Doddiscombsleigh
Primary School

E- Safety Policy

This policy reflects the school's commitment to being a
Rights Respecting School.

Approved at FGB 14.03.2018
Due for renewal Spring 2019

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the *Governing Body on:*	*14th March 2018*
The implementation of this e-safety policy will be monitored by the:	Head of School
Monitoring will take place at regular intervals:	*Annually*
The *Governing Body* will receive a report on the implementation of the e-safety policy generated by the the Head of School and Safeguarding Governor (which will include anonymous details of e-safety incidents) at regular intervals:	*Annually in Spring Tern*
The E-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 e-safety or incidents that have taken place. The next anticipated review date will be:	*Spring 2019*
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*LA, MASH, , Police* *USF Executive Head and IT team*

The school will monitor the impact of the policy using:

- *Logs of reported incidents*
- *Monitoring logs of internet activity (including sites visited) if required*
- *Internal monitoring data for network activity*

Scope of the Policy

This policy applies to all members of the *school* community (including staff, students / 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*

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students / 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 e-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 (see appendix for policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The *school* will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate 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 *Governors* 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* The role of the on line safety *Governor* will include:

- *regular meetings with the on line-Safety Co-ordinator*
- *regular monitoring of on line-safety incident logs*
- *reporting to relevant Governors' meetigs*

Executive Head and Head of School:

- The Executive Head has a duty of care for ensuring the safety (including on line safety) of members of the school community.
- The Head of School and another member of the Senior Leadership Team 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.
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-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
- receives reports of online safety incidents and creates a log of incidents to inform future on line safety developments,
- meets regularly with on line safety Governor to discuss current issues, review incident logs and filtering / change control logs
- that the *school's* technical infrastructure is secure and is not open to misuse or malicious attack
- that the *school* meets required on line safety technical requirements and any *Local Authority on line* Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy**.**

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 / Agreement (AUP)
- they report any suspected misuse or problem to the Head of School for investigation / action / sanction
- all digital communications with pupils / parents / carers should be on a professional level

Child Protection 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.

Policy Statements

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school'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.

On line safety should be a focus in all areas of the curriculum and staff should reinforce e-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 should be provided as part of Computing and PHSE lessons and should be regularly revisited
- Key on line safety messages should be reinforced as part of a planned programme of assemblies
- Pupils 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.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

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 not underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- *Curriculum activities*
- *Letters, newsletters, web site,*
- *Parents / Carers evenings / sessions*
- *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 (see appendix for further links / resources)

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.
- 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.

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school 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 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 outlined in the SWGfL Security Policy and Accepatble Usage Policy and any relevant Authority E-Safety Policy and guidance
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with usernames and password. Users will be responsible for the security of their username and password and must not allow other users to access systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The "master / administrator" passwords for the school IT system, used by the IT technician must also be available to the Head of School or other nominated senior leader and kept in a secure place (eg school safe)
- Security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations and hand held devices etc. from accidental or malicious attempts which might threaten the security of the schools systems and data. All filtering issues must be reported to the IT technician
- Personal data must not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments.

- The school has a set of clear expectations and responsibilities for all users
- The school adheres to the Data Protection Act principles
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the school's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe

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 in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should parents / carers comment on any activities involving other *pupils* in the digital / video images.
- *Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.*
- *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.*
- *Written permission from parents or carers will be obtained before photographs of pupils are published on the school website*

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate

- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school must ensure that:

- **It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.**
- **Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.**
- **All personal data will be fairly obtained 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)**

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 data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications

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

	Staff & other adults			Pupils				
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	N a v
Mobile phones may be brought to school	x x						z 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							
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.**
- **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 / carers (email, chat, VLE etc) must be professional in tone and content.**

Social Media - Protecting Professional Identity

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

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

- Training to include: acceptable use; social media risks; checking of settings; 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 / 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:

