Ferndown First School

E-Safety Policy

Reviewed September 2015 in line with Prevent Duty

Background

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 and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and children / pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies).
As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build children' / pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

Development / Monitoring / Review of this Policy

This e-safety policy was originally developed by a working group made up School E-Safety Champion, Headteacher ICT staff, Governors, Parents and Carer

Consultation with the whole school community took place through the following: Staff meeting, Pupil Council, Governors meeting, School website / newsletters

This policy applies to all members of the school community (including staff, children / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

Roles and Responsibilities

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports

The Headteacher is responsible 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 Champion
- ensuring that the E-Safety Champion and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- The Headteacher 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.
- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The Headteacher will follow the most up to date guidance from SWGfl

E-Safety Champion

- 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
- liaises with school ICT staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
- meets with Safeguarding Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors

Network Manager:

The Network Manager is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed.
- SWGfL is informed of issues relating to the filtering applied by the Grid. The school's filtering policy, which is provided by SWGFL is overseen by the ICT systems manager. This is also monitored by the E Safety Governor.
- that he / she keeps 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
- that the use of the network / remote access (when implemented) is monitored in order that any misuse / attempted misuse can be reported to the E-Safety Champion and Headteacher.

Teaching and Support Staff:

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 practice
- they have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP
- they report any suspected misuse or problem to the E-Safety Champion or Headteacher for investigation / action / sanction
- digital communications with children (email /online/voice) 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 school activities

- children understand and follow the school e-safety and acceptable use policy
- they monitor ICT activity in lessons and extra curricular school activities and provide parents with advice on safe use of ICT outside of school.
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned children should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead:

- should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:
    - sharing of personal data
    - access to illegal / inappropriate materials
    - inappropriate on-line contact with adults / strangers
    - potential or actual incidents of grooming
    - cyber-bullying

Children

- are responsible for using the school ICT systems in accordance with the Children's Acceptable Use Policy, which parents will be expected to sign before being given access to school systems.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so (visual reminders near computers)
- should understand the importance of adopting good e-safety practice when using digital technologies out of 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 and information about national / local e-safety campaigns / literature.

- Parents and carers will be responsible for:
    - endorsing (by signature) the Acceptable Use Policy
    - accessing the school website in accordance with the relevant school Acceptable Use Policy.

Prevent Duty - How to protect children from online extremism

The new Counter-Terrorism and Security Act 2015 obliges schools (and other authorities) to prevent people from being drawn into terrorism including online

At Ferndown First School we will

- Assess the risk of a child being drawn into terrorism and their support for extremist ideas.
- using robust safeguarding policies to identify children at risk,

- Devise a relevant intervention plan and select the most appropriate referral option.

- Work in partnership with your local safeguarding children board to ensure you're following the correct policies and procedures.

- Train staff to identify children at risk of being drawn into terrorism and challenge extremist ideas, recognise the signs of extremism and counter the online extremism rhetoric

- Implement strict IT policies that allow for an appropriate level of filtering.

- Take responsibility for reporting concerns. It is now the law for any individual to follow the appropriate safeguarding reporting procedure.

Policy Statements

Education - Children

E-Safety education will be provided in the following ways:

- A planned e-safety programme should be provided as part of ICT / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key e-safety messages should be reinforced as part of a planned programme.
- Children / 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
- Children / pupils should be helped to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Rules for use of ICT systems / internet will be posted by computers.
- Staff should act as good role models in their use of ICT, the internet and mobile devices
- Education – parents / carers
- The school will therefore seek to provide information and awareness to parents and carers through:
- Letters, newsletters, website, workshops and reference to the SWGfL website

Education - Staff

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:

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly. This will be linked to safe guarding training.
- 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 Policies
- The E-Safety Champion (or other nominated person) will receive regular updates through attendance at CPD.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safety Champion (or other nominated person) will provide advice / guidance / training as required 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 sub committee / group involved in ICT / e-safety / health and safety / child protection and safeguarding

Curriculum

- E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.
- in lessons where internet use is pre-planned, it is best practice that children / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where children / pupils are not allowed to freely search the internet, eg using search engines

Use of digital and video images

- When using digital images, staff should inform and educate children / 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.
- Staff 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 children / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Parents must not share, publish or distribute images of others without their permission and must not publish images taken at school online.
- Photographs published on the website, or elsewhere that include children / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Children' / 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 children / pupils are published on the school website. (induction permission slip)

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.

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 where appropriate. (This is being investigated.)

Communications (Taken from Camera and Mobile Phone Acceptable Use Policy)

- Ferndown First School allows staff to bring in personal mobile telephones and devices for their own use on the strict understanding that:
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device
- Under no circumstance does the school allow a member of staff to contact a current pupil or parent/carer using their personal device
- All staff must ensure that their mobile telephones/devices are placed in a secure place unless requested by the Headteacher to move them to another appropriate location
- During off duty periods eg: lunch breaks the staff are permitted to use their mobile phones in designated areas.

- With the exception of the caretaker and site manager, no staff are allowed to keep mobile phones in their pockets whilst on duty.
- If staff have a personal emergency they can ask to use the school's phone or make a personal call from their mobile in the designated areas.
- If any staff member has a specific family emergency and are required to keep their mobile phone to hand, prior permission must be sought from the Headteacher.
- Staff will need to make their families, children's schools etc. aware of emergency work telephone numbers. This is the responsibility of the individual staff member

- It is the responsibility of all members of staff to be vigilant and report any concerns to the Headteacher.

All parent helpers will be requested to place their bag containing their phone in a secure area or another appropriate location and asked not to take or receive any calls whilst on the premises.

Cameras

- The school cameras including I-Pads are for the sole use of photographing children taking part in activities and used for developmental records.
- Photographs will only be taken of those children whose parents have signed the relevant consent form
- School cameras must be used or the school memory card should be put into personal cameras.
- Staff must seek permission before using personal cameras
- Only designated cameras are to be used to take any photo within the school, with the permission of the Headteacher
- The memory card should then be removed and the content loaded onto a school computer not a personal computer by nominated members of staff
- Images taken must be deemed suitable without putting the child/children in any situation that could cause embarrassment or distress.
- Photographs should not be taken in the toilets.
- Senior colleagues reserve the right to check the image content of a member of staff's mobile phone, should there be any cause for concern over the appropriate use of it.
- Concerns will be taken seriously, logged and investigated appropriately (see Handling Allegations Policy)
- Should inappropriate material be found then the DSL Safeguarding will be contacted immediately and the appropriate Disciplinary Procedure instigated.
- Parents or visitors are not allowed to use cameras at school unless a specific announcement has been made at the start of the event and any photographs taken are for personal use only and are not be posted on social networking sites or similar internet/public domains.

Unsuitable / Inappropriate activities

Some internet activity eg accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities eg Cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

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.

		Acceptable at certain times	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**			X
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation			X
	adult material that potentially breaches the Obscene Publications Act in the UK			X
	criminally racist material in UK			X
	pornography		X	
	promotion of any kind of discrimination		X	
	promotion of racial or religious hatred		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	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school			X	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions			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	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and 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 networking sites		X		
Use of video broadcasting eg YouTube		X		

Social Networking Sites

Children will not be allowed on social networking sites

- Staff should not access social networking sites on school equipment in school or at home. Staff should access sites using personal devices
- Staff users should not reveal names of staff, children, pupils, parents/carers or any other member of the school community on any social networking site or blog.
- Children/Parents/carers should be aware the school will investigate misuse of social networking if it impacts on the well-being of other children or stakeholders.

If inappropriate comments are placed on social networking sites about the school or school staff then advice would be sought from the relevant agencies, including the police if necessary and sanctions will be imposed. Where the abuse is bullying or racism this will also trigger sanctions under those policies.

Children will be taught about e-safety on social networking sites in an age appropriate way.

Digital Images

- The school record of parental permissions granted/not granted must be adhered to when taking images of our children.

- A list is published to all Base Leaders but can also be obtained from the school office

- Under no circumstances should images be taken using privately owned equipment without the express permission of the Headteacher
- the ICT Champion.

- Where permission is granted the images should be transferred to school storage systems (server or disc) and deleted from privately owned equipment at the earliest opportunity.

- Although many of the above points are preventative and safeguarding measures, it should be noted that the school will endeavour whenever possible to use social networking in positive ways to publicise, inform and communicate information. The school has an active website which is used to inform, publicise school events and celebrate and share the achievement of children.

Removable Data Storage Devices

- Only school authorised removable media should be used

- All files downloaded from the Internet, received via e-mail or provided on removable media (eg. CD, DVD, USB flash drive, memory cards etc) must be checked for viruses using anti-virus software provided before run, opened or copied/moved on to local/network hard disks.

- Children should not bring their own removable data storage devices into the school unless asked to do so by a member of staff.

Websites

In lessons where Internet use is pre-planned, children should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.

- Staff will preview any recommended sites before use.
- “Open” searches (e.g. “find images/ information on...”) are discouraged when working with younger children who may misinterpret information.
- If Internet research is set for home learning, specific sites will be suggested that have previously been checked by staff.
- Parents will be advised to supervise any further research.
- All users must observe copyright of materials published on the Internet.
- Children are allowed access to the internet only supervision.

Passwords

Staff

- Passwords or encryption keys should not be recorded on paper or in an unprotected file
- Passwords should be changed when directed
- Users should not use the same password on multiple systems or attempt to “synchronise” passwords across systems

Use of Own Equipment

- Privately owned ICT equipment should never be connected to the school's network without the specific permission of the Headteacher or Network Manager.
- Children should not bring in their own equipment
- Use of School Equipment
- No personally owned applications or software packages should be installed on to school ICT equipment;
- Personal or sensitive data (belonging to staff) should not be stored on the local drives of desktop or laptop PCs. If it is necessary to do so, the local drive must be encrypted.
- All should ensure any screens are locked (by pressing Ctrl, Alt, Del simultaneously) before moving away from a computer during the normal working day to protect any personal, sensitive, confidential or classified data and to prevent unauthorised access.

Monitoring

- All use of the school's Internet access is logged and the logs are randomly but regularly monitored.
- Whenever any inappropriate use is detected it will be followed up by the E-Safety Champion or members of the Senior Leadership Team depending on the severity of the incident.
- E-Safety Champion and Network Manager will log and record any breaches, suspected or actual, of the filtering systems
- Any member of staff employed by the school who comes across an e-safety issue does not investigate any further but immediately reports it to the E-safety Champion or relevant Base Leader and impounds the equipment. This is part of the school safeguarding protocol.
- If the concern involves the E-Safety Champion then the member of staff should report the issue to the Headteacher
  Staff should keep any records of the abuse – text, e-mails, voice mail, web site or instant message. Screen prints of messages or web pages should be taken and time, date and address of site should be recorded.
  Staff should inform the nominated person of incidents at the earliest opportunity.
- Monitoring and confiscation must be appropriate and proportionate.
- Where a potential criminal offence has been identified, and reported to the police, the federation will ensure that any internal investigation does not interfere with police inquiries
- Where pupils are found to have made unfounded, malicious claims against staff members, relevant and appropriate disciplinary processes will be applied.
- Staff should report all incidents to the nominated person. The nominated person will take responsibility for ensuring the person being bullied is supported, for investigating and managing the incident, and for contacting the police and Local Authority if appropriate.

Action for Inappropriate Use of Social Networking Sites

Following a report of inappropriate use of social networking sites, the nominated person will take the following action:

Where online content is upsetting and inappropriate, and the person or people responsible for posting are known, the nominated person will explain why the material is unacceptable and request that it be removed. If the person responsible has not been, or cannot be, identified, or will not take material down, the nominated person will contact the host (for example, the social networking site) with a view to removal of the content. The material posted may breach the service provider's terms and conditions of use and can then be removed

In cases where the victim's personal identity has been compromised – for example, where a site or an online identity alleging to belong to the victim is being used, the nominated person will support the victim in establishing their identity and lodging a complaint directly with the service provider.

The governors recognise their legal duty to protect staff from unlawful harassment as well as mental and physical injury at work

In cases of potentially criminal content, the nominated person will consider whether the police should be involved, following appropriate liaison with staff, and parents where necessary.

How to Stay 'Cybersafe' – Do's and Don'ts

Staff should:

- keep passwords secret and protect access to accounts;
- not "befriend" children, pupils or parents/carers on social networking sites.
- keep personal phone numbers private and not use their own mobile phones to contact pupils or parents;
- keep a record of their phone's unique International Mobile Equipment Identity (IMEI) number,
- keep phones secure while in school premises and report thefts to the police and mobile operator as soon as possible;
- ensure that school rules regarding the use of technologies are consistently enforced;
- report any incident to the appropriate member of staff in a timely manner;
- keep any evidence of an incident, for example by not deleting text messages or e-mails and by taking a screen shot

If staff are related to pupils or ex- pupils and wish to have them as "friends" they should let school management know

Staff should not:

- personally retaliate to any incident;
- post information and photos about themselves, or federation -related matters, publicly that they wouldn't want employers, colleagues, children, pupils or parents to see;

This policy has been reviewed in line with the 9 principles set out in the Single Equality Policy and an initial screening Equality Impact Assessment has been carried out.

Reviewed and ratified: 26th March 2015

Amended on 21st September – in line with Prevent Duty

Date of next review: 26th March 2016 (Annually)

Appendix 1

Ferndown Firsts School
Staff Acceptable Use Agreement

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. All users should have an entitlement to safe internet access.

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 users and systems are protected from accidental or deliberate misuse that could put the security of the users and systems at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work. (safer working practices)

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 children's 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 children 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 children.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, VLE etc) out of school. (schools should amend this section in the light of their policies which relate to the use of school systems and equipment 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. (schools should amend this section in the light of their policies which relate to the personal use, by staff and volunteers, of school systems)
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

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

- I will not maliciously access, copy, remove or otherwise alter any other user's files, without their express permission.
- 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 (eg 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 children / 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:

- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, 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 only use personal email addresses on the school ICT systems at designated times. (ie lunch break, after school)
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download 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 knowingly 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. (schools should amend this section in the light of their policies on installing programmes / altering settings)
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School's Personal Data Policy
- I understand that data protection policy requires that any staff or child's 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.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

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 if I am responsible for supervising volunteers I am required to give guidance and supervise the volunteers use of ICT including how children use the equipment. Helpers are not permitted to use ICT for personal use

I understand that I am responsible for my actions in and out of 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 out of school and my use of personal equipment in school 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 a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above 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

Staff Name

Signed **Date**

Appendix 2

Ferndown Firsts School
Parent/Carer Acceptable Use Agreement

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. Children should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that children 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 parents and carers are aware of the importance of e-safety and are involved in the education and guidance of children with regard to their on-line behaviour.

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

I know that my son / daughter will receive e-safety education to help them understand the importance of safe use of ICT – 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.

I understand that if I am helping in school I will ensure my mobile phone is kept securely when I am working with children. Similarly when helping on a school trip I will keep my mobile phone secure and only use in accordance with guidance given.

I understand that if I am helping in school I am not permitted to use school ICT equipment for personal use.

Name of my Child

Class

Signed by Parent/ Carer - **Date**

FERNDOWN FIRST ISCHOOL

Personal Data Handling Policy

Staff should ensure the safety and security of any material of a personal or sensitive nature. Care should be taken when handling, using or transferring personal data so that it cannot be accessed by people not authorised to do so – Beta 2008)

Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances.

This will include:

- Personal information about members of the school community – including *pupils / children,* members of staff and parents and carers egg names, addresses, contact details, legal guardianship / contact details, health records, disciplinary record
- Curricular / academic data egg class lists, pupil / student progress records, reports, references
- Professional records egg employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members

Responsibilities

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner. Governors are required to comply fully with this policy in the event that they have access with personal data, when engaged in their role as a Governor.

Secure Storage of and access to data

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

The school will ensure that ICT systems are set up so that access to information on IT systems is limited to authorised users only. All users will be given secure user names and passwords. User names and passwords must never be shared.

Personal data can only be stored on school equipment (this includes computers and portable storage media). Private equipment (i.e. owned by the users) must not be used to store personal information. When personal data is stored on any portable computer system, USB stick or any other removable media care must be taken to ensure it is kept safe. The school is currently investigating the use of encryption.

The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.

The school recognises that under Section 7 of the Data Protection Act, data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place – Privacy Notices and Access to Personal Files Policy (for staff) to deal with Subject Access Requests

Disposal of data

The school will ensure the safe destruction of personal data when it is no longer required.
The disposal of protected data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance and other media must be shredded, incinerated or otherwise disintegrated for data.

Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies

Users may not remove or copy sensitive or personal data from the school or authorised premises without permission

Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (egg family members) when out of school.