Davenham Church of England Primary *School*

"Working Together, Playing Together, Serving God and Serving Others"

"...encourage one another and build each other up..."
1 Thessalonians 5:11.

POLICY FOR E SAFETY

The safeguarding of all our pupils is of the upmost importance. This policy applies to all members of the Davenham Primary School community (including staff, students / children, volunteers, parents / carers, visitors, community users) who have access to, and are users of, Davenham ICT systems; both in and outside the school. The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of children when they are not on school premises and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of school but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. Davenham 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 e-safety behaviour that take place out of Davenham Primary School.

ROLES AND RESPONSIBILITIES

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school.

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving information about e-safety incidents and monitoring reports. A member of the Governing Body takes on the role of E-Safety Governor.

The role of the E-Safety Governor will include:

- meetings with the E-Safety Officer
- monitoring of e-safety incident logs
- monitoring of filtering / change control logs
- reporting to relevant Governors

Headteacher / Principal and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Officer.
- The Headteacher and members of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff**.** (see flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR disciplinary procedures).

- The Headteacher and Senior Leaders are responsible for ensuring that the E-Safety Officer and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

The E Safety Officer is responsible for:

- the day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- providing training and advice for staff
- liaising with the Local Authority / relevant body
- liaising with technical staff
- receiving reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- meeting with the E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- reporting to the Senior Leadership Team as necessary.

Network Manager / Technical staff are responsible for ensuring that:

- the school's technical infrastructure is secure and is not open to misuse or malicious attack
- school meets required e-safety technical requirements and any Local Authority / other relevant body E-Safety Policy / Guidance that may apply.
- users only access the networks and devices through a properly enforced password protection policy.
- filtering is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- the use of the network / internet / remote access / email is regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher or E-Safety Coordinator for investigation / action / sanction.
- monitoring software is implemented and updated

Teaching Staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher; E-Safety Coordinator for investigation / action / sanction
- all digital communications with students / children / parents / carers is on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities where appropriate
- children understand and follow the e-safety and 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 children 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

The Child Protection / Safeguarding Designated Person should be trained in e-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

Children are responsible for:

- using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- understanding the importance of reporting abuse, misuse or access to inappropriate materials and are taught how to do so
- knowing about and understanding how to use mobile devices and digital cameras safely, including the taking / use of images and what is meant by cyber-bullying
- understanding the importance of adopting good e-safety practice when using digital technologies out of school and realise that the Davenham Primary School 's E-Safety Policy covers their actions out of school, if it is 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. Davenham will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at Davenham Primary School events
- access to parents' sections of the website and on-line student / pupil records
- their children's personal devices in the Davenham Primary School / (where this is allowed)

Policy Statements

Education – children

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

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

- a planned e-safety curriculum should be provided as part of Computing
- key e-safety messages should be reinforced as part of a planned programme of assemblies
- children should 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.
- children should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- children should be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use 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 children 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.
- it is accepted that from time to time, for good educational reasons, students 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 Staff (or other relevant designated person) 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 e-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.

Davenham will therefore seek to provide information and awareness to parents and carers through:

- curriculum activities
- web site
- parents evenings
- high profile events / campaigns e.g. Safer Internet Day
- reference to the relevant web sites

Education – The Wider Community

Davenham will provide opportunities for local community groups / members of the community to gain from the Davenham Primary School 's / e-safety knowledge and experience. This may be offered through the following:

- providing family learning courses in use of new digital technologies, digital literacy and e-safety
- E-Safety messages targeted towards grandparents and other relatives as well as parents.
- Davenham Primary School website will provide e-safety information for the wider community
- supporting community groups e.g. Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their e-safety provision

Education & Training – Staff / Volunteers

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

- the E-Safety Officer will receive regular updates through attendance at external training events.
- this E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings.
- the E-Safety Officer will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any group involved in technology / e-safety / health and 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 training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

We will ensure 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 e-safety responsibilities:

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

- All users at KS2 will be provided with a username and secure password by Mr Ashworth who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The “master / administrator” passwords for the Davenham ICT system, used by the Network Manager (or other person) must also be available to the Headteacher
- 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 monitored.
- 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.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and children instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and children 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 children 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 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 children 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.
- Care should be taken when taking digital / video images that children are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Children must not take, use, share, publish or distribute images of others without their permission

- Photographs published on the website, or elsewhere that include children will be selected carefully and will comply with good practice guidance on the use of such images.
- Written permission from parents or carers will be obtained before photographs of children are published.

