FERNDOWN MIDDLE SCHOOL

E-SAFETY POLICY

(Online Safety Policy)

Policy to be reviewed by governor committee	**Community & Curriculum Committee**
Frequency:	**Annually**

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

Table of Contents

Development / Monitoring / Review of this Policy

This e-safety policy has been developed by a working group made up of:

- Head teacher
- E-Safety Co-Ordinator
- Network Manager
- Co-ordinator for Computing
- Staff – including Teachers, Support Staff, Technical staff
- Governors

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

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the Governors Community and Curriculum Committee on:	*Insert date*
The implementation of this e-safety policy will be monitored by the:	*Curriculum & Community Governor Committee and the Senior Leadership team*
Monitoring will take place at regular intervals:	Once a year
Governors Community and Curriculum Committee will receive a report on the implementation of the e-safety policy generated by the E-Safety Coordinator (which will include anonymous details of e-safety incidents) at regular intervals:	Termly
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:	*Insert date*
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*LA Safeguarding Officer, Police , SWGfL*

The school will monitor the impact of the policy using:

- Logs of reported incidents (paper log in main office)
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity

Scope of the Policy

This policy applies to all members of the *school (*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*.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the *school* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other 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. Refer to the published Behaviour Policy regarding potential issues and appropriate actions.

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 e-safety behaviour that take place out of school.

In addition, the following documents need to be considered in parallel with this policy:

- FMS Staff Acceptable Use of ICT Policy
- FMS Pupil Acceptable Use of ICT Policy
- FMS Pupil Media Consent Form
- Guidance for FMS Staff on the use of Digital Media
- Use of Biometric systems
- Behaviour policy
- School Technical Security Policy
- Social networking policy
- Code of Conduct Policy
- SWGfL Filtering Policy

Roles and Responsibilities

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

Governors:

The full governing body is responsible for the ratification of the E-Safety Policy. The discussion and review of the effectiveness of the policy will be delegated to the Governors' Community and Curriculum Committee, receiving regular information about E-Safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Safeguarding Governor. The role of Safeguarding Governor will include:

- Regular meetings with the E-Safety Co-ordinator (at least annually)
- Regular monitoring of E-Safety incident logs (at least annually)
- Regular monitoring of filtering / change control logs
- Reporting to relevant Governors Community and Curriculum Committee (annually or following a serious breach of E-Safety procedures)

Headteacher 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 Co-ordinator.
- The Headteacher and Senior Leaders 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 –"Responding to incidents of misuse" and relevant Local Authority HR disciplinary procedures).
- The Headteacher / Senior Leaders are responsible for ensuring that the E-Safety Co-ordinator 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 Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal E-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. There is a log of all website access (available on request from SWGfL) that happens in school. There is a filtering system in place (RM SafetyNet).
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator .

E-Safety Co-ordinator:

- 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 E-Safety incident taking place.
- Provides training and advice for staff
- Liaises with the Local Authority / relevant body
- Receives reports of E-Safety incidents and creates a log of incidents to inform future E-Safety developments, (See appendix for Log sheet templates).
- Meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs(annually)
- Attends relevant E-Safety meetings
- Reports regularly to Senior Leadership Team
- Investigation of any serious incidents would be carried out by the Year Leader/Headteacher and /or Deputy Headteacher

Network Manager:

The Network Manager is responsible for ensuring that:

- The school's technical infrastructure is secure and is not open to misuse or malicious attack
- The school meets required E-Safety technical requirements and any Local Authority / other relevant body E-Safety Policy / Guidance that may apply
- Users may only access the networks and devices through a properly enforced password protection policy
- The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (see appendix "Technical Security Policy" for good practice)
- 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 is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / E-Safety Co-Ordinator for investigation / action / sanction
- Monitoring software / systems are implemented and updated as agreed in school.

Teaching and Support 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 and volunteers Acceptable Use Policy
- They report any suspected misuse or problem to the E-Safety Co-ordinator for investigation / action / sanction
- All digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- E-Safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the E-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 (where allowed) and implement current policies with regard to these devices
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Child Protection / Safeguarding Designated Person / Officer:

Should be trained in E-Safety issues and be aware of the potential for serious child protection / safeguarding issues that could 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
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying
- Should understand the importance of adopting good E-Safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers:

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE 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 school events
- Access to parents' sections of the website / VLE and on-line pupil records
- Their children's personal devices in the school

Community Users:

Community Users who access school systems / website / VLE as part of the wider school provision will be expected to sign a Staff and Volunteers Acceptable Use Policy before being provided with access to school systems.

