ONLINE SAFETY POLICY

School Mission Statement

At Garstang Community Primary School we treasure each and every one of our pupils. We create inspirational learning opportunities in a vibrant, supportive environment in which our pupils grow together and are excited about their future in an ever changing world.

Aims

- We recognise the individuality of each of our pupils and nurture them emotionally, socially, spiritually, morally and culturally.
- We create inspirational learning opportunities within an exciting curriculum which equips our pupils with the skills and knowledge needed to be successful in a dynamic world.
- Our pupils become enterprising, inquisitive young people with high expectations of themselves and a lifelong love of learning.
- We develop strong partnerships with parents, creating an atmosphere of mutual trust, and working together to provide the very best for our pupils.
- We create opportunities for our pupils to be active participants in the local and global communities and to develop an understanding of their place in the world.

Policy created: January 2015

Date reviewed	Changes made	Signed
September 2017	Updated wording in line with new guidance and new uses of technology, altered Community User Responsibilities and inclusion of incident reporting procedures	SN
March 2018	Included Online Safety Committee and general review by new Computing lead.	RW
November 2018	Edited wording to mobile phone usage in school and whilst out of school (in school time with children). Reviewed all areas as per Online Safety committee meeting.	RW
October 2019	Policy reviewed in INSET – no changes made.	Whole staff
September 2020	Updated on curriculum about teacher's responsibility to teach an online safety lesson at least once per half term.	RW

Garstang Community Primary School

Online Safety Policy

Development / Monitoring / Review of this Policy

This Online Safety Policy has been written as part of a consultation process involving the following people:

- Headteacher / Senior Leaders
- Computing Co-ordinator
- Staff – including Teachers, Support Staff, Technical Manager
- Governors
- Parents and Carers
- Community users

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

Schedule for Development / Monitoring / Review

This online safety policy was approved by the Governing Body on:	January 2015
The implementation of this online safety policy will be monitored by the:	Online Safety Committee
Monitoring will take place at regular intervals:	Termly
The Governing Body will receive a report on the implementation of the Online Safety Policy generated by the Online Safety Committee (which will include anonymous details of online safety incidents) at regular intervals:	Annually
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	October 2020
Should serious online safety incidents take place, the following external persons / agencies should be informed:	LA Safeguarding Officer LA ICT Manager Police

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Surveys / questionnaires / interviews of
  - pupils / pupils
  - parents / carers
  - staff

Garstang Community Primary School

Online Safety Policy

Scope of the Policy

This policy applies to all members of The School community (including staff, pupils, volunteers, parents / carers, visitors, community users) 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 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 outside of the school, but are linked to membership of The School.

The School will deal with such incidents within this policy, following The School's associated **Anti-Bullying** and **Behaviour Policies**, and the **Sexting in Schools Guidance** (detailed in the **Whole School Policy for Safeguarding & Child Protection**) and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. Governors will receive regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- regular meetings with the Computing Co-ordinator
- regular monitoring of online safety incident logs
- regular monitoring of filtering logs
- reporting to relevant Governors

Headteacher and Senior Leaders:

- The Headteacher 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 Computing Co-ordinator.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Headteacher is responsible for ensuring that the Computing Co-ordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher 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.

- The Senior Leadership Team will receive monitoring reports from the Computing Co-ordinator when series incidents have occurred.

Computing Co-ordinator:

- leads the Online Safety Committee
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies
- 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
- works with the Headteacher to liaise with the Local Authority / relevant body
- liaises with School Technical Manager
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets regularly with Online Safety Governor to discuss current issues, review incident and filtering logs
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

Technical Manager:

The Computing Co-ordinator is responsible for ensuring that any external ICT providers carry out the following:

The external ICT providers are responsible for ensuring:

- that The School's technical infrastructure is secure and is not open to misuse or malicious attack
- that The School meets required online safety technical requirements and any Local Authority / other relevant bodies' Online Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced **Password Security Policy**, in which passwords are regularly changed.
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- that the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher and Computing Co-ordinator for investigation / action / sanction.