Davenham follows the regulations set out by GDPR (please refer to associated policy) and will 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 has clear and understood arrangements for the security, storage and transfer of personal data
- 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 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.

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 data must be securely deleted from the device, in line with Davenham Primary 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:

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

When using communication technologies the Davenham Primary 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 children 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 children or 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.
- 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 staff at Davenham have a duty of care to provide a safe learning environment for children and staff. Davenham Primary School and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully or discriminate 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 minimize risk of harm to children, staff and the school through limiting access to personal information:

- Training to include: 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 children, 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 minimize risk of loss of personal information.

Davenham Primary School 's use of social media for professional purposes will be checked regularly by the e-safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

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 Davenham Primary School or outside Davenham Primary School when using school equipment or systems. The school policy restricts usage as follows:

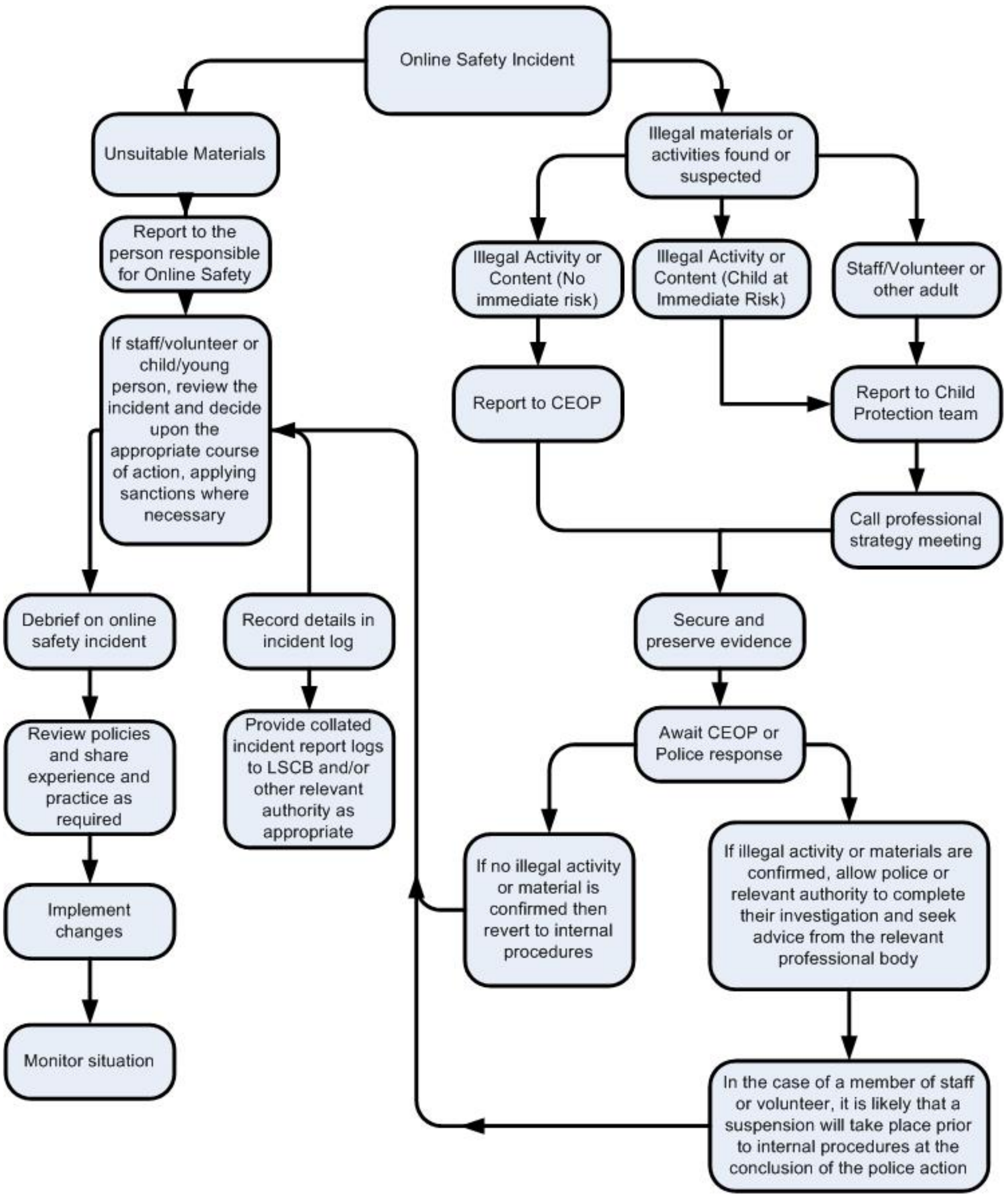
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child 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 Davenham Primary School or brings Davenham Primary School into disrepute				X	
Using Davenham Primary School systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Davenham Primary 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		X			
Use of messaging apps		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 and appendix) for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Debrief on online safety incident
Record details in incident log
Secure and preserve evidence
Review policies and share experience and practice as required
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
Implement changes
Monitor situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow our 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 / volunteer 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.

Davenham Primary School Actions & Sanctions

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

Students / Children **Actions / Sanctions**

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Headteacher / Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	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).			X	X					
Unauthorised use of non-educational sites during lessons	x								
Unauthorised use of mobile phone / digital camera / other mobile device	x		x			x			
Unauthorised use of social media / messaging apps / personal email	x		x			x			
Unauthorised downloading or uploading of files	x		x			x			
Allowing others to access Davenham Primary School network by sharing username and passwords	x								
Attempting to access or accessing the Davenham Primary School network, using another student's / pupil's account	x								
Attempting to access or accessing the Davenham Primary 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			
Continued infringements of the above, following previous warnings or sanctions	x		x	x		x			
Actions which could bring the Davenham Primary School into disrepute or breach the integrity of the ethos of the Davenham Primary School	x			x		x			
Using proxy sites or other means to subvert the	x			x		x			

Davenham Primary School ’s / ’s filtering system									
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			
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	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	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		
Unauthorised downloading or uploading of files		x			x			
Allowing others to access Davenham Primary School network by sharing username and passwords or attempting to access or accessing the Davenham Primary School network, using another person’s account		x						
Careless use of personal data e.g. holding or transferring data in an insecure manner		x			x			
Deliberate actions to breach data protection or network security rules		x			x	x		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		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
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / children		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 Davenham Primary School / into disrepute or breach		x	x	x		x	x	x

the integrity of the ethos of the Davenham Primary School /								
Using proxy sites or other means to subvert the Davenham Primary School 's / 's filtering system		x			x	x		
Accidentally accessing offensive or pornographic material and failing to report the incident		x						
Deliberately accessing or trying to access offensive or pornographic material		x	x	x	x		x	x
Breaching copyright or licensing regulations		x						
Continued infringements of the above, following previous warnings or sanctions							x	

EQUALITY STATEMENT

Davenham Primary School is committed to ensuring equality of opportunity for all children, staff, parents, carers and visitors irrespective of their race, gender, gender identity, disability, religion or belief, sexual orientation, marital status, age or pregnancy and maternity. We tackle discrimination through the positive promotion of equality, by valuing diversity, challenging bullying and stereotypes and by creating an inclusive environment which champions fairness and respect for all.

Davenham Church of England Primary Davenham Primary School

"Working Together, Playing Together, Serving God and Serving Others"

POLICY FOR E-SAFETY

<table>
<tr><th colspan="2">Effective Date</th><th colspan="2">June 2017</th></tr>
<tr><th colspan="2">Review Date</th><th colspan="2">Every 2 years</th></tr>
<tr><th colspan="2">Person Responsible</th><th colspan="2">Joanne Hyslop</th></tr>
<tr><th>Signed Headteacher</th><th colspan="2">Signed Chair of Governors</th><th>Date Ratified</th></tr>
<tr><td>J Hyslop</td><td colspan="2">J Green</td><td>June 2017</td></tr>
</table>

Review Date	Signed Headteacher	Signed Chair of Governors
November 2019	Joanne Hyslop	Debbie Mercer
13 December 2021	Joanne Hyslop	Debbie Mercer