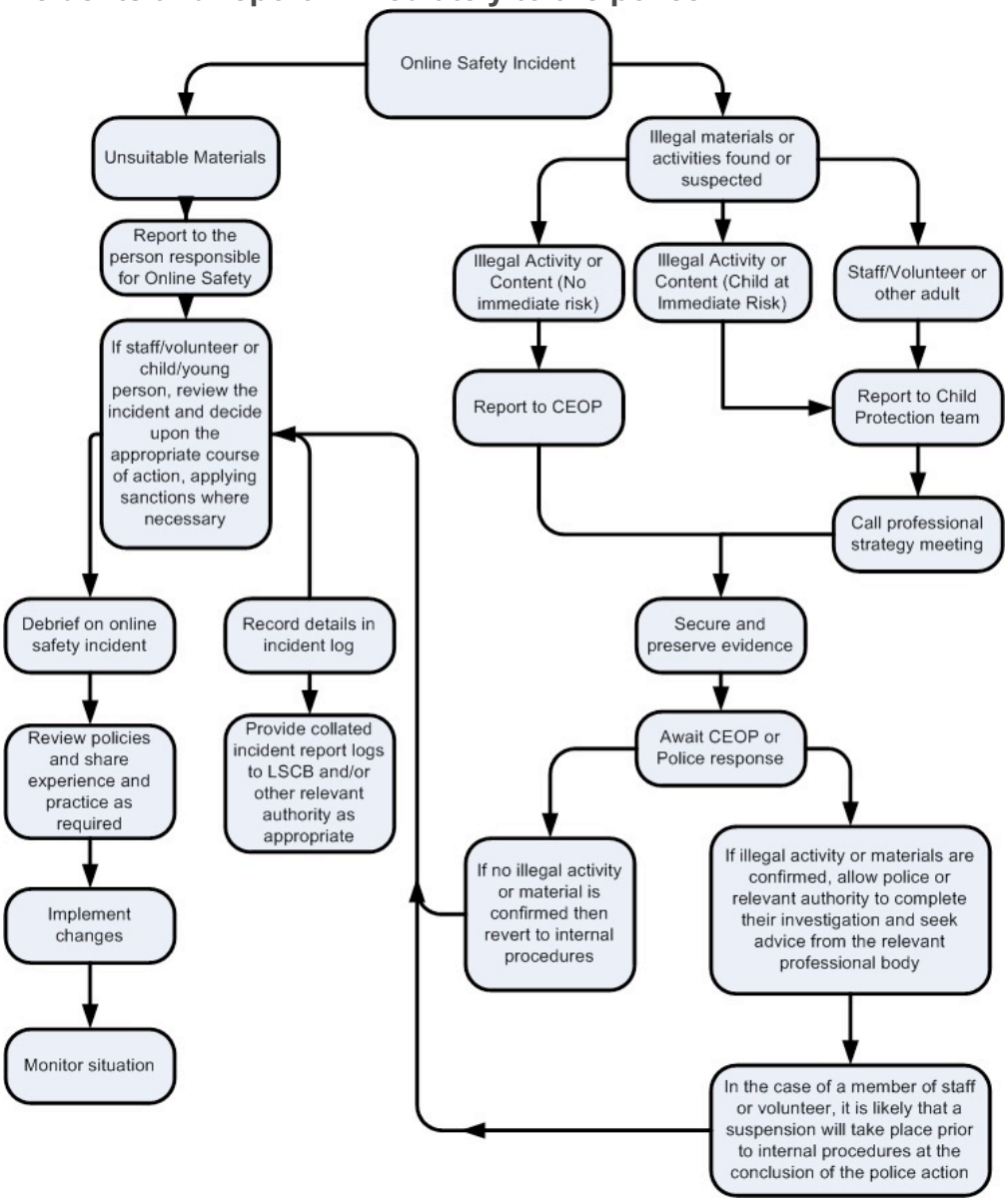
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child 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			

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 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.

School Actions & Sanctions

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

Students / Pupils

Incidents:	Refer to class teacher	Refer to Headteacher	Refer to Police	Inform parents / carers	Removal of network / 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							
Unauthorised use of mobile phone / digital camera / other mobile device		X		X		X	
Unauthorised use of social media / messaging apps / personal email		X			X		
Unauthorised downloading or uploading of files		X			X		
Allowing others to access school network by sharing username and passwords		X			X		
Attempting to access or accessing the school network, using another student's / pupil's account		X			X		
Attempting to access or accessing the school / academy network, using the account of a member of staff		X			X		
Corrupting or destroying the data of other users		X			X		
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X			X		
Continued infringements of the above, following previous warnings or sanctions		X			X		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X			X		
Using proxy sites or other means to subvert the school's / academy's filtering system		X			X		
Accidentally accessing offensive or pornographic material and failing to report the incident		X			X		
Deliberately accessing or trying to access offensive or pornographic material		X			X		

Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X			X		

Staff

Incidents:	Refer to line manager	Refer to Headteacher Principal	Refer to Local Authority / HR	Refer to Police	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	
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	
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	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X		x	x	x	
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		X			x		
Actions which could compromise the staff member's professional standing		X					x
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy		X					x
Using proxy sites or other means to subvert the school's / academy's filtering system		X				x	
Accidentally accessing offensive or pornographic material and failing to report the incident		X			x		
Deliberately accessing or trying to access offensive or pornographic material		X	x			x	x
Breaching copyright or licensing regulations		X			x		
Continued infringements of the above, following previous warnings or sanctions		X					x

Acknowledgements

SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School E-Safety Policy Template and of the 360 degree safe E-Safety Self Review Tool:

- Members of the SWGfL E-Safety Group
- Avon and Somerset Police
- Representatives of SW Local Authorities
- Plymouth University Online Safety
- NEN / Regional Broadband Grids