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 have read, understood and signed the **Staff Acceptable Use Policy**
- they report any suspected misuse or problem to the Headteacher / Computing Co-ordinator for investigation / action / sanction
- all digital communications with pupils / parents / carers 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 activities
- pupils understand and follow the **Online Safety** and **Pupil Acceptable Use Policies**
- 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 they follow The School's **Inappropriate Content Process** (Appendix I) if dealing with any unsuitable material that is found in internet searches

Child Protection Officer:
Should be trained in online safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Online Safety Committee:
The Online Safety Committee provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the **Online Safety Policy**. Membership includes the Online Safety Governor, Safeguarding Governor, Computing Co-ordinator, Technical Manager, a parent representative, teaching assistant and 4 pupil representatives (Digital Leaders) where appropriate. The group will also be responsible for regular reporting to the Governing Body.

Members of the Online Safety Committee will assist the Computing Co-ordinator with:

- the production / review / monitoring of the school online safety policies / documents.
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the pupils about the online safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool

Pupils:

- are responsible for using the school digital technology systems in accordance with the **Pupil Acceptable Use Policy for Key Stage 1 and Key Stage 2**.
- 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 policies on the use of mobile devices and digital cameras. They should also know and understand 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 parents' evenings, newsletters, letters, website etc.. 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

Community Users:

Community Users who access school systems / website as part of the wider School provision will be provided with restricted access to school systems through guest logins and passwords.

Policy Statements

Education – pupils

At Garstang Community Primary School we believe that whilst regulation and technical solutions are very important when keeping pupils safe, their use must be balanced by educating pupils to take a responsible approach to the use of technology. The education of pupils in online safety is 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 across the curriculum and staff should reinforce online safety messages where possible. 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 curriculum provided as part of Computing and PHSE. This should be regularly revisited and updated. At least one online safety lesson should be planned into the Computing timetable once per half term ensuring that children have a minimum of six lessons solely dedicated to this each academic year. In addition, once every half term the computing lead will use an assembly slot for a whole school assembly on the topic of online safety.

- Pupils should be taught to be critically aware of the materials / content they access online and be guided to validate the accuracy of information.
- Pupils should be helped to understand the need for the **Pupil Acceptable Use Agreement** and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit and follow the **Inappropriate Content Process** (Appendix I) that is in place for dealing with any unsuitable material that is found in internet searches
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Manager or Computing Co-ordinator can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

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 behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material and may be unsure about how to respond.

The School will therefore seek to regularly provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site, social media
- Parents / Carers sessions
- High profile events / campaigns e.g. Safer Internet Day

Education – The Wider Community

The School aims to provide opportunities for local community groups / members of the community to gain from The School's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community
- Supporting community groups e.g. Early Years Settings, Child-minders, youth / sports / voluntary groups to enhance their online safety provision if requested.

Education & Training – Staff / Volunteers

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

- 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. It is expected that some staff will identify online safety as a training need within the performance management process.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand The School's **Online Safety Policy** and **Acceptable Use Policy**.
- The Computing Co-ordinator (or other nominated person) will receive regular updates through attendance at external training events 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 / INSET days.
- The Computing Co-ordinator (or other nominated person) will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any sub-committee / group involved in technology / online safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation.
- Participation in school training / information sessions for staff or parents.

Technical – infrastructure / equipment, filtering and monitoring

The School (working with the Technical Manager) will be responsible for ensuring that infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School technical systems will be managed in ways that ensure that The School meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of School technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.