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.

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 / PHSCE / other lessons and should be regularly revisited
- Key E-Safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access 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
- 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
- If pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request (giving appropriate notice) that the Technical Staff can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be formally made, 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.

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 e.g. Safer Internet Day
- Reference to the relevant web sites / publications.

Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's E-Safety knowledge and experience. This may be offered through the following:

- E-Safety messages targeted towards grandparents and other relatives as well as parents
- The school website will provide E-Safety information for the wider community.

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:

- All new staff should receive E-Safety training as part of their induction programme, ensuring that they fully understand the school E-Safety policy and Acceptable Use Agreements
- The E-Safety Co-Ordinator will receive regular updates through attendance at external training events (e.g. from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days
- The E-Safety Co-Ordinator (or other nominated person) 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 subcommittee / 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 (e.g. 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 / 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 identified in the above sections will be effective in carrying out their E-Safety responsibilities.

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices
- All users will be provided with a username and secure password by the Network Manager who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password regularly
- The "master / administrator" passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher and kept securely in a sealed envelope in the school safe
- Network Manager and Senior Finance Officer are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations

- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored
- The school has provided enhanced / differentiated user-level filtering
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement
- An appropriate system is in place (the e safety log – template available in appendix) for users to report any actual / potential technical incident / security breach to the relevant person, as agreed). This log is held in the school office
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly within the SWGfL. The school infrastructure and individual workstations are protected by up to date anti-virus software
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems. A generic staff account is available for a supervised visitor/supply teacher
- An agreed policy is in place 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 that forbids staff from downloading executable files and installing programmes on school devices
- An agreed policy is in place regarding the use of removable media (e.g. 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.

Bring Your Own Device (BYOD)

No external devices from home to be used in the classroom, Staff and Pupils.

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 cyber-bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the 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 or blog, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

Schools and their employees should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- have permission to access that data
- need to have access to that data.

Data breaches can have serious effects on individuals and / or institutions concerned, can bring the school into disrepute. This may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office~~,~~ for the school and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must adhere to the legal requirements contained in relevant data protection legislation and relevant regulations and guidance (where relevant from the Local Authority).

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) http://www.ico.org.uk/what_we_cover/register_of_data_controllers.aspx
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system or any other removable media:

- the data must be encrypted and password protected
- memory sticks must not be used.

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				Students / Pupils			
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 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 e.g. 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 can be monitored by school technical staff
- Sensitive and personal data must not be sent via e-mail unless encrypted. Whilst the connection from your device to the school e-mail system is secure, as with any commercial e-mail service, messages sent to recipients on different e-mail domains travel via the internet and are therefore not secure
- Users must immediately report, to the E-Safety Co-ordinator – 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 students / pupils or parents / carers must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal e-mail addresses, text messaging or social media must not be used for these communications
- Pupils should be taught about E-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.

