Online Safety Policy

For primary schools within the
Twynham Learning Multi-Academy Trust

Last amended 27.08.19 by Heather Watson

Reviewed by representatives of the Trust Primary Schools

Ratified by Board of Trustees 08.07.20

Next scheduled review date June 2021

This policy has been reviewed in line with the 8 principles set out in the Single Equality Policy and an initial screening Equality Impact Assessment has been carried out.

Development / Monitoring / Review of this Policy

This Online Safety policy has been developed with input from the Online Safety Group, Trustees and Headteachers from within the Trust.

Schedule for Development / Monitoring / Review

The 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. Should serious online safety incidents take place, the LA Safeguarding Officer, LADO and police (SSCT) should be informed.

The implementation of this policy will be monitored by the SLT and monitoring will take place once per year using:

- Logs of reported incidents
- Surveys / questionnaires of pupils, parents and staff

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents, visitors and community users) who have access to and are users of school IT systems, both in and out of the 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 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 of incidents of inappropriate online safety behaviour that take place out of school.

SECTION 1 – ROLES AND RESPONSIBILITES

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

1.1 Governors

Governors are responsible for monitoring the Online Safety Policy and for reviewing the effectiveness of the policy within the school. Regular information about online safety incidents will be provided to governors. An Online Safety Governor will be appointed within each school and their role will include:

- regular contact with the Online Safety Coordinator
- attendance at Online Safety Group meetings
- reporting to the Local Advisory Board or appropriate committee

1.2 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 Online Safety Coordinator.

- 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 (see flow chart on dealing with online safety incidents – included Section 5.2.1 – “Responding to incidents of misuse” and relevant Local Authority HR / other relevant body disciplinary procedures).

- The Headteacher / Senior Leaders are responsible for ensuring that the Online Safety Coordinator receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

- leads the Online Safety Group
- has joint responsibility (alongside Designated Safeguarding Leads) 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 Local Authority / relevant body
- liaises with school technical staff
- ensures that a log of incidents is maintained to inform future online safety developments,
- liaises regularly with Online Safety Governor to discuss current issues

1.3 Network Manager

The Trust Network Manager is 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 body Online Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy

- 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 monitoring software / systems are implemented and updated as agreed in school policies

1.4 Teaching and Support Staff (including volunteers)

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 Agreement
- they report any suspected misuse or problem to the Designated Safeguarding Lead
- all digital communications with pupils / parents 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 Policy and acceptable use policies
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- 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
- where pupils need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked, staff can request that the Technical Staff 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. Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

1.5 Designated Safeguarding Lead

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

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

1.6 Online Safety Group

The Online Safety Group 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 including the impact of initiatives. The group will also be responsible for regular reporting to the Advisory Board.

Members of the Online Safety Group (or other relevant group) will assist the Online Safety Coordinator (or other relevant person, as above) with:

- the production / review / monitoring of the Online Safety Policy / documents.
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression

- consulting stakeholders – including parents and the pupils about the online safety provision

1.7 Pupils

- are responsible for using the school IT systems in accordance with the pupil Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- 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.

1.8 Parents

Parents play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Each school will take every opportunity to help parents understand these issues through parent information evenings. Parents will be encouraged to support their school in promoting good online safety practice. Parents will sign to confirm their permissions for:-

- use of digital images by the school of their child
- appropriate use of school internet
- use of images in social media

upon entry in to school. They may review this at any point in the child's journey through the school.

SECTION 2 – EDUCATION AND TRAINING

2.1 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 curriculum should be provided as part of Computing / PD (PSHE) / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- 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.
- Pupils should be helped to understand the need for the pupil Acceptable Use and encouraged to adopt safe and responsible use both within and outside school.

2.2 Education – Parents

Parents play an essential role in the education of their children and in the monitoring / regulation of children's online behaviours. However, keeping up-to-date with the ever-changing online safety risks and issues is a real challenge. 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.

Schools will therefore seek to provide information and awareness to parents through:

- Curriculum activities
- Parent information evenings
- Newsletters
- A dedicated Online Safety website portal via the school website with a link to CEOP

2.3 Education – The Wider Community

Schools will 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.

2.4 Education & Training – Teaching and Support Staff (including 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 programme of 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.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Coordinator (or other nominated person) will receive regular updates through attendance at external training events (eg from SWGfL / LA / other relevant organisations) 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 / team meetings / INSET days.
- The Online Safety Coordinator (or other nominated person) will provide advice / guidance / training to individuals as required.