- All staff will be provided with a username and secure password by the Technical Manager who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every academic year – see **Password Security Policy** for more details.
- The "master / administrator" passwords for the school ICT system, used by the Technical Manager and Computing Co-ordinator, must also be available to the Headteacher and kept in a secure place
- The School Technical Manager and Computing Co-ordinator are 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
- Internet access is filtered for all users through the Lightspeed Filtering System provided by the current internet provider. Content lists are regularly updated and internet use is regularly monitored. There is a clear process in place to deal with requests for filtering changes (Appendix II)
- The Technical Manager regularly monitors the activity of users on the school technical systems and users are made aware of this in the **Staff Acceptable Use Policy**.
- Users can report any actual / potential technical incident / security breach directly to the Computing Co-ordinator / Technical Manager, Headteacher or other member of the Senior Leadership Team and these will be recorded on the relevant **Online Safety Log**.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of The School systems and data. The School infrastructure and individual workstations are protected by up to date virus software.
- Temporary and limited access to school systems for "guests" (e.g. trainee teachers, supply teachers, visitors) will be provided by the Technical Manager.
- The **Staff Acceptable Use Policy** is in place regarding the extent of personal use that staff and their family members are allowed on school devices that may be used out of school.
- The **Staff Acceptable Use Policy** is in place regarding the downloading of executable files and installing programmes on school devices.
- Personal data can only be sent over the internet via the School's One Drive System.

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 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.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the GDPR). 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. These are detailed in the **Parents / Carers Use of Digital Images and Video Agreement**.
- 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
- 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.
- Written permission from parents or carers will be obtained before photographs of pupils or their work are published on the school websites, blogs or on project display boards as detailed in the **Parents / Carers Use of Digital Images and Video Agreement** signed by parents or carers at the start of the year.

GDPR

Personal data will be recorded, processed, transferred and made available according to the GDPR 2016 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.

Garstang Community Primary School

Online Safety Policy

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 in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the GDPR
- 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 GDPR 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 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.
- Personal data is not stored on any memory sticks or other removable media and only stored on the School's One Drive System.

When personal data is stored on any portable computer system:

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

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 benefits of using these technologies in school for education outweighs their risks / disadvantages:

	Staff and other adults				Pupils			
Communication Technologies	**Allowed**	**Allowed at certain times**	**Allowed without disturbing others**	**Not allowed**	**Allowed**	**Allowed at certain times**	**Allowed with staff permission**	**Not allowed**
Mobile phones may be brought to school	✓						✓[1]	
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time			✓					✓
Taking photos on mobile phones / personal devices				✓				✓
Use of personal mobile devices e.g. tablets, gaming devices				✓				✓
Use of personal email addresses in school or on school network	✓							✓
Use of school email for personal emails	✓							✓
Use of messaging apps on school devices				✓				✓
Use of social media on school devices for school purposes	✓							✓
Use of blogs for school purposes	✓							✓

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 are monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication regarding School business between staff and parents / carers (email, chat etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media 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.

[1] Under certain exceptional circumstances and only agreed by the Headteacher

- 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 and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools 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 or local authority 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 limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; GDPR; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

When using social media, School staff should ensure that they follow the guidelines set out in the **Staff Acceptable Use Policy**.

Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that 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**					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	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					X

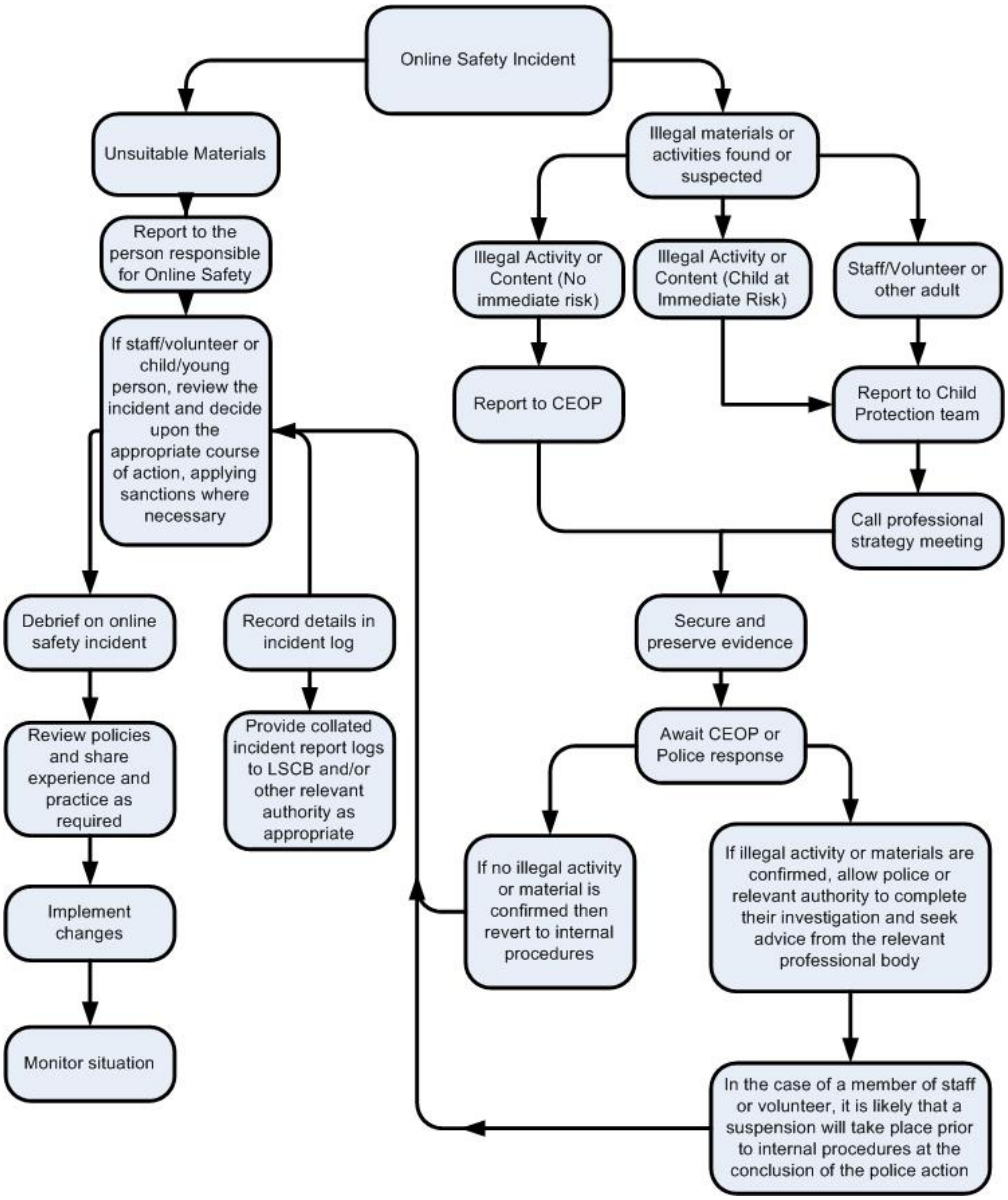
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright						X
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)	X					
On-line gaming (non educational)		X				
On-line gambling					X	
On-line shopping / commerce		X				
File sharing	X					
Use of social media on school devices		X				
Use of messaging apps on school devices					X	
Use of video broadcasting e.g. Youtube			X			

Responding to incidents of misuse

This guidance is intended for use when 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).