Unsuitable / Inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

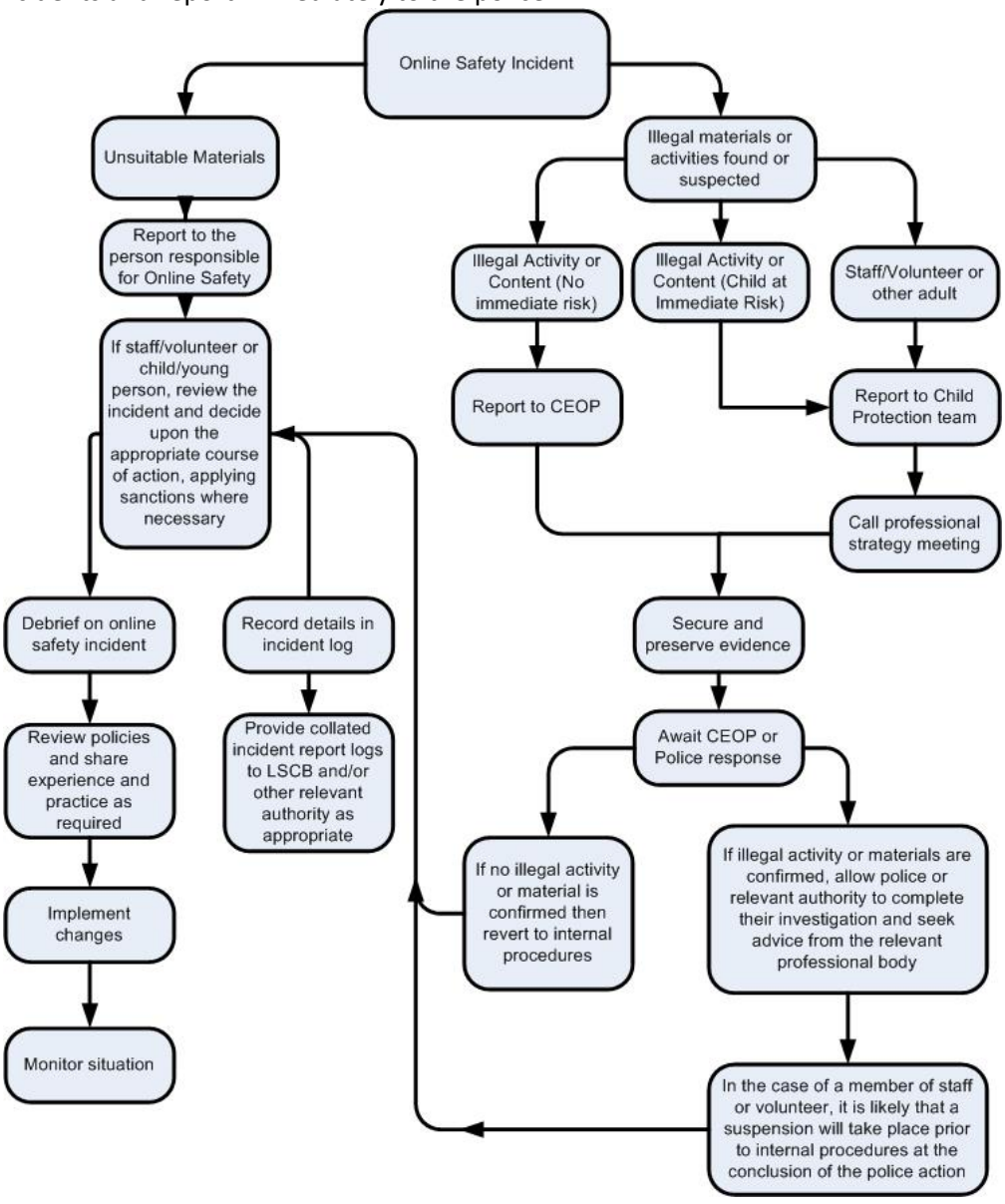
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files (Computer misuse Act 1990)						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 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.

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:

Pupils	***Actions / Sanctions***								
Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Headteacher	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	X	X	X	X		X
Unauthorised use of non-educational sites during lessons		X					X		X
Unauthorised use of mobile phone / digital camera / other mobile device		X				X		X	X
Unauthorised use of social media / messaging apps / personal email		X				X	X	X	X
Unauthorised downloading or uploading of files		X	X		X	X	X		X
Allowing others to access school network by sharing username and passwords	X	X			X			X	
Attempting to access or accessing the school network, using another student's / pupil's account		X			X	X	X	X	X
Attempting to access or accessing the school network, using the account of a member of staff			X		X	X	X		X
Corrupting or destroying the data of other users	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
Continued infringements of the above, following previous warnings or sanctions			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	X
Using proxy sites or other means to subvert the school's filtering system		X	X	X	X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X		X	X	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 managerr	Refer to Headteacher	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	X	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		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		
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils		X				X		
Actions which could compromise the staff member's professional standing	X	X				X		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X		X	X		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
Breaching copyright or licensing regulations		X			X	X		
Continued infringements of the above, following previous warnings or sanctions		X	X				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.

Appendices

- Pupil Acceptable Use Agreement
- Parents / Carers Acceptable Use Agreement
- Staff and Volunteers Acceptable Use Agreement
- Responding to incidents of misuse – flowchart
- Record of reviewing sites (for internet misuse)
- E-Safety Reporting Log
- E-Safety Training Needs Audit
- Technical Security Policy
- Fair Processing Privacy Notice
- Legislation
- Glossary of terms

Pupil Acceptable Use Policy Agreement

School Policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications. It should be noted that users should not expect that files stored on servers or disks would be private
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I will not log anybody else onto the system and will not log onto more than one computer at a time
- I will be aware of "stranger danger", when I am communicating on-line
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, e-mail addresses, telephone numbers, age, gender, educational details, financial details etc.) unless I am given permission by a teacher to do so
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line. I understand that my report would be confidential but that the teacher may pass this information on as it may help protect others and myself.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission
- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, for commercial purposes (e.g. buying or selling goods) or video broadcasting (e.g. YouTube).

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission

- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions
- Pupils must not take, use, share, publish or distribute images of others without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the *school*:

- I will not eat or drink near computer equipment
- I will not intentionally damage, disable, or otherwise harm the operation of computers, or waste resources, and will immediately report any damage or faults involving equipment or software, however this may have happened
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings
- I will not open any hyperlinks on webpages or embedded links in documents, unless I know and trust them, due to the risk of exposure to viruses or other harmful programmes.
- I will not attempt to download any files or other materials from the Internet unless I am given permission to do so
- I will only use my own personal devices (mobile phones / USB devices etc.) in school if I have permission, and they have been checked with anti-virus software, and found to be clean of viruses. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials
- I will not attempt to use social media sites at any time.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information)
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action as per the sanctions detailed in the school behaviour policy.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Pupil Acceptable Use Agreement Form

This form relates to the pupil Acceptable Use Agreement, to which it is attached.

CCC070617/1

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices, USB devices, cameras etc.
- I use my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school website etc.

Name of Pupil:	
Group / Class:	
Signed:	
Date:	

Parent Acceptable Use Agreement Form

Name of Parent / Carer:	

As the parent / carer of the pupil identified above, I give permission for my son / daughter to have access to the internet and to ICT systems at school. These systems include several cloud / web based applications and services that are available to pupils to support and extend their learning.

I know that my son / daughter and has received, or will receive, e-safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Signed		Date	

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website, in the school prospectus and occasionally in the public media.

The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their full names.

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 pupils in the digital / video images.

Digital / Video Images Permission Form

Name of Pupil:

Name of Parent / Carer:

As the parent / carer of the above pupil:

I agree that if I take digital or video images at, or of, – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

I agree to the school taking and using digital / video images of my child. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school ☐

I do not agree to the school taking and using digital / video images of my child. ☐

Signed

Date

CCC070617/1

Use of Biometric Systems

Biometric Library Management System – Fingerprint Registration

Ferndown Middle School uses a voluntary biometric fingerprint recognition system. This is used with the library management administration system. We find this provides the school with a number of very significant benefits including:

- Reduction in administration time and cost dealing with lost or forgotten cards/passwords/PINs
- Students do not have to remember to bring a card
- Reduction in queuing time

In order to comply with the provisions of the Protection of Freedoms Act 2012, we need written permission from a parent in order for students to use the biometric system. Please complete the permission slip below.

The images collected by the fingerprint reader cannot be used to create a whole fingerprint / palm print of your child and that these images will not be shared with anyone outside the school. Once your child ceases to use the biometric recognition system, his/her biometric information will be securely and permanently deleted by the school.

We offer an opportunity to opt out for those pupils who would prefer to use alternative forms of identification. If you would like more information or the chance to discuss this further, please feel free to contact the school.

Biometric Systems Permission Form

Name of Pupil:

Name of Parent / Carer:

I agree to my child using biometric systems for current or future use of the library management until he/she leaves the school. ☐

I do not agree to my child using biometric systems for current or future use of the library management until he/she leaves the school. ☐

Signed

Date

CCC070617/1

Staff and Volunteers Acceptable Use Policy

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- That staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use
- That school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- That staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed E-Safety in my work with young people.

For my professional and personal safety:

- I understand that the school may monitor my use of the systems, devices and digital communications. It should be noted that users should not expect that files stored on servers or disks would be private
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, e-mail, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school
- I will not disclose my username or password to anyone else, nor will I try to use any other staff member username and password. I understand that I should not write down or store a password where it is possible that someone may steal it
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person
- I will not play or display any images, text, audio or video that is inappropriate to any potential audience
- I will not leave a workstation unattended or insecure when I am logged on. To secure the logged on workstation I will lock it so my password must be re-entered before regaining access
- I will not save/cache passwords for internet services that contain personal or sensitive information (e.g. SIMS, MyConcern). If my web browser prompts to save passwords or keep me logged in, I must ensure my credentials are not saved.

