Green Lea First School
On-line Safety Policy

Our school aims to be an inclusive school. We are committed to promoting equality and good relationships. We will always tackle any discrimination quickly and firmly. We aim to make equality of opportunity a reality for our pupils, our staff and their families. We achieve this by recognising and paying attention to the nine different protected characteristics.

Race, disability, sex, age, religion or belief, sexual orientation, pregnancy, maternity and gender reassignment are known as protected characteristics (Equality Act 2010).

We consider the dyslexic child in all our planning and recognise that good teaching for dyslexic students is good for all.

Children with dyslexia will be given as much opportunity as possible to access the curriculum through a variety of strategies. The difficulties of the individual pupil will be taken into account in each lesson and every opportunity will be given for them to succeed.

Each individual is unique and the key to success lies in teaching on the basis of individual preferences.

On-Line Safety Policy

Introduction

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 the school. 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 on-line 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 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 on-line safety behaviour that take place out of school.

Roles and Responsibilities

Governors:
Governors are responsible for the approval of the On-line Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the teaching and learning committee receiving regular information about on-line safety incidents and monitoring reports. A member of the Governing Body has taken on the role of On-line Safety Governor. This Governor is Mr George Wilde.

Headteacher:
- The Headteacher has a duty of care for ensuring the safety (including on-line safety) of members of the school community, though the day to day responsibility for on-line safety will be delegated to the On-Line Safety Co-ordinator.

- The Headteacher and (at least) one other member of the staff should be aware of the procedures to be followed in the event of a serious On-Line safety allegation being made against a member of staff.

- The Headteacher is responsible for ensuring that the On- line Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their On-Line safety roles and to train other colleagues, as relevant.

On-line safety Co-ordinator:
- Takes day to day responsibility for On-Line safety issues and has a leading role in establishing and reviewing the school On-Line safety policies / documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an On-Line safety incident taking place.
- Provides training and advice for staff.
- Liaises with the Local Authority / relevant body.
- Liaises with any technicians.
- Receives reports of on-line safety incidents and creates a log of incidents to inform future On-Line safety developments.
- Meets with On-Line Safety Governor to discuss current issues, review incident logs and filtering / change control logs.
- Attends relevant meetings of teaching and learning committee of Governors.
- Ensures that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- Ensures that the school meets required on-line safety technical requirements and any *Local Authority / other relevant body On-Line Safety Policy / Guidance* that may apply.

• **Ensures** that they keep up to date with On-Line Safety technical information in order to effectively carry out their on-line safety role and to inform and update others as relevant.
• Ensures that monitoring software / systems are implemented and updated as required.

Teaching and Support Staff

Are responsible for ensuring that:
• They have an up to date awareness of on-line safety matters and of the current school on-line safety policy and practices.
• They have read, understood and signed the Staff Acceptable Use Policy (AUP).
• They report any suspected misuse or problem to the Headteacher and On-line safety Coordinator for investigation.
• All digital communications with pupils and parents / carers should be on a professional level and only carried out using official school systems.
• On-Line safety issues are embedded in all aspects of the curriculum and other activities.
• Pupils understand and follow the on-line safety and acceptable use policies.
• Pupils have a good understanding of research skills and 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 and implement current policies with regard to these devices.

Designated Safeguarding Lead

Should be trained in on-line 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

Pupils:

• Are responsible for using the *school* digital technology systems in accordance with the Pupil Acceptable Use Policy.
• Are developing 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.
• Understand the importance of adopting good on-line safety practice when using digital technologies in and out of school and realise that the school's On-Line 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, our website and information about national / local on-line safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good on-line 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 expected to sign a Community User AUA before being provided with access to school systems.

<u>Policy Statements</u>

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 on-line safety is therefore an essential part of the school's on-line safety provision. Children and young people need the help and support of the school to recognise and avoid on-line safety risks and build their resilience.

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

- A planned on-line safety curriculum, which is part of the Computing curriculum. This is reviewed regularly.
- Key on-line safety messages as part of a programme of assemblies.
- Pupils will be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- When at an appropriate age, pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

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

In lessons where internet use is pre-planned, it is best practice that 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 are allowed to freely search the internet, staff should have carried out internet searches using the same key words prior to the lesson. Teachers will also need to be particularly vigilant in monitoring the content of the websites the young people visit when pupils are allowed to do this..

Where online learning from home is taking place, clear guidelines and expectations are in place for children and parents. Live online learning is monitored by an administrative member of staff and parents are asked to be present during the lesson. The chat facility is turned off.

Education – parents / carers

Many parents and carers have only a limited understanding of on-line 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 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:

- Letters, newsletters, web site
- Parents' / Carers' evenings
- High profile events / campaigns eg Safer Internet Day
- Reference to the relevant web sites / publications eg www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education & Training – Staff / Volunteers

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

- A planned programme of formal on-line safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the on-line safety training needs of all staff will be carried out regularly. SWGfL BOOST includes unlimited online webinar training for all, or nominated,

staff (http://www.swgfl.org.uk/Staying-Safe/On-line safety-BOOST/Boost-landing-page/Boost-Hub/Professional-Development) It is expected that some staff will identify on-line safety as a training need within the performance management process.

- All new staff should receive on-line safety training as part of their induction programme, ensuring that they fully understand the school on-line safety policy and Acceptable Use Agreements. SWGfL BOOST includes an array of presentations and resources that can be presented to new staff (http://www.swgfl.org.uk/Staying-Safe/On-line safety-BOOST/Boost-landing-page/Boost-Hub/Resources)

- The On-Line Safety Coordinator will receive regular updates through attendance at LA update meetings and by reviewing guidance documents released by relevant organisations.

- This On-Line Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.

- The On-Line Safety Coordinator will provide advice / guidance to individuals as required. SWGfL BOOST includes an array of presentation resources that the on-line safety coordinator can access to deliver to staff (http://www.swgfl.org.uk/Staying-Safe/On-LineSafety-BOOST/Boost-landing-page/Boost-Hub/Resources). It includes presenter notes to make it easy to confidently cascade to all staff

Training – Governors

Governors should take part in on-line safety training / awareness sessions, with particular importance for those who are responsible for on-line safety or safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (eg SWGfL).

- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure 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 on-line 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.
- The Head teacher and office manager 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 (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.
- School staff regularly monitor and record the activity of users on the school technical systems, using SENSO, and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report, to class teachers or the Hedteacher, any actual / potential technical incident / security breach to the relevant person, as agreed.
- 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 policy is in place, AUP, regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.

- An agreed policy is in place, AUP, that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place, AUP, 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. (see School Personal Data Policy Template in the appendix for further detail)

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 eg 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 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 *students / 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, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website (part of the AUA signed by parents or carers at the start of the year).
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than 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 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 Data Protection Act (DPA).
- 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.

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, memory 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 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:

Communication Technologies	Staff & other adults				Students / Pupils				
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	lowed with staff permission	Not allowed
Mobile phones may be brought to school		X			X				
Use of mobile phones in lessons	X				X				
Use of mobile phones in social time			X		X				
Taking photos on mobile phones / cameras	X				X				
Use of other mobile devices eg tablets, gaming devices	X				X				
Use of personal email addresses in school, or on school network				X	X				
Use of school email for personal emails	X				X				
Use of messaging apps			X		X				
Use of social media			X		X				
Use of blogs				X	X				

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 (eg 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. (SWGfL BOOST includes an anonymous reporting app Whisper - http://www.swgfl.org.uk/Staying-Safe/On-LineSafety-BOOST/Boost-landing-page/Boost-Hub/SWGfL-Whisper)
- Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils should be taught about on-line 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.

<u>Social Media - Protecting Professional Identity</u>

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:

- Clear reporting guidance, including responsibilities, procedures and sanctions.

School staff should ensure that:

- No reference should be made in social media to 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 or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
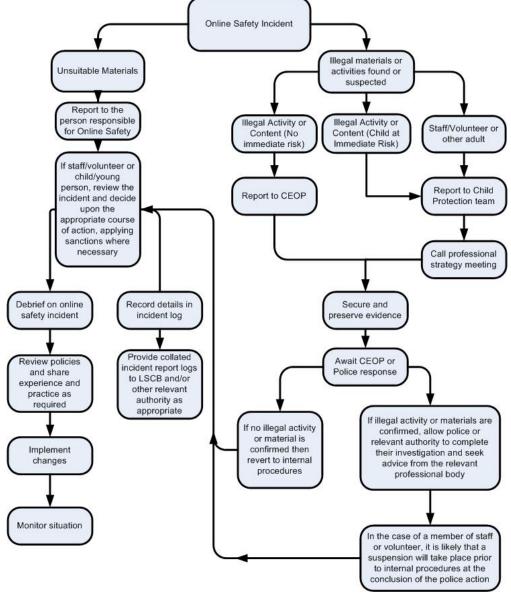
Unsuitable / inappropriate activities

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 / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg 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			X			
Use of messaging apps			X			
Use of video broadcasting eg Youtube				X		

Responding to incidents of misuse

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.

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 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 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 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.

Students / Pupils

Incidents:	Refer to class teacher	Refer to Head teacher	Refer to Police	Refer to technician for action re filtering / security etc	Inform parents / carers	Removal of internet access rights	Warning	Further sanction eg 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					
Unauthorised use of non-educational sites during lessons	X					X	X	
Unauthorised use of mobile phone / digital camera / other mobile device		X						
Unauthorised use of social media / messaging apps / personal email		X						
Unauthorised downloading or uploading of files		X				X	X	
Allowing others to access school network by sharing username and passwords		X				X	X	

Incidents								
Attempting to access or accessing the school network, using another pupil's account		X				X	X	
Attempting to access or accessing the school network, using the account of a member of staff		X				X	X	
Corrupting or destroying the data of other users	X	X						X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X		X	X		X
Continued infringements of the above, following previous warnings or sanctions		X		X	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
Using proxy sites or other means to subvert the school's filtering system		X		X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X		X				
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X		X	X	X	X	

Staff   Actions / Sanctions

Incidents:	Refer to line manager	Refer to Headteacher Principal	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).		X	X	X				
Inappropriate personal use of the internet / social media / personal 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 eg holding or transferring data in an insecure manner	X	X			X	X		
Deliberate actions to breach data protection or network security rules	X	X	X		X	X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	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	X	X	X	X	X	X

	1	2	3	4	5	6	7	8
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X	X		X	X	X	X
Actions which could compromise the staff member's professional standing	X	X	X			X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school / academy	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		X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X	X
Breaching copyright or licensing regulations	X	X	X		X	X		X
Continued infringements of the above, following previous warnings or sanctions	X	X	X		X	X	X	X

Schedule for Development / Monitoring / Review

This on-line safety policy was approved by the Governing Body on:	21st October 2021
The implementation of this on-line safety policy will be monitored by the:	Online Safety Co-ordinator Headteacher
This policy was written by:	Online Safety Co-ordinator
Monitoring will take place at regular intervals:	Annually
The *Governing Body* will receive a report on the implementation of the online safety policy (which will include anonymous details of online safety incidents) at regular intervals:	Annually
The On-Line 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 on-line safety or incidents that have taken place. The next anticipated review date will be:	October 2022
Should serious on-line safety incidents take place, the following external persons / agencies should be informed:	Staffordshire Safeguarding Board Police

This on-line safety policy has been developed through consultation with

• Headteacher
• Online Safety Co-ordinator
• Staff – including Teachers & Support Staff
• Governors
• Parents and Carers
• Pupils

The school will monitor the impact of the policy using:

• Logs of reported incidents
• Monitoring logs of internet activity (SENSO)
• Surveys / questionnaires of
  • pupils
  • parents / carers
  • staff