Illegal Incidents

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) 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 The 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 / governor 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 **Incident Log** (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 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
        - 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 child protection purposes. The completed **Incident Log** 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. Staff should follow the **Process for Inappropriate Content**. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Pupils **Actions / Sanctions**

Incidents	Refer to class teacher	Refer to Deputy Head / Assistant Headteacher	Refer to Headteacher	Refer to Police	Refer to technical support re filtering / security etc	Inform parents / carers	Removal of network access for specified time	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).			X	X	X	X	X		X
Unauthorised use of non-educational sites during lessons	X						X	X	
Unauthorised use of mobile phone / digital camera / other mobile device			X			X	X	X	
Unauthorised use of social media / messaging apps / personal email			X			X	X	X	
Unauthorised downloading or uploading of files			X	X[2]	X	X	X	X	X
Allowing others to access school network by sharing username and passwords			X		X	X	X	X	
Attempting to access or accessing the school network, using another pupil's account			X		X	X	X	X	
Attempting to access or accessing the school network, using the account of a member of staff			X		X	X	X	X	X
Corrupting or destroying the data of other users			X		X	X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			X	X[2]		X	X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			X	X		X	X	X	X
Using proxy sites or other means to subvert the school's filtering system			X	X	X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident			X	X	X	X			
Deliberately accessing or trying to access offensive or pornographic material			X	X	X	X			X
Continued infringements of the above, following previous warnings or sanctions			X						X

[2] Depends on the nature of the files

Staff **Actions / Sanctions**

Incidents	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to police	Refer to technical support	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X			X	X
Inappropriate personal use of the internet / social media / email		X	X			X		X
Unauthorised downloading or uploading of files		X	X	X		X		X
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network using another person's account		X	X			X		X
Careless use of personal data e.g. holding or transferring data in an insecure manner		X	X			X		X
Deliberate actions to breach GDPR or network security rules		X	X		X	X		X
Corrupting or destroying the data other users or causing deliberate damage to hardware or software		X	X	X	X	X		X
Sending an email or message that is regarded as offensive, harassment or of a bullying nature		X	X	X		X		X
Using email / social media / messaging to carryout digital communications with pupils that aren't for educational purposes		X	X	X		X		X
Actions which could compromise the staff member's professional standing		X	X			X		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X	X	X		X		X
Using proxy sites or other means to subvert the school's filtering system		X			X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X	X	X	X		X
Deliberately accessing or trying to access offensive or pornographic material		X	X	X	X	X	X	X
Breaching copyright or licensing regulations		X	X	X	X	X	X	X
Continued infringements of the above, following previous warnings or sanctions		X	X				X	X

Appendix I – Inappropriate Content Process

Garstang Community Primary School

Online Safety Policy

When using the Internet, you or a child may come across images or content that are not appropriate, despite the School's filtering system.

Please remind children, every time they go online (computers and ipads) to do a search, what to do if they come across something inappropriate.

If they do, please follow the steps below.

1. Calmly minimise (don't close) the window trying to prevent other children from being exposed.

2. Tell an adult immediately.

3. The adult must remove the machine to a spot where children cannot see it and note down the website before closing the search.

4. The adult must inform the Computing Co-ordinator and Headteacher verbally and through the use of the **Incident Reporting Log** kept in the HT's office.

5. The adult must talk to the child about what they have seen and use the **Letter of Inappropriate Content** template to send a letter home to the parents that day.

6. The Computing Co-ordinator can then request that the website is blocked, recording this on the **Blocked Website Reporting Log**.

The Letter of Inappropriate Content can be found on the Staff One Drive under Online Safety.

The Blocked Website Reporting Log is in the HT's office.

Appendix II – Changes to Filtering Process

When using the internet, you may wish to use websites or resources that are blocked through the School's filtering system for educational purposes. If this is the case, please follow this process.

1. Check your website thoroughly for inappropriate content.

2. Submit a request to the Computing Co-Ordinator via email stating which website you would like unblocking and why.

3. Once approved, the Computing Co-ordinator or Technical Manager will unblock the website and complete the **Request to Unblock a Website Log** (located in the Headteacher's office) attaching the reasoning to the log.

4. If, once the website has been used, the Computing Co-ordinator believes that the website needs to be blocked to ensure that no inappropriate content is accessed by other pupils, they or the Technical Manager will block the website and note changes on the **Request to Unblock a Website Log**.