I will be professional in my communications and actions when using *school* ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission, except for those belonging to pupils I teach
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured
- I will only use chat and social networking sites in school in accordance with the school's policies
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the *school*:

- I will not eat or drink near computer equipment
- I will not disable or intentionally cause any damage to school equipment, or the equipment belonging to others. I will not waste resources
- I will immediately report any damage or faults involving equipment or software, however this may have happened
- I will immediately report any computer viruses or malware to the Network Manager
- If I am using a laptop trolley I understand that it is my responsibility to collect and return it and that only a member of staff should be taking out and returning laptops to the trolley
- When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement and supporting policy, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses
- I will not use personal email addresses on the school ICT systems
- I will not open any hyperlinks on webpages, unless I know and trust the website. I will not open any hyperlinks in emails or any attachments to emails (unless I know and trust the person / organisation who sent the email), or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will ensure that my data is regularly backed up to the school network, secure cloud storage or to secure secondary USB storage
- I will not try to upload, download, send or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage
- I understand that the School / LA Personal Data Policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary

that I am required by law or by school policy to disclose such information to an appropriate authority.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the *school*:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include relevant sanctions as outlined in the Disciplinary Procedure and in the event of illegal activities the involvement of the police.

Staff loan laptop. Also applies to other types of loaned IT Equipment:

- The laptop remains the property of the school and is to be used only by the member of staff it is issued to
- For insurance and security purposes equipment must not be left in an unattended vehicle
- Anti-virus software must be kept regularly updated
- Must be password protected
- Must not be connected in any way to an unsecured home network
- Must not be accessed by family members or other unauthorised persons
- Must be kept securely or locked away when not in use
- Personal Data – Should it be necessary to take Staff/Pupil data off-site, this must only reside on school loaned equipment
  - Never take more data than is directly relevant to the task
  - Never transfer data to a home PC or other personal device
  - Information must be transferred back to the central system as soon as work is complete and all sensitive data deleted from the device.

Staff and Volunteers Acceptable Use Agreement Form

I have read and understand the above staff and volunteers acceptable use policy as well as the school E-Safety Policy, and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name:	
Signed:	
Date:	

Record of reviewing devices / internet sites, responding to serious incidents of misuse (template)

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and location of computer used for review (for web sites)

Web site(s) address / device	Reason for concern

Conclusion and Action proposed or taken

CCC070617/1

E-Safety Incident Reporting Log

Ferndown Middle School
E-Safety Incident Reporting Log (use more than one row if needed)

Date	Time	Incident details: Include pupil name, class, computer name/location	Action taken		Reported by
			What	By Whom	
e.g. 1/3/2016	e.g. 13:45	Indecent image was displayed in web browser on site www.innocent-pictures.org . Pupil <name> alerted <class teacher name> . Web address and/or search term were noted by <teacher>. Notified network manager. Computer ICT2-21 / ICT2	Web search and displayed page/image validated. School web filter updated to block. SWGfL filtering team notified.	<Network Manager>	<TA Name>

E-Safety Training Needs Audit

Ferndown Middle School **E-Safety Training Needs Audit Log**						
Name	**Position**	**Relevant training in last 12 months**	**Identified training need**	**To be met by**	**Cost**	**Review date**

Technical Security Policy

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that:

- Users can only access data to which they have right of access
- No user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies)
- Access to personal data is securely controlled in line with the school's personal data policy
- Logs are maintained of access by users and of their actions while users of the system
- There is effective guidance and training for users
- There are regular reviews and audits of the safety and security of school computer systems
- There is oversight from senior leaders and these have impact on policy and practice

Responsibilities

The management of technical security will be the responsibility of the Network Manager

Technical Security

Policy statements

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people will receive guidance and training and will be effective in carrying out their 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
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, workstations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff
- All users will have clearly defined access rights to school technical systems. Details of the access rights available to groups of users will be recorded by the Network Manager / Technical Staff (or other person) and will be reviewed, at least annually, by the E-Safety Committee (or other group)
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security. (See Password section below)
- The Network Manager and Senior Finance Officer 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
- Mobile device security and management procedures are in place. Staff, visitors and pupils are not allowed to connect personal devices to the main school wireless network. Temporary access may be granted to supervised visitors in exceptional circumstances
- School technical staff regularly monitors and records the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement
- Remote management tools are used by staff to control workstations and view users activity
- Users should report via e-mail any actual / potential technical incident to the E-Safety Coordinator / Network Manager

- An agreed policy is in place (described in e-Safety Policy) for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school system
- An agreed policy is in place (described in e-Safety Policy) regarding the downloading of executable files and the installation of programmes on school devices by users
- An agreed policy is in place (described in e-Safety Policy) regarding the extent of personal use that users (staff / pupils / community users) and their family members are allowed on school devices that may be used out of school
- An agreed policy is in place (described in e-Safety Policy) regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices.
- The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from malware including viruses, worms and trojans
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, e-mail, Virtual Learning Environment (VLE) and Software As A Service systems.

Policy Statements:

- All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the E-Safety Committee (or other group)
- All school networks and systems will be protected by secure passwords that are regularly changed
- The "master / administrator" passwords for the school systems, used by the technical staff must also be available to the Headteacher or other nominated senior leader and kept in the school safe
- Passwords for new users, and replacement passwords for existing users will be allocated by the Network Manager or nominated Office Staff, dependent upon system (Network, e-Mail, SIMS or other secure web service)
- All users (adults and young people) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- Users will change their passwords at regular intervals – as described in the staff and pupil sections below
- Requests for password changes should be authenticated by the responsible person to ensure that the new password can only be passed to the genuine user.

Staff passwords:

- All staff users will be provided with a username and password (for access to the school network) by the Network Manager who will keep an up to date record of users and their usernames
- the password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters
- must not include proper names or any other personal information about the user that might be known by others
- the account should be "locked out" following five successive incorrect log-on attempts
- temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on
- shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)
- should be different for different accounts, to ensure that other systems are not put at risk if one is compromised
- should be different for systems used inside and outside of school

- Where appropriate should be changed at least every 60 to 90 days.

Pupil passwords

- All users will be provided with a username and password by the Network Manager who will keep an up to date record of users and their usernames
- Users must not share their passwords
- Pupils will be taught the importance of password security
- The complexity (i.e. minimum standards) will be set with regards to the cognitive ability of the children.

Training / Awareness

Members of staff will be made aware of the school's password policy:

- At induction
- Through the school's E-Safety Policy
- Through the Acceptable Use Agreement.

Pupils / students will be made aware of the school's password policy:

- In lessons as part of induction for new year groups and included in regular E-Safety refresher sessions
- Through the Acceptable Use Agreement.

Audit / Monitoring / Reporting / Review

The Network Manager will ensure that full records are kept of:

- User IDs
- Requests for password changes
- Security incidents related to this policy

Filtering

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the internet continually changes, in many cases is dynamically created and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for E-Safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

As filtering services develop and enhancements are introduced, the school will consider introducing the following functionality:

- Differentiated filtering for different groups / ages of users
- Remove filtering controls for some internet use (e.g. social networking sites) at certain times of the day for certain users
- Any changes will only be implemented after discussions and agreement between the Network Manager and the SLT.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the Network Manager, who will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must:

- be logged in change control logs or filtering logs
- be reported to the senior leadership team as and when changes are made in the form of an audit of the change control logs or filtering logs
- be reported to the Curriculum and Community Committee under a standing agenda item at each meeting in the form of an audit of the change control logs or filtering logs.

All users have a responsibility to report immediately to the E-Safety Co-Ordinator, any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for authorised staff and customised filtering changes are managed by the school. Illegal content is filtered by the filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system.

- The school maintains and supports the managed filtering service provided by SWGfL/RM
- The school has provided enhanced / differentiated user-level filtering through the use of the RM SafetyNet filtering programme (allowing different filtering levels for different ages / stages and different groups of users – staff / pupils / students etc.)
- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher.
- Mobile devices that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems
- Any filtering issues should be reported immediately to the filtering provider
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Group.

Education / Training / Awareness

Pupils will be made aware of the importance of filtering systems through the E-Safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- The Acceptable Use Agreement
- Induction training
- Staff meetings, briefings, INSET.

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through E-Safety awareness sessions / newsletter etc.

Changes to the Filtering System

Changes to the school filtering system can be requested:

- Staff may request changes to the filtering by sending an e-mail to the Network Manager, including accurate details of the relevant URL(s), access change required and reason. If an e-mail cannot be sent, then a signed, written request including all relevant details must be submitted.
- The grounds on which the request may be allowed or denied should be based on strong educational reasons.
- As a result of audit or review of logs.

