Whitstone Community Primary School

E-Safety Policy

Whitstone C.P. School
E-Safety Policy

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, who have access to and are users of school ICT systems.

The Education and Inspections Act 2006 empowers Head teachers 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. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

This policy should be read in conjunction with the school's policies on Bullying, Safeguarding, Behaviour, Data Protection and Computing.

Roles and Responsibilities

Governors / Board of Directors:
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 E- Safety governor is

The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Co-ordinator
- regular monitoring of e-safety incident logs
- reporting to Governors

Head teacher and Senior Leaders:

- The Head teacher 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 Head teacher , Senior teacher and E-Safety coordinator are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The Head teacher is responsible for ensuring that the E-Safety Coordinator 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 Head teacher 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
- The Head teacher will receive regular monitoring reports from the E-Safety Co-ordinator.

E-Safety Coordinator:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policy.
- 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 school technical staff (NCi)
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- meets annually (or more regularly if there is an issue) with E-Safety Governor to discuss current issues, review incident logs.
- reports regularly to the Head teacher.

Technical Staff (NCi)

The ICT Technician is responsible for ensuring that:

- the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- users may only access the school's networks through a properly enforced password protection policy
- shortcomings in the infrastructure are reported to the ICT coordinator or head teacher so that appropriate action may be taken.

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 Acceptable Use Policy
- they report any suspected misuse or problem to the Headteacher / Senior Leader ; E-Safety Coordinator for investigation.
- all digital communications with students / 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
- students / pupils understand and follow the e-safety and acceptable use policies
- students / pupils have a good understanding of research skills
- 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 students / 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

Designated Person for Safeguarding and Child Protection

The designated person for child protection, Paul Woolner (Head teacher) and Becky Towe (the Deputy), are trained in e-safety issues and aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Students / pupils:

- are responsible for using the school digital technology systems in accordance with the Student / Pupil Acceptable Use Policy. Children in Key stage 2 will to sign to say they will follow the Acceptable use policy

Parents / Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Parents and carers will be encouraged to sign the Parent/ Carer acceptable use Policy and 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
- their children's personal devices in the school (where this is allowed)

For further information about e-safety please visit the website below.

http://www.childnet.com/parents-and-carers

Policy Statements

Education – pupils
Children will be given the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety will be a focus in all areas of the curriculum and staff reinforce e-safety messages across the curriculum. The e-safety curriculum will be provided in the following ways:

- A planned e-safety curriculum as part of Computing / PHSE / other lessons and which is revisited regularly
- Students / 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 are encouraged to adopt safe and responsible use both within and outside school and Key stage 2 pupils will understand and sign the Acceptable use policy.

- 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 students / 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 students / pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

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 online 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. This may be done through:

- Letters, newsletters, web site, VLE
- Parents / Carers evenings /sessions
- Reference to the relevant web sites / publications eg www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Staff and governor training
This school

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection (for further information, see the school's Data Protection Policy);
- Makes regular training available to staff on e-safety issues and the school's e-safety education program.
- Provides ,as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the eSafeguarding policy and the school's Acceptable Use Policies.

Communications

At Whitstone School the internet will be used to communicate with others in a range of different ways, including through: emails, blogs and webcams.

Users must immediately report, to the nominated person (Paul Woolner- headteacher), 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. The school will contact the Police if one of our staff or pupils receives any form of communication that we consider to be particularly disturbing or that breaks the law.

Emails:

Whitstone School uses RM Easy Mail to provide children and staff with email accounts. These official school email services may be regarded as safe and secure and are monitored.

Children:

•At Whitstone School children use class accounts, run by RM Easy Mail.

•In school they will only be able to communicate with individuals who have been approved by members of staff.

•Will be made aware that all emails on the school network are monitored.

•Will be given a structured education programme that makes them aware of the dangers of and good practices associated with the use of email (see 'Education-Pupils').

•Should use only the school email services to communicate with others when in school.

•Must follow the school rules when sending emails.

Staff:

•Staff should not use their school email address for personal or business use.

•Will be made aware that their emails may be monitored.

•School email addresses are the preferred email address for professional business.

•Any emails sent must be professional in tone and content (for further details, see 'Professional Standards for Staff Communication' section). Personal emails should not be used to contact pupils & parents.

Blogs/ Wiki Pages

Blogs/ Wiki pages may be used to support Computing lessons and other curriculum areas. To ensure the safety of users staff will ensure that:

- Only educational, whole class blog websites are used and that these are password protected.
- Full names of the children in the class will not be used
- Children understand how to communicate respectfully online; any comments made by children will not be published until they have been approved by members of staff.
- The use of images complies with school policy (see 'Use of digital and video image' section of this policy)

Video Conferencing

At times the School may be used video conferencing to support learning in the classroom, for example to communicate with guest speakers or to practise foreign languages.

At Whitstone School we:

•Only use approved or checked webcam sites, such as Skype.

•Ensure children will only take part in whole class video conferencing activities, which are supervised and organised by members of staff.

•Seek parental permission before allowing children to take part in video conferencing.

•Ensure all Video conferencing equipment in classrooms is switched off when not in use and not set to auto answer.

•Will not put Videoconferencing contact information on the school website.

•Only give unique log on and password details for the educational videoconferencing services to members of staff.

•Only use accounts created in the name of the school.

•Only key administrators have access to videoconferencing administration areas.

•Carryout appropriate checks on any guest speakers.

Use of web-based publication tools

Website (and other public facing communications)

Our school website (***whitstone.cornwall****.sch.uk/*) is used for sharing information with the community beyond our school. This includes, from time-to-time celebrating work and achievements of children. All users are required to consider good practice when publishing content:

• Uploading of information is restricted.

• The school web site complies with the statutory DfE guidelines for publications;

• Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;

•Personal information should not be posted on the school website and only the general school email will be published (secretary@whitstone.cornwall.sch.uk).

•Only pupil's first names are used on the website, and only then when necessary.

• Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images (for further information see 'Use of digital and video images' section):

• pupils' full names will not be used anywhere on a website or blog, and never in association with photographs
•We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;
•Written permission from parents or carers will be obtained before photographs of pupils are published on the school website (this will normally be done when children enter the school).

Professional standards for staff communication
In all aspects of their work in our school teachers abide by the Teachers' Standards as described by the DfE (http://media.education.gov.uk/assets/files/pdf/t/te
achers%20standards.pdf.)

Teachers translate these standards appropriately for all matters relating to e-safety. Any digital communication between staff and pupils or parents / carers (email, chat, website etc) must be professional in tone and content.
•These communications may only take place on official (monitored) school systems.
•Personal email addresses, text messaging or public chat / social networking technology must not be used for these communications.

When using the internet for personal use staff should ensure that:

- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions are not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Use of digital and video images

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.

•Members of staff are allowed to take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should be captured using school equipment; the use of personal equipment of staff is not encouraged. Where personal equipment is used, then the permission of the headteacher (Paul Woolner) should be sought before use. If it personal equipment is used then the images must be deleted once they have been downloaded to the school network or printed. No images should be used for personal, illegal or business use.

•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 permission

• With permission from the headteacher, parent/carers may take digital/ video images of pupils at school events. However, they will be asked not to share these on public platforms without permission (Facebook etc).

Mobile Devices

•It is a school rule that pupils should not have personal mobile phones or devices in school. Pupils will be allowed to use the school phone if they should need to.
•If a pupil brings an unauthorised phone or mobile device to school, it will be confiscated and given to the child's parents or carers at the end of the day.
•Pupils will be taught how to use mobile devices safely and responsibly, as part of the Computing curriculum.
•If staff do have an educational reason to allow children to use personal mobile phones or devices, then the headteacher (Paul Woolner) must give permission before their use.
•Mobile phones should not be used in 'vunerable' areas. Eg. toilets, changing areas etc.
•Staff may need to use mobiles for work-related duties. Should they need to use their own devices, they may need to hide their number for confidentiality purposes. This can be done by inputting 141.
•Staff are encouraged to use school devices to take images. If personal mobile devices are used, then permission from the headteacher should be sought (for further guidance see section on 'use of digital and video images).
•Parents should also seek the headteacher's permission before taking digital/ video images on personal devices (see 'use of digital and video images' section).
•Mobile phones brought into school are entirely at the staff member, student's, parent's or visitor's own risk. The school accepts no responsibility for the loss, theft or damage of any mobile devices.
•Staff should not use mobile phones during lesson time, unless there are exceptional circumstances and the head teacher has given them permission to.

Passwords

The school's internet connection is password protected.
To access the network, pupils in Key Stage 1 will use a shared password and username (whitstone/pupil). Older children in the school will be encouraged to use their own login details and as part of the Computing curriculum they will learn about the importance of passwords.

Members of staff have also have individual logins and passwords to access teacher area of the network and email accounts. Staff must ensure that these remain private and are not left where others may find them.

Infrastructure

Filtering

The school's filtering system is managed by the SWGfL (South West Grid for Learning).

As 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.

Users will also be required to notify the esafety co-ordinator/ head teacher of any failures in the filtering systems. These should then be reported to SWGfL and NCi. Staff may request for certain websites to be unblocked, where appropriate.

Users will also be made aware of the school's appropriate use policies (see pupil, staff, parent agreements).

Security (Virus Protection)

The School uses virus protection software to protect the network and this is regularly updated by the school's ICT technicians (NCi). This is used to scan and block unsafe internet pages and emails. In addition, it prevents children from downloading internet files on pupil accounts.

Staff and administrator accounts are able to download internet files. However, staff are encouraged to scan these before opening them on the school's network. The school's virus protection software should also before opening personal devices, such as memory sticks.

Before new software is downloaded and installed on the school network, staff should contact Mr Lawrence and NCi for authorisation.

Children must not download programs or install apps onto the school network or devices.

Asset disposal

Details of all school-owned hardware will be recorded in a hardware inventory.
Details of all school-owned software will be recorded in a software inventory.
All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen
Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

Staff constantly monitor and evaluate developing technologies, balancing risks and benefits, and consider how appropriate these are for learning and teaching. These evaluations help inform policy and develop practice. The views and experiences of pupils are used to inform this process also.

Next Steps:
-Ensure all members of the school community are aware of the contents of the e-safety policy and agreements.
-Raise parental awareness of esafety by providing links/ pamphlets.
-Set up an esafety log.
-Ensure that esafety is embedded into the computing curriculum.

This e-safety policy was approved by the *Governing Body*	
The implementation of this e-safety policy will be monitored by the:	*Head teacher*
Monitoring will take place at regular intervals:	Annually
Governing Body will receive a report on the implementation of the e-safety policy (which will include anonymous details of e-safety incidents) at regular intervals:	*Annually*
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:	*October 2015*
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*LA ICT Manager, LA Safeguarding Officer, Police*

Parent / Carer Acceptable Use Policy 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. 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 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 young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Student / Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent / Carers Name	
Student / Pupil Name	

As the parent / carer of the above pupils, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or 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.

Signed Date

Staff (and Volunteer) Acceptable Use Policy 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. 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 students / 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 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 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 person's 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 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.
- 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) it will not be possible to identify by name, or other personal information, those who are featured.
- I will not use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with students / 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 / academy*:

- 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, 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 open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , 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, 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 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 / academies 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 / academy 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 / Academy / LA Personal Data Policy (or other relevant 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 data protection 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.
- 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 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 / academy
- 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 / Directors 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 / Volunteer Name

Signed

Date

Key Stage 1 pupil agreement

I will ask for permission from a member of staff before using the computers in school.

I will ask for permission from a member of staff before using the Internet.

I will only use the computers in school for school work or homework.

I will not bring in and use any portable device (i.e.USB stick) from outside school without asking a member of staff.

I will tell a member of staff if I see anything unpleasant or that I am unhappy with on the computer.

I will always be kind to others when working online and on the computer.

I know that school staff may check the Internet sites I visit.

I know the school may check my computer files.

I understand that if I deliberately break these rules I could be stopped from using the school's computers.

Key Stage 2 pupil agreement

I will ask for permission from a member of staff before using the computers and internet in school.

I will only use the computers in school for school work or homework.

I know that school staff may check the Internet sites I visit.

I will not bring in and use any portable device (i.e.USB stick) from outside school without asking a member of staff.

I will not use my own mobile devices in school (tablets, phones, cameras etc), unless I have permission.

I will ask for permission before taking and using photos.

I will tell a member of staff if I see anything unpleasant or that I am unhappy with on the computer.

I know about ‘stranger danger’ and will not share personal information when working online, such as my telephone number, address etc.

I understand that my passwords should be kept private.

I will always be polite to others when working online.

I will not damage anyone else’s work.

I will not download programs or apps onto the school computers or ipads.

I will not alter computer settings (eg. screen savers etc).

I know the school may check my computer files.

I understand that if I deliberately break these rules I could be stopped from using the school's computers.