2.5 Training – Governors

Governors should take part in online safety training / awareness sessions. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (e.g. SWGfL).
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

SECTION 3 – Technical infrastructure

Each school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. 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 each 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.
- Users are responsible for the security of their username and password.
- The school I.T. Leader 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 (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs).
- 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. There is a clear process in place to deal with requests for filtering changes
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school has provided enhanced / differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users – staff / pupils etc)
- The activity of users on the school IT systems is recorded and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed procedure is in place for the provision of temporary access of ‘guests’ (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed procedure is in place regarding the extent of personal use that users (staff / pupils / community users) and their family members are allowed on school devices that may be used out of school.
- An agreed procedure is in place that controls the extent to which staff can download executable files and install programmes on school devices.
- An agreed procedure is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

SECTION 4 – USE OF EMERGING TECHNOLOGIES

4.1 Mobile technologies (including BYOD/BYOT for staff, visitors)

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud-based services such as email and data storage.

All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Anti-bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme.

- The school Acceptable Use Agreements for staff, pupils and parents will give consideration to the use of mobile technologies
- The school allows:

	School Devices (LAC/SEN, Sixth Form, Staff)			**Personal Devices**	
	School owned for single user	**School owned for multiple users**	**Authorised device[1]**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*		
Internet only				*Yes*	*Yes*
No network access					

4.2 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 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.

[1] Authorised device – purchased by the pupil/family through a school-organised scheme, such as Clingan's Trust. This device may be given full access to the network as if it were owned by the school.

- Parents will be given the opportunity to opt out of consenting for photographs of their child to be published on the school website / social media / local press.
- In accordance with guidance from the Information Commissioner's Office, parents 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 made publicly available on social networking sites, nor should parents 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.
- Pupils' work can only be published with the permission of the pupil and parents.

4.2.1 Data Protection

This is covered separately in the Data Protection Policy, which includes guidance relating to online safety.

4.3 Communication technologies

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			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed
Mobile phones may be brought to the school	✓			
Use of mobile phones in lessons				✓
Use of mobile phones in social time	✓			
Taking photos on mobile phones / cameras				✓
Use of other 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		✓		
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 are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- 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 between staff and pupils or parents (email, social media, chat, blogs, VLE 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.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

4.4 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. Trusts, 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 / academy group 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 pupils, parents 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 or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school social media accounts are established there should be:

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

Personal Use:

- Personal communications are those made via a 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
- The school permits reasonable and appropriate access to private social media sites

Monitoring of Public Social Media:

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

The school's use of social media for professional purposes will be checked regularly by the Online Safety Coordinator and Online Safety Group to ensure compliance with the school and Trust policies.

SECTION 5 – RESPONDING TO INCIDENTS OF MISUSE

5.1 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.

Schools believe 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 or outside the school when using school equipment or systems. The Trust policy restricts usage as follows:

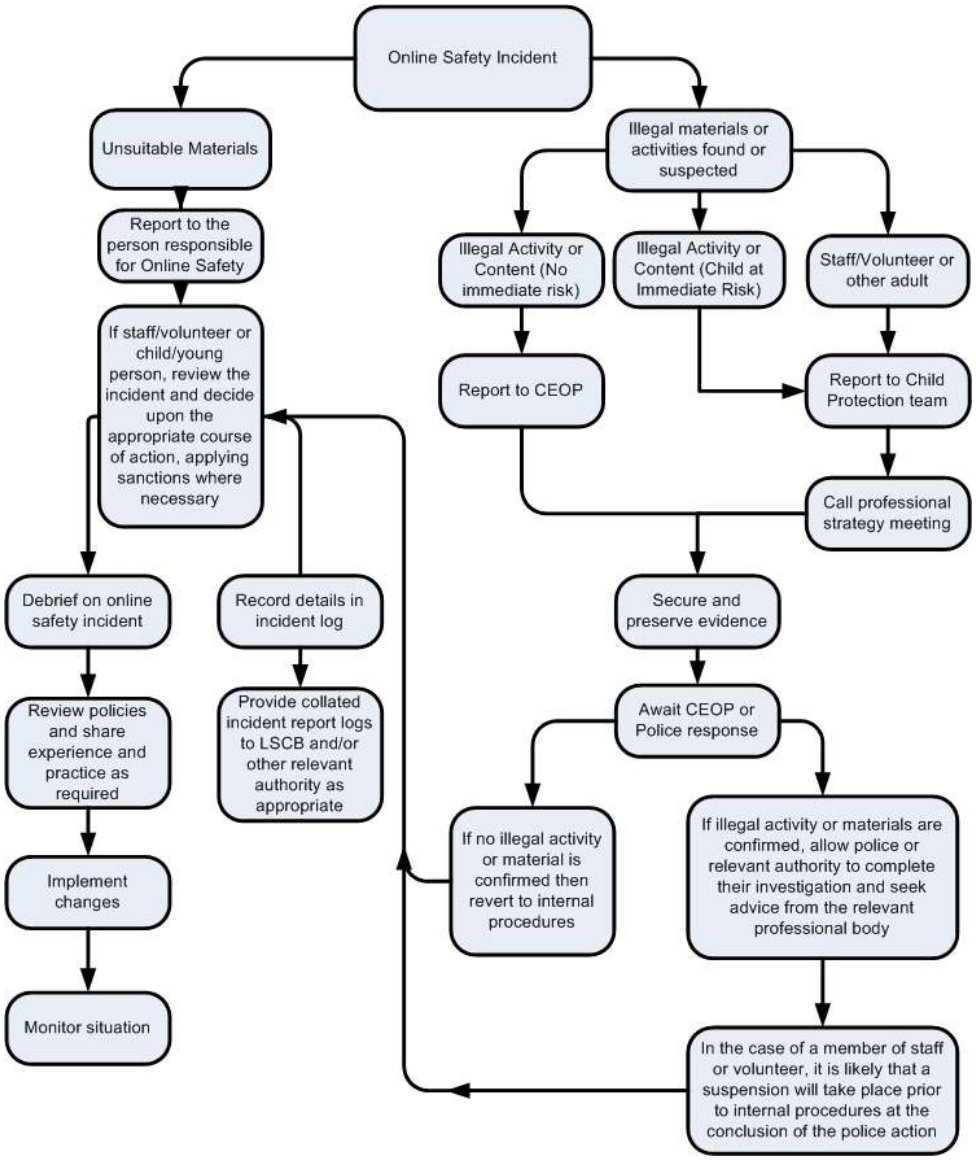
User Actions		Unacceptable and illegal	Unacceptable	Acceptable at certain times	Acceptable for nominmated users	Acceptable at all times for all users
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that 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		✓			
	Threatening behaviour, including promotion of physical violence or mental harm	✓				
	Promotion of extremism or terrorism	✓				
	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			✓			
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school			✓			
Revealing or publicising confidential or proprietary information (eg 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)			✓			
Online gaming (educational)				✓		
Online gaming (non-educational)			✓			
Online gambling			✓			
Online shopping/commerce, file sharing, use of social media, use of messaging apps, use of video broadcasting (e.g. YouTube)				✓		

5.2 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).

5.2.1 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 and appendix) for responding to online safety incidents and report immediately to the police.



5.2.2 Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow Trust 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
    - Trust involvement, when necessary
    - 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.

5.3 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:

Pupil Incidents	Actions					Sanctions			
	Refer to class teacher	Refer to SLT	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents	Removal of network / internet access rights	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).			✓	✓		✓			✓
Unauthorised use of non-educational sites during lessons	✓	✓			✓		✓	✓	
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device	✓	✓				✓		✓	
Unauthorised/inappropriate 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 another pupil's account		✓			✓		✓	✓	
Attempting to access or accessing the school network, using the account of a member of staff		✓	✓		✓	✓	✓		✓
Corrupting or destroying the data of other users		✓	✓		✓	✓	✓		✓
Sending an email, text or 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		✓	✓	✓	✓	✓	✓		✓
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		✓	✓		✓	✓	✓		✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		✓			✓		✓	✓	

Staff Incidents	Actions					Sanctions
	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	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 / personal email	✓	✓			✓	
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 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	✓	✓	✓	✓	✓	✓

Equality Impact Assessment – Initial Screening Record

1. What policy is being reviewed?	Online Safety Policy for Primary Schools
2. Upon whom will this impact?	Students, staff and parents

3. How would the work impact upon groups; are they included and considered?

The Equality Strands	Negative impact	Positive impact	No impact
Minority ethnic groups			√
Gender			√
Disability			√
Religion, faith or belief			√
Sexual orientation			√
Transgender			√
Age (N/A to pre-school and school children)			√
Rurality			√

4. Does data inform this work, research and/or consultation, and has it been broken down by the equality strands?

	NO	YES	Uncertain
Minority ethnic groups	√		
Gender	√		
Disability	√		
Religion, Faith or belief	√		
Sexual Orientation	√		
Transgender	√		
Age	√		
Rurality	√		

Does the initial screening highlight potential issues that may be illegal? NO

Further comments:-

Do you consider that a full Equality Impact Assessment is required? NO

Comment by CEO: