Petersfield E-Safety Policy 2018

Version	Final
Policy Type	Standards
Discussed by staff	May 2018
Approved by the Headteachers	May 2018
Adopted by the FGB	June 2018
Next Review	Summer 2019

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, at Petersfield we need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

E-safety involves pupils, staff, governors and parents making best use of technology, information, training and this policy to create and maintain a safe online and ICT environment for Petersfield School.

"As in any other area of life, children and young people are vulnerable and may expose themselves to danger - knowingly or unknowingly - when using the Internet and other digital technologies. Indeed, some young people may find themselves involved in activities which are inappropriate or possibly illegal.
"To ignore e-safety issues when implementing the requirements of Every Child Matters could ultimately lead to significant gaps in child protection policies, leaving children and young people vulnerable."
From: Safeguarding Children in a Digital World. BECTA 2006

Our e-safety Policy has been written following government guidance, it has been agreed by pupils, staff, senior management and approved by governors.

- The school's E-safety Lead is Mr Carter.
- The e-Safety Governor is Damian Hales
- The e-safety Policy and its implementation shall be reviewed annually.

Roles and Responsibilities
Governors:
Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. The role of the E-Safety Governor will include:

- Regular meetings with the E-Safety Lead.
- Regular monitoring of e-safety incident logs.
- Reporting to the Standards Committee.

Headteachers and Senior Leaders:

- The Headteachers are 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 Lead.
- The Headteachers/Senior Leaders are responsible for ensuring that the E-safety Lead 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 Headteachers/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of teachers 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 Headteachers and Senior Leaders together with all staff 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 E-Safety Lead:

- Takes day-to day-responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policy/documents.
- Works with the Designated Child Protection Lead to address any Safeguarding issues. As detailed in our Child Protection and Safeguarding 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 ICT technical staff.
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.

Teaching and Learning

The Internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and so the school has a duty to provide pupils with quality Internet access as part of their learning experience:

- The school Internet access will be designed expressly for pupil use including appropriate content filtering.
- Pupils will be given clear objectives for Internet use and taught what use is acceptable and what is not.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- As part of the new ICT (computing) curriculum, all year groups have digital literacy units that focus on different elements of staying safe on line. These units include topics from how to use a search engine, digital footprints and cyber bullying.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Through ICT we ensure that the school meets the needs of all, taking account of gender, ethnicity, culture, religion, language, age, ability, disability and social circumstances. It is important that in this school we meet the diverse needs of pupils to ensure inclusion for all and that all pupils are prepared for full participation in a multi-ethnic society. We also measure and assess the impact regularly through meetings our SENDCo and individual teachers to ensure all children have equal access to succeeding in this subject.

Pupils are taught in all lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information

Authorised Internet Access

By explicitly authorising use of the school's Internet access, pupils, staff, governors and parents are provided with information relating to e-safety and agree to its use:

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.

- Parents will be informed that pupils will be provided with supervised Internet access and asked to sign and return a consent form for pupil access.
- Only authorised equipment, software and Internet access can be used within the school.

World Wide Web

The Internet opens up new opportunities and is becoming an essential part of the everyday world for children: learning, homework, sharing are some of the legitimate and beneficial uses. However, there are inappropriate and undesirable elements that must be managed:

- If staff or pupils discover unsuitable sites, the URL (address), time and content shall be reported to the teacher who will then complete an E-Safety Incident form and hand this immediately to the E-Safety Lead. The E-Safety Lead will report to the Headteacher, file the E-Safety Incident form in the HT files and complete the SLT E-Safety Log. The e-Safety Log will be reviewed termly by the e-Safety Lead.
- Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.
- The school will work in partnership with the Local Authority to ensure filtering systems are as effective as possible.

E-mail

- E-mail is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of e-safety:
- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Whole class or group e-mail addresses should be used in school rather than individual addresses.
- Access in school to external personal e-mail accounts is not allowed.
- E-mail sent to external organisations should be written carefully and authorised by the teacher before sending..
- Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding.

Security and passwords

Passwords should be changed regularly. The system will inform users when the password is to be changed. Pupils and staff should never share passwords and staff must never let pupils use a staff logon. Staff must always 'lock' the PC if they are going to leave it unattended (the picture mute or picture freeze option on a projector will allow an image to remain on the screen and also allow a PC to be 'locked').