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to E-Safety Co-Ordinator who will decide whether to make school level changes (as above).

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School E-Safety Policy and the Acceptable Use Agreement.

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- the senior leadership team
- E-Safety Governor / Governors committee
- External Filtering provider / Local Authority / Police on request.

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision. The evidence might show a large number of requests to remove the filtering from sites – in which case schools might question whether their current level of filtering is too restrictive for educational purposes. Alternatively, a large number of incidents where users try to subvert the filtering system might suggest that improved monitoring / disciplinary action might be necessary.

Fair Processing Privacy Notice

Name …….. Form ……..

FERNDOWN MIDDLE SCHOOL
Peter Grant Way Ferndown Tel: 876556

Privacy Notice - Data Protection Act 1998

We Ferndown Middle School are a data controller for the purposes of the Data Protection Act. We collect information from you and may receive information about you from your previous school and the Learning Records Service. We hold this personal data and use it to:

- Support your teaching and learning;
- Monitor and report on your progress;
- Provide appropriate pastoral care, and
- Assess how well your school is doing.

This information includes your contact details, national curriculum assessment results, attendance information and personal characteristics such as your ethnic group, any special educational needs and relevant medical information. If you are enrolling for post 14 qualifications we will be provided with your unique learner number (ULN) by the Learning Records Service and may also obtain from them details of any learning or qualifications you have undertaken.

We will not give information about you to anyone outside the school without your consent unless the law and our rules allow us to.

We are required by law to pass some information about you to the Local Authority and the Department for Education (DfE)

Once you are aged 13 or over, we are required by law to pass on certain information to providers of youth support services in your area. This is the local authority support service for young people aged 13 to 19 in England. We must provide both your and your parent's/s' name(s) and address, and any further information relevant to the support services' role. However, if you are over 16, you (or your parent(s)) can ask that no information beyond names, address and your date of birth be passed to the support service. Please inform Mrs Dale in the school office if you wish to opt-out of this arrangement.

If you want to see a copy of the information we hold and share about you then please contact Mrs Dale.

For more information about young peoples' services, please go to the Directgov Young People page at www.direct.gov.uk/en/YoungPeople/index.htm or to the LA website shown below.

If you require more information about how the Local Authority (LA) and/or DfE store and use your information, then please go to the following websites:

https://www.dorsetforyou.com/schools
https://www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data

CCC070617/1

If you are unable to access these websites we can send you a copy of this information. Please contact the LA or DfE as follows:

If you are unable to access these websites, please contact the LA or the DfE as follows:

Data Protection Officer Records Management
Dorset County Council
Colliton Park
DORCHESTER
Dorset
DT1 1XJ
website: www.dorsetforyou.com
email: d.j.wilson@dorsetcc.gov.uk
Telephone: 01305 225175

Public Communications Unit, Department for Education
Sanctuary Buildings, Great Smith Street, London
SW1P 3BT
Website: www.education.gov.uk
email: http://www.education.gov.uk/help/contactus
Telephone: 0370 000 2288

Legislation

Schools should be aware of the legislative framework under which this E-Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.
It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority
- Obtain unauthorised access to a computer
- "Eavesdrop" on a computer
- Make unauthorised use of computer time or facilities
- Maliciously corrupt or erase data or programs
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Not kept longer than necessary
- Processed in accordance with the data subject's rights
- Secure
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts
- Ascertain compliance with regulatory or self-regulatory practices or procedures

- Demonstrate standards, which are or ought to be achieved by persons using the system
- Investigate or detect unauthorised use of the communications system
- Prevent or detect crime or in the interests of national security
- Ensure the effective operation of the system
- Monitoring but not recording is also permissible in order to:
    - Ascertain whether the communication is business or personal
    - Protect or support help line staff
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an

indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education.

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent / carer to use Biometric systems

The School Information Regulations 2012

Requires schools to publish certain information on its website:
https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

CCC070617/1

Glossary of terms

AUP	Acceptable Use Policy – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPC	Child Protection Committee
CPD	Continuous Professional Development
CYPS	Children and Young Peoples Services (in Local Authorities)
FOSI	Family Online Safety Institute
EA	Education Authority
ES	Education Scotland
HWB	Health and Wellbeing
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by NAACE
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational e-safety programmes for schools, young people and parents.
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol