical violence or mental harm				√	
	Any other information which may be offensive 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					√	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by TME, Lightspeeed and / or the school					√	

Infringing copyright				√	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)				√	
Creating or propagating computer viruses or other harmful files				√	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				√	
On-line gaming (educational)			√		
On-line gaming (non-educational)				√	
On-line gambling				√	
On-line shopping / commerce			√		
File sharing		√			
Use of social media				√	
Use of video broadcasting e.g. You tube **NOTE: Videos must be viewed and checked for suitability prior to use in class.**	√				
Use of messaging apps	√				

Responding to incidents of misuse

This guidance is intended for use when members of staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet

access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).

- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by Local Authority / Academy Group or national / local
  - organisation (as relevant).
  - Police involvement and/or action
- If content being reviewed includes images of Child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
  - incidents of 'grooming' behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - promotion of terrorism or extremism
  - other criminal conduct, activity or materials

- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the *school* and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

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

Students / Pupils — Actions / Sanctions

Incidents:	Refer to class teacher	Refer to Assistant Head	Refer to Head teacher	Refer to Police	Refer to technical support staff for action re filtering /	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanctions per behaviour policy
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).									
Unauthorised use of non-educational sites during lessons	√	√	√	*	√	√	√	√	√
Unauthorised use of mobile phone / digital camera / other mobile device	√	√	√	*	√	√	√	√	√

Unauthorised use of social media/ messaging apps / personal email	√	√	√	*	√	√	√	√	√
Unauthorised downloading or uploading of files	√	√	√	*	√	√	√	√	√
Allowing others to access school network by sharing username and passwords	√	√	√	*	√	√	√	√	√
Attempting to access or accessing the school network, using the account of a member of staff or another pupil's account	√	√	√	*	√	√	√	√	√
Corrupting or destroying the data of other users	√	√	√	*	√	√	√	√	√
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	√	√	√	*	√	√	√	√	√
Continued infringements of the above, following previous warnings or sanctions	√	√	√	*	√	√	√	√	√
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	√	√	√	*	√	√	√	√	√
Accidentally accessing offensive or pornographic material and failing to report the incident	√	√	√	*	√	√			
Deliberately accessing or trying to access offensive or pornographic material	√	√	√	*	√	√	√	√	√
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	√	√	√	*	√	√	√	√	√
Using proxy sites or other means to subvert the school's filtering system	√	√	√	*	√	√	√	√	√

Staff

Actions / Sanctions

Incidents:	Refer to SLT	Refer to Head teacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	√	√	√	√	√	√	√	√
Inappropriate personal use of the internet / social media / instant messaging	√	√			√	√		
Unauthorised downloading or uploading of files	√	√			√	√		

Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	√	√				√		
Careless use of personal data e.g. holding or transferring data in an insecure manner	√	√			√			
Deliberate actions to breach data protection or network security rules	√	√	√	√	√	√	√	√
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	√	√	√	√	√	√	√	√
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	√	√	√	√	√	√	√	√
Using personal email / social networking / instant messaging / text messaging to carry out digital communications with students / pupils		√				√	√	√
Actions which could compromise the staff member's professional standing	√	√	√			√	√	√
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	√	√				√	√	√
Using proxy sites or other means to subvert the school's filtering system	√	√	√		√	√		
Accidentally accessing offensive or pornographic material and failing to report the incident	√	√						
Deliberately accessing or trying to access offensive or pornographic material	√	√	√	√	√	√	√	√
Breaching copyright or licensing regulations	√	√				√		
Continued infringements of the above, following previous warnings or sanctions	√	√	√	√	√	√	√	√

Acknowledgements

Fremington Primary School would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School Online Safety Policy Template:

- Members of the SWGfL Online Safety Group and the SWGfL Online Safety Conference Planning Group
- Tarka Learning Partnership
- Devon and Cornwall Police
- Representatives of SW Local Authorities
- Plymouth University Online Safety
- Regional Broadband Grids