Virtual Learning Platform

An important aim of virtual learning platforms is to teach pupils how to interact safely and respectfully online. In order to learn how to do this, pupils will practise these skills and develop them in a safe environment. Our bespoke virtual learning platform has been set up to prevent cyber-bullying. This is achieved through:

- Restricting contact so that pupils can only message internal contacts (other Petersfield Pupils)
- The teachers can monitor messages sent between pupils
- We have set up a reporting system for pupils to notify teachers if a particular message has upset them

Blogging via the Virtual Learning Platform

At Petersfield we aim to give our pupils a voice and an audience through blogging. These are in the form of class blogs but can also be in the form of project blogs or individual pupil blogs. Our blogs will run via our Virtual Learning Platform and will:

→ Safely give our pupils a wider audience for their learning
→ Encourage reluctant learners to participate and succeed
→ Allow pupils to receive quality feedback safely from many different people
→ Allow pupils to peer assess each other's learning
→ Encourage parental engagement
→ Promote pupils' learning

E-Safety

Blogging involves pupils working on a dedicated part of the school's Virtual Learning Platform whilst in school and also at home. To be able to post, pupils need to log into the Virtual Learning Platform. The blogs will be sent to the class teacher for approval before appearing on the Virtual Learning Platform or school website.

Petersfield School seeks permission annually for photographs and videos.

In addition, the following is to be strictly adhered to:

- There is to be no identification of students using first name and surname; first name only is to be used
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use (i.e. creative commons).

Notice and take down policy – should it come to the schools attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed.

Incidents - Any e-safety incident is to be brought to the immediate attention of the E-Safety Lead and head teacher. They will take the appropriate action to deal with the incident and to fill out an incident log.

Blog Rules:

Using a blog safely is the most important thing about being a blogger. The following rules, if followed, will minimise any risks and will ensure that pupils will stay safe whilst blogging. The blog rules are explained clearly to each class during launch and are displayed in the classes. Teachers will remind **the children about e-safety and blogging rules when they are blogging.**

Don'ts:

1. Never give away any personal information about your location or identity.
2. Don't post pictures of yourself without specific permission from your teacher or parents.
3. Never give out your log in details to anyone.
4. Don't use text language in your posts

Dos:

1. If you see anything that shouldn't be on your screen, do tell your teacher or parents immediately.
2. Try to post about things that your audience would like to read.
3. Try to show off your best work/writing whilst blogging and use the tips people suggest to you to improve.
4. Always tag your posts with your first name and include key words specific to your post.
5. Post things that interest you.
6. If you receive a comment, it is polite to respond, say thank you and reply to a question if they have left one.
7. If your post doesn't appear straight away, you teacher might be busy, do be patient.
8. Comment on other people's posts too. Blogging is about commenting and posting!
9. Do visit other class blogs regularly to read and comment. This helps people come back to your blog.

The Role of the Blog Admin/Teacher:

The blog admin normally is the class teacher. This responsibility as gatekeeper is key to ensuring safety for the pupils using the blog. The following guidelines should be followed if a successful flowing blog is to be achieved:

1. Visit the blog regularly. It is better to visit short and often than catching up once a week. Your bloggers will appreciate comments and posts being approved quickly!
2. If you use a shared computer, log out at the end of each session.
3. Promote the links on the class blog to the parents and the wider community.
4. A blog can take a while to gather momentum and an audience. Be patient... the audience will come!
5. Mention the blog in assemblies and have it on display at parent evenings or school events, a blogging culture will soon be established!
6. Make sure each blog looks different in your school. This will help keep the interest high for the pupils from year to year.
7. Visit other blogs regularly and promote these to your class through links on your blog. What goes around comes around with blogging and strong loyal communities will form quickly.

Social Networking and Chat Facilities

- Social networking Internet sites (such as, MySpace, Facebook) provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact.
- Use of social networking sites and newsgroups in the school, is not allowed and will be blocked/filtered.
- Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Pupils will be encouraged to only interact with known friends, family and staff over the Internet and deny access to others.
- Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. The governors will consider taking legal advice, where appropriate, to protect pupils and staff against cyber bullying and defamatory comments.

Online Gaming

It is essential that children are aware of the potential issues regarding internet safety within the online gaming environment and are given the skills and knowledge to help manage and reduce these risks, with the help of those around them. At Petersfield, we follow the Childnet SMART Rules:

SMART rules

Safe: Keep safe by being careful not to give out personal information when playing online. This includes your e-mail address, phone number and password, as well as images and videos of yourself, friends and family

Meeting: Meeting someone you have only known online can be dangerous. Remember that no matter how long you have spoken to someone for, or how nice they are, if you have never met this person before then they are still a stranger. If anyone asks to meet up then tell an adult immediately.

Accepting: Accepting gaming requests, direct messages or clicking on links from people you don't know can lead to problems – they may contain viruses, inappropriate content or nasty messages!

Reliable: People we speak to online might not always be who they say they are as it is very easy to give away false information online. Try to only speak to your friends and family.
Tell: Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.
For a useful introduction to online gaming for parents, please see our website or: https://www.childnet.com/ufiles/Online-gaming-an-introduction-for-parents-and-carers-2017.pdf

Reporting
All breaches of the e-safety policy need to be recorded on and E-Safety Incident Form and handed to the E-Safety Lead. The details of the user, date and incident should be reported.

Incidents which may lead to child protection issues need to be passed on to one of the Designated Teachers immediately – it is their responsibility to decide on appropriate action not the class teachers.

Incidents which are not an immediate child protection issues but may require Senior Leadership intervention (e.g. cyberbullying) should be reported to the Headteacher the same day.

Allegations involving staff should be reported to the Head teachers. If the allegation is one of abuse then it should be handled according to the DFE document titled 'Dealing with allegations of abuse against teachers and other staff'. If necessary the local authority's LADO should be informed.

Evidence of incidents must be preserved and retained.

The curriculum will cover how pupils should report incidents (e.g. CEOP button, trusted adult, Childline)

Mobile Phones and Devices
Many new mobile phones have access to the Internet and picture and video messaging. Whilst these are the more advanced features, they present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying, or inappropriate contact.

- Pupils should not have mobile phones or smart watches in school. Further information is detailed in the Mobile Phone Policy.
- Staff should always use the school phone to contact parents.
- Staff including students and visitors should not access or use their mobile phones within the classroom whilst pupils are present. All staff, visitors and volunteers should ensure that their phones do not ring and are not used and stored safely away during the teaching day.
- Parents cannot use mobile phones on school trips to take pictures of the children.
- On trips staff mobiles are used for emergency only

Digital/Video Cameras/Photographs
Pictures, videos and sound are not directly connected to the Internet but images are easily transferred.

- Pupils will not use digital cameras or video equipment at school unless specifically authorised by staff.
- Publishing of images, video and sound will follow the policy set out in this document under 'Publishing Content'.

- Parents and carers are permitted to take photos/videos of their own children in school events. They are required to sign to say they, and anyone who attends with them, will not to share photos/videos from school events on social networking sites.
- One of the Head teachers or a nominee will inform parent(s)/guardian(s) and others present at school events that photographs/videos may be taken on the basis that they are for private retention and not for publication in any manner.
- Staff should always use a school camera to capture images and should not use their personal devices.
- Photos taken by the school are subject to the Data Protection Act.

Published Content and the School Website

The school website is a valuable source of information for parents and potential parents.

- Contact details on the Website will be the school address, e-mail and telephone number.
- Staff and pupils' personal information will not be published.
- One of the Head teachers or a nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Photographs and videos that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used in association with photographs.
- Consent from parents will be obtained annually before photographs of pupils are published on the school website.
- Named work will only be published with the permission of the pupil.
- Parents should not upload any images from within school onto social networking sites.
- The Governing body may ban the use of photographic equipment by any parent who does not follow the school policy.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority.
- E-safety will be discussed with our ICT support and those arrangements incorporated in to our agreement with them.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and Freedom of Information Act.

Assessing Risk

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school does not accept liability for the material accessed, or any consequences of Internet access. The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

Handling E-Safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to one of the Headteachers.
- Complaints of a child protection nature shall be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.

- Discussions will be held with the community police officer to establish procedures for handling potentially illegal issues.

Communication of Policy

Pupils:

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.
- Pupils will be informed of the importance of being safe on social networking sites such as msn. This will be strongly reinforced across all year groups during ICT lessons and all year groups look at different areas of safety through the digital literacy lessons.

Staff:

- All staff will be given the School e-safety Policy and its importance explained.

Parents:

- Parents' attention will be drawn to the School e-safety Policy in newsletters and on the school Website.
- Parents, staff and Governors sign to agree to the ICT policy annually.

Further Resources

We have found these web sites useful for e-safety advice and information.

http://www.thinkuknow.co.uk/	Set up by the Police with lots of information for parents and staff including a place to report abuse.
http://www.childnet-int.org/	Non-profit organisation working with others to "help make the Internet a great and safe place for children".

Appendix 1 – Acceptable Use for Data Processors (adult)

A: Use of school based equipment and services

Access to school equipment, the school network and the internet

- I will access the internet and other ICT systems using an individual username and password, which I will keep secure. I will ensure that I log out after each session and never allow other users to access the internet through my username and password. I will report any breach of security to the E-safety coordinator/Headteacher.
- I will not search for, download, upload or forward any content that is illegal or that could be considered an offence by another user. If I encounter any such material I will report it immediately to the e-safety coordinator/ Headteacher. I will not download or install any software from the internet or from any other media which may compromise the school network or information situated on it.
- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the e-safety coordinator.
- I will seek written consent from the E-safety coordinator/ headteacher prior to the use of any new technologies (hardware, software, cloud-based services) within school.
- I understand that my files, communications and internet activity may be monitored.

Creation, storage and security of digital content

- I will take reasonable precautions to ensure that any devices (laptops, tablets, cameras, removable media or phones) are stored in a secure manner when taken off site (car / home/ other location). Devices will not be stored in a car unattended or left in sight when not in use, e.g. by an open window. I will ensure that any personal or sensitive information taken off site will be situated on a school-owned device with appropriate technical controls such as encryption / password protection. If using my own device at home to view data, I will ensure that it is encrypted / password protected.
- I will use only school-provided portable storage (USB sticks, SD cards, portable hard drives etc) with encryption unless permission has been granted by the E-safety coordinator / Headteacher.
- I will demonstrate professional, safe and responsible behaviour when creating, using and storing digital images, video and sound within school. I will model safe and responsible behaviour in the creation and publishing of online content.
- I will use only school equipment to create digital images, video and sound unless prior permission is granted by the E-safety coordinator / Headteacher.
- I will ensure that I am familiar with the current permission status of pupils (see Parental Consent Form for Digital Images and Video). A summary of all permissions are circulated to all staff and available from the office. If additional permission is needed, e.g. for a surname in the press or for a medical form on SIMS, then I will discuss this with the E-safety coordinator and further written permission will be sought.
- I will ensure that I am familiar with the current Data Protection Policy. I will manage my digital files in accordance with this and I will make myself familiar with procedures in case of a breach of data security.
- I will not leave my computer unattended whilst working on screen; instead I will press CTL/ALT/DLT to lock the screen.
- I will only store / retain data files in line with the Data Retention Policy and will be responsible for deleting files which are no longer required.

School email and calendars

- I will use my school email address for all school-related correspondence. I understand that any use of the school email system will be monitored and checked. I will not use my private email account for any school-related business. Email is the main method

of communication for all school matters and I will check my e-mail regularly and respond in a timely manner (in normal working hours) to communications that require my attention.

- I will take care in opening any attachments sent by email. I will only open emails and associated attachments from trusted senders.
- Communication between staff or members of the wider school community should be professional and related to school matters only. Emails sent to external organisations will be written carefully and if necessary authorised before sending to protect members of staff. All communications to parents and carers should be sent to the office email account for onward transmission. It is best practice when emailing parents and/or carers to add all intended recipients to the BCC address field. This ensures that parents' personal email addresses are not visible to others.
- To avoid the misrepresentation of others I will not make changes to someone else's e-mail and then pass it on without making it clear where changes have been made.
- I will take great care when forwarding messages to ensure that no confidential or sensitive material (e.g. other's email addresses) are attached
- The school calendar on Central Hosting is the central calendar for all school matters. I will check it regularly and take events into account when planning lessons and visits etc. I will add events and appointments to the diary dates as necessary. I will also regularly check the school website calendar.

Learning and teaching

- In line with every child's legal entitlement I will ensure I teach / model an age-appropriate e-safety curriculum.
- I will support and promote the school e-safety policy at all times. I will model safe and responsible behaviour to pupils when using ICT to support learning and teaching.
- I will ensure that I am aware of my individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.
- I understand the importance of respecting and acknowledging copyright of materials found on the internet and will model best practice in the creation of my own resources at all times.
- I will ensure that all online services and software that I use as part of my teaching are appropriate and are used in line with current guidance.
- I agree to adhere by the school's Prevent guidelines and action plan.

B: Personal equipment and services

Social media and messaging

- I will not talk about my professional role in any capacity when using personal social media. I will not use social media tools to communicate with current or former pupils under the age of 18 nor to communicate with parents in a professional capacity. I will be mindful of potential conflicts of interest where a parent or carer of a child at the school is also a personal friend. I will set and maintain my profile on social networking sites to maximum privacy. I will not access social networking sites for personal use during school hours.
- If I experience any derogatory, negative or slanderous comments relating to the school, colleagues or my professional status, I will take screenshots for evidence and bring this to the attention of the e-safety coordinator or Headteacher.
- Use of school equipment or e-mail accounts for personal financial gain, gambling, political purposes or advertising is forbidden. However, nothing in this paragraph is intended to restrict members of staff conducting any trade union or professional association using school computers or e-mail accounts, outside of teaching hours.

Personal mobile phones and other devices

- I will not bring my mobile into teaching spaces unless with the overt permission of the Headteacher. If permitted, I will ensure that my mobile phone and any other

personally-owned device is switched off or switched to silent mode and out of sight during teaching hours and used only in emergencies.

- I will not contact any parents or pupils on my personally-owned device unless in an emergency. If a pupil or parent contacts me using my personal device I will inform the Headteacher as soon as possible. On educational visits my personal mobile phone may be used to contact the school.
- I will not use any personally-owned mobile device to take images, video or sound recordings in school without the overt, written permission of the Headteacher.
- I will seek permission from the E-safety coordinator / Headteacher if I need to synchronise any school email account with a personally-owned device. If permission is granted then I will ensure that the device has the appropriate technical controls such as encryption / password protection.

Data Processors found to be in breach of these rules may face disciplinary action in line with the school's disciplinary procedures.

Full name (Please print):_____

Signed:_____

Date:_____

Appendix 2 - EYFS / KS1 Acceptable Use

Think before you click

S

I will only use the Internet, icons, links and email with an adult's permission.

A

I will only not share any of my details online.

F

I will only send friendly and polite messages.

E

If I see something I don't like on a screen, I will always tell an adult.

Child's name: _____ Child's signature: _____

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety. I will support the school's approach to e-Safety and will not upload or add any pictures, video or text onto any social media that could upset, offend, identify or threaten the safety of any member of the school community. I have read and agree to the E-safety and Data Protection policies.

Parent's signature: _____ Date: _____

Appendix 3 – KS2 Acceptable Use

Petersfield Church of England Aided Primary School
Pupil KS2 Rules for Responsible Internet Use

These rules will keep me safe and help me to be fair to others:

- I will ask permission to go online.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will only e-mail people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.
- If I need to bring a phone to school, I will pass it to the office for safe keeping.
- If I use material that is the work of others in my work, I will state where I found the information.
- I will use a range of passwords, keep all passwords safe and never share accounts.

I have read and understand these rules and agree to them.

Child's name: _____ Child's signature: _____

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety. I will support the school's approach to e-Safety and will not upload or add any pictures, video or text onto any social media that could upset, offend, identify or threaten the safety of any member of the school community. I have read and agree to the E-safety and Data Protection policies.

Parent's signature: _____ Date: _____

The school accepts no responsibility for inappropriate use of the Internet outside school, even when children are researching a school-based subject.