Cliddesden Primary School

e-Safety Policy

(including Staff Acceptable use of ICT)

Version March 2019

This policy will be reviewed every 2 years

Ratified by the Governing Body March 2019

Stephen Mourant Chair of Governors …… Date: ……

Headteacher: …… …… Date: ……

Kenneth Davies

The Computing Curriculum

Introduction

A computing education also ensures that pupils become digitally literate – able to use, and express themselves through, information and communication technology – at a level suitable for the future workplace and as active participants in a digital world.

Aims

The National Curriculum for computing aims to ensure that all pupils:

- are responsible, competent, confident and creative users of information and communication technology.

Key Stage 1

Pupils should be taught to:

- communicate safely and respectfully online, keeping personal information private and recognise common uses of information technology beyond school.

Key Stage 2

Pupils should be taught to:

- describe how internet search engines find and store data; use search engines effectively; be discerning in evaluating digital content; respect individuals and intellectual property; use technology responsibly, securely and safely.

It is clear that digital technology provides amazing educational opportunities but is not without its risks. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually. We also know that ICT can offer new weapons for bullies, who may torment their victims via websites or text messages. On top of all this is the ever-present risk that children and young people may be exposed to inappropriate content when online and the potential results of this are yet to be fully understood.

At Cliddesden Primary School, we recognise it is our duty to ensure that every child in our care is safe and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings. However, we also believe that our duty of care extends beyond the physical boundaries of the school and so aim to equip our students with the understanding and skills they need to negotiate the digital world safely at all times.

This Policy document is drawn up to protect all parties – the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks, develop awareness and resilience in our pupils and how to deal with any infringements effectively.

Key Messages

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- E-mail
- Instant messaging often using simple web cams
- Blogs
- Podcasts
- Social networking sites
- Video broadcasting sites
- Chat Rooms
- Gaming Sites
- Music download sites
- Mobile phones with camera and video functionality
- Games consoles, including those with internet functionality
- Smart phones with full internet capability
- Tablets
- Internet enabled televisions

It is essential that all teachers are aware of the technologies that children are using both inside and outside school. This awareness can be achieved through the following:

- regular discussions about use of technologies

- being clear that there is a 'no blame' cultures for anyone who has had a bad experience
- zero-tolerance of any form of bullying
- reinforcement of key messages:
    - Zip it, block it, flag it.
    - Keep adults informed of what you are doing online.

Whole school approach

Creating a safe ICT learning environment includes four main elements at this school:

- Technological tools that are well-managed with regular security updates
- Policies and procedures, with clear roles and responsibilities
- An effective E-Safety education programme for pupils, staff and parents
- A 'no blame' culture in which issues can be openly discussed

Roles and Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Headteacher, with the support of Governors, aims to embed safe practices into the culture of the school. The Headteacher ensures that the Policy is implemented and compliance with the Policy is monitored. The Headteacher (Kenneth Davies) has overall responsibility for e-Safety with support from the Designated Safeguarding Lead (Jane Smith) and IT and computing curriculum coordinator (Laura Robinson).

The DSL and IT Coordinator ensure that they keep up to date with E-Safety issues and guidance. They ensure the Headteacher and Governors are updated as necessary.

Governors need to have an overview understanding of e-Safety issues and strategies at this school. Governors are responsible for the approval of the e-safety Policy and for reviewing its effectiveness. We ensure our governors are aware of our local and national guidance on e-Safety and are updated on policy developments.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

All staff should be familiar with the schools' Policy including:

- safe use of e-mail
- safe use of Internet including use of internet-based communication services, such as instant messaging and social network
- safe use of school network, equipment and data
- safe use of digital images and digital technologies, such as mobile phones and digital cameras
- publication of pupil information/photographs and use of website; particularly in respect of new GDPR regulations.
- eBullying / Cyberbullying procedures
- their role in providing e-Safety education for pupils
- ensuring a no blame culture is embedded within every class

Staff are reminded / updated about all e-Safety matters at least once a year.

The school includes e- safety in the curriculum and ensures that every pupil has been educated about safe and responsible use. Pupils need to know how to contrail and minimise online risks and how to report a problem. The school holds an annual e-safety week.

School ensures that they make efforts to engage with parents over e-safety matters and that parents/guardians/carers have signed and returned a Responsible Internet Use Form.

Communications

Many pupils are very familiar with the culture of new technologies and may have encountered e-safety issues themselves. However, pupils' perceptions of the risks involved may not be mature or the concepts may appear abstract at first. For this reason, e-safety rules should be introduced in the context of real life experiences. The school has developed a sequence of lessons that are delivered throughout the year that begin with children's experiences and utilise some of the excellent resources that exist, including:

- Think U Know (www.thinkuknow.co.uk)
- https://learning.nspcc.org.uk/research-resources/schools/e-safety-for-schools/
- Net Smart Kidz (www.netsmartzkids.org)

It is important that all staff feel confident to use new technologies in teaching. Staff are given regular opportunities to discuss the issues and develop appropriate teaching strategies.

With the current speed of on-line change, some parents and carers have only a limited understanding of online risks and issues. Parents may underestimate how often their children come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. Some of the risks could be:

- unwanted contact
- grooming
- online bullying including sexting
- digital footprint

The school will therefore seek to provide information and awareness to both pupils and their parents through:

- Acceptable use agreements for children, teachers, parents/carers and governors
- Curriculum activities involving raising awareness around staying safe online
- Information included in letters, newsletters, web site,
- Parents evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Building awareness around information that is held on relevant web sites and or publications

Social media

https://www.thinkuknow.co.uk/Teachers/Resources/

http://www.saferinternet.org.uk/search-results?keywords=social%20networking

http://www.childnet.com/search-results/?keywords=social%20networking

https://learning.nspcc.org.uk/research-resources/schools/e-safety-for-schools/

Cyberbullying

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

http://www.hampshire.police.uk/internet/asset/f0db2eea-0e3c-4fb4-b98c-e3fa681b860P/primary-social-networking-cyber-bullying

Central to the School's anti-bullying policy should be the principle that '*bullying is always unacceptable'* and that '*all pupils have a right not to be bullied*.

The school should also recognise that it must take note of bullying perpetrated outside school which spills over into the school and so we will respond to any cyber-bullying we become aware of carried out by pupils when they are away from the site.

Cyber-bullying is defined as "an aggressive, intentional act carried out by a group or individual using electronic forms of contact repeatedly over time against a victim who cannot easily defend himself/herself."

By cyber-bullying, we mean bullying by electronic media:

- Bullying by texts or messages or calls on mobile phones
- Use of or exclusion from group chats e.g Whats App
- The use of mobile phone cameras to cause distress, fear or humiliation
- Posting threatening, abusive, defamatory or humiliating material on websites, to include blogs, personal websites, social networking sites, apps
- Using e-mail, chat groups, Instagram, Apps etc, to message others
- Hijacking/cloning e-mail accounts
- Making threatening, abusive, defamatory or humiliating remarks in on-line forums

Cyber-bullying may be at a level where it is criminal in character.

It is unlawful to disseminate defamatory information in any media including internet sites.

Section 127 of the Communications Act 2003 makes it an offence to send, by public means of a public electronic communications network, a message or other matter that is grossly offensive or one of an indecent, obscene or menacing character.

The Protection from Harassment Act 1997 makes it an offence to knowingly pursue any course of conduct amounting to harassment.

If we become aware of any incidents of cyberbullying, we will need to consider each case individually as to any criminal act that may have been committed. The school will pass on information to the police if it feels that it is appropriate or are required to do so.

Sexting

https://www.thinkuknow.co.uk/Teachers/Resources/

http://www.hampshire.police.uk/internet/advice-and-information/safe4me/Safe4me+%27Sexting%27

https://www.ceop.police.uk/Media-Centre/Press-releases/2009/What-does-sexting-mean/

'Sexting' often refers to the sharing of naked or 'nude' pictures or video through mobile phones and the internet. It also includes underwear shots, sexual poses and explicit text messaging.

While sexting often takes place in a consensual relationship between two young people, the use of Sexted images in revenge following a relationship breakdown is becoming more commonplace. Sexting can also be used as a form of sexual exploitation and take place between strangers.

As the average age of first smartphone or camera enabled tablet is 6 years old, sexting is an issue that requires awareness raising across all ages.

The school will use age appropriate educational material to raise awareness, to promote safety and deal with pressure. Parents should be aware that they can come to the school for advice.

Gaming

http://www.saferinternet.org.uk/search-results?keywords=gaming

http://www.childnet.com/search-results/?keywords=gaming

http://www.kidsmart.org.uk/games/

Online gaming is an activity that the majority of children and many adults get involved in. The school will raise awareness:

- By talking to parents and carers about the games their children play and help them identify whether they are appropriate.
- By support parents in identifying the most effective way of safeguarding their children by using parental controls and child safety mode.
- By talking to parents about setting boundaries and time limits when games are played.
- By highlighting relevant resources.

Online reputation

http://www.childnet.com/resources/online-reputation-checklist

http://www.saferinternet.org.uk/search-results?keywords=online%20reputation

http://www.kidsmart.org.uk/digitalfootprints/

Online reputation is the opinion others get of a person when they encounter them online. It is formed by posts, photos that have been uploaded and comments made by others on people's profiles. It is important that children, staff and governors are aware that anything that is posted could influence their future professional reputation. The majority of organizations and work establishments now check digital footprint before considering applications for positions or places on courses.

Grooming

http://www.saferinternet.org.uk/search-results?keywords=grooming

http://www.childnet.com/search-results/?keywords=grooming

http://www.internetmatters.org/issues/online-grooming/

Online grooming is the process by which one person with an inappropriate sexual interest in children will approach a child online, with the intention of developing a

relationship with that child, to be able to meet them in person and intentionally cause harm.

The school will build awareness amongst children and parents about ensuring that the child:

- Only has friends online that they know in real life
- Is aware that if they communicate with somebody that they have met online, that relationship should stay online

That parents should:

- Recognise the signs of grooming
- Have regular conversations with their children about online activity and how to stay safe online

The school will raise awareness by:

- Identifying with both parents and children how they can be safeguarded against grooming

Staff

Staff must understand that the rules for information systems misuse. If a member of staff is concerned about any aspect of their ICT use in school, they should discuss this with their line manager to avoid any possible misunderstanding.

ICT use is widespread and all staff including administration, caretaker, governors and helpers will be included in appropriate awareness raising and training. Induction of new staff will include a discussion of the school's e-Safety Policy.

- Staff should be aware that Internet traffic is monitored and can be traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.
- Staff training in safe and responsible Internet use and on the school e-Safety Policy will be provided every 2 years.

Do's and Don'ts: Advice for Staff

Whilst the wide range of ICT systems and resources available to staff, both in school and outside of school, have irrefutable advantages, there are also potential risks that staff must be aware of. Ultimately if staff use ICT resources inappropriately, this may become a matter for a police or social care investigation and/or a disciplinary issue which could lead to their dismissal. Staff should also be aware that this extends to inappropriate use of ICT outside of school.

This Dos and Don'ts list has been written as a guidance document. Whilst it is not fully comprehensive of every circumstance that may arise, it indicates the types of behaviours and actions that staff should not display or undertake as well as those that they should in order to protect themselves from risk.

General issues

Do

- ensure that you do not breach any restrictions that there may be on your use of school resources, systems or resources
- ensure that where a password is required for access to a system, that it is not inappropriately disclosed
- respect copyright and intellectual property rights
- ensure that you have approval for any personal use of the school's ICT resources and facilities
- be aware that the school's systems will be monitored and recorded to ensure policy compliance
- ensure you comply with the requirements of the Data Protection Act when using personal data
- seek approval before taking personal data off of the school site
- ensure personal data is stored safely and securely whether kept on site, taken off site or accessed remotely
- report any suspected misuse or concerns that you have regarding the school's systems, resources and equipment to the Headteacher or designated manager and/or Designated Safeguarding Lead as appropriate
- be aware that a breach of your school's Acceptable Use Policy will be a disciplinary matter and in some cases, may lead to dismissal

- ensure that any equipment provided for use at home is not accessed by anyone not approved to use it
- ensure that you have received adequate training in ICT
- ensure that your use of ICT bears due regard to your personal health and safety and that of others

Don't

- access or use any systems, resources or equipment without being sure that you have permission to do so
- access or use any systems or resources or equipment for any purpose that you don't have permission to use the system, resources or equipment for
- compromise any confidentiality requirements in relation to material and resources accessed through ICT systems
- use systems, resources or equipment for personal use without having approval to do so
- use other people's log on and password details to access school systems and resources
- download, upload or install any hardware or software without approval
- use unsecure removable storage devices to store personal data
- use school systems for personal financial gain, gambling, political activity or advertising
- communicate with parents and pupils outside normal working hours unless absolutely necessary.

Use of email, the internet, VLEs and school and HCC intranets

Do

- alert your Headteacher or designated manager if you receive inappropriate content via email
- be aware that the school's email system will be monitored and recorded to ensure policy compliance
- ensure that your email communications are compatible with your professional role
- give full consideration as to whether it is appropriate to communicate with pupils or parents via email, or whether another communication mechanism (which may be more secure and where messages are less open to misinterpretation) is more appropriate
- be aware that the school may intercept emails where it believes that there is inappropriate use
- seek support to block spam
- alert your Headteacher or designated manager if you accidentally access a website with inappropriate content
- be aware that a website log is recorded by the school and will be monitored to ensure policy compliance
- answer email messages from pupils and parents within your directed time
- mark personal emails by typing 'Personal/Private' within the subject header line

Don't

- send via email or download from email, any inappropriate content
- send messages that could be misinterpreted or misunderstood
- use personal email addresses to communicate with pupils or parents
- send messages in the heat of the moment
- send messages that may be construed as defamatory, discriminatory, derogatory, offensive or rude
- use email systems to communicate with parents or pupils unless approved to do so
- download attachments from emails without being sure of the security and content of the attachment
- forward email messages without the sender's consent unless the matter relates to a safeguarding concern or other serious matter which must be brought to a senior manager's attention
- access or download inappropriate content (material which is illegal, obscene, libellous, offensive or threatening) from the internet or upload such content to the school or HCC intranet

- upload any material onto the school website that doesn't meet style requirements and without approval

Use of telephones, mobile telephones and instant messaging

Do

- ensure that your communications are compatible with your professional role
- ensure that you comply with your school's policy on use of personal mobile telephones
- ensure that you reimburse your school for personal telephone calls as required
- use school mobile telephones when on educational visits

Don't

- send messages that could be misinterpreted or misunderstood
- excessively use the school's telephone system for personal calls
- use personal or school mobile telephones when driving
- use the camera function on personal or school mobile telephones to take images of colleagues, pupils or of the school

Use of cameras and recording equipment

Do

- ensure that material recorded is for educational purposes only
- ensure that where recording equipment is to be used, approval has been given to do so
- ensure that material recorded is stored appropriately and destroyed in accordance with the school's policy
- ensure that parental consent has been given before you take pictures of school pupils

Don't

- bring personal recording equipment into school without the prior approval of the Headteacher
- inappropriately access, view, share or use material recorded other than for the purposes for which it has been recorded

- put material onto the VLE, school intranet or intranet without prior agreement from a member of senior staff

Use of social networking sites

Do

- ensure that you understand how any site you use operates and therefore the risks associated with using the site
- familiarise yourself with the processes for reporting misuse of the site
- consider carefully who you accept as friends on a social networking site
- report to your Headteacher any incidents where a pupil has sought to become your friend through a social networking site
- take care when publishing information about yourself and images of yourself on line – assume that anything you release will end up in the public domain
- ask yourself about whether you would feel comfortable about a current or prospective employer, colleague, pupil or parent viewing the content of your page
- follow school procedures for contacting parents and/or pupils
- only contact pupils and/or parents via school based computer systems
- through your teaching, alert pupils to the risk of potential misuse of social networking sites (where employed in a teaching role)

Don't

- spend excessive time utilising social networking sites while at work
- accept friendship requests from pupils – you may be giving them access to personal information, and allowing them to contact you inappropriately
- put information or images on line or share them with colleagues, pupils, or parents (either on or off site) when the nature of the material may be controversial
- post anything that may be interpreted as slanderous towards colleagues, pupils or parents
- use social networking sites to contact parents and/or pupils

Staff are required to sign the Code of Conduct for ICT (Appendix 1)

How will parents' support be enlisted?

Internet use in pupils' homes is increasing rapidly and unless parents are aware of the dangers, pupils may have unrestricted access to the Internet.

Cliddesden Primary School strives to help parents plan appropriate supervised use of the Internet at home. This is done through:

- Suggested online activities through the Headteacher's Newsletter and Creative Curriculum booklets.
- A section of useful web links for parents on the school website.
- Provision of mymaths website for pupils to use at home.
- Informing parents immediately of any concerns regarding any individual's use of technology.
- E-safety training for parents during the school's annual e-safety week.

How will complaints regarding e-safety be handled?

The school and local authority will take all reasonable precautions to ensure that risks are kept to a minimum through strict systems of filtering content and monitoring activity. However, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access. Any inappropriate material is reported to the local authority for them to block.

Staff and pupils are aware of infringements and the possible sanctions attached. Sanctions available include:

- informing parents or carers;
- removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system];
- referral to LA / Police.

Our Designated Safeguarding Leads, **Kenneth Davies (Headteacher)** and **Jane Smith** act as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

Staff Code of Conduct for ICT **Appendix 1**

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with parents, pupils and others, they are asked to sign this code of conduct. Staff should consult the detail of the school's Policy for Staff Acceptable Use of ICT for further information and clarification.

- I appreciate that ICT includes a wide range of system, including mobile phones, personal digital assistants, cameras, email, internet and HCC intranet access and use of social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that it may be a criminal offence to use the school ICT system for a purpose not permitted.
- I understand that I must not communicate information which is confidential to the school or which I do not have the authority to share.
- I understand that school information systems and hardware may not be used for personal or private without the permission of the Headteacher.
- I understand that my use of school information systems, internet and email may be monitored and recorded, subject to the safeguards outlined in the policy to ensure policy compliance.
- I understand the level of authority required to communicate with parents and pupils using the various methods of communication.
- I understand that I must not use the school ICT system to access inappropriate content.
- I understand that accessing, viewing, communicating and downloading material which is pornographic, offensive, defamatory, derogatory, harassing or bullying is inappropriate use of ICT.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager. I will not use anyone's account except my own.
- I will not install any software or hardware without permission.
- I will follow the school's policy in respect of downloading and uploading of information and material.
- I will ensure that personal data is stored securely and is used appropriately whether in school, taken off the school premises or accessed remotely. I will not routinely keep personal data on removable storage devices. Where personal data is required, it will be password protected/encrypted and removed after use.
- I will respect copyright, intellectual property and data protection rights.

- I understand use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.
- I will report any incidences of concern regarding children's safety to the Designated Safeguarding Lead or Headteacher.
- I will report any incidences of inappropriate use or abuse of ICT and inappropriate electronic communications, whether by pupils or colleagues, to the Headteacher, or if appropriate, the Chair of Governors.
- I will ensure that any electronic communication undertaken on behalf of the school, including email and instant messaging are compatible with my professional role and that messages do not present personal views or opinions and cannot be misunderstood or misinterpreted.
- I understand the school's stance on use of social networking and given my professional role working with children, will exercise care in any personal use of social networking sites.
- I will ensure that any electronic communications with pupils, where permitted, are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote e-safety with pupils in my care and help them to develop a responsible attitude to system use, communication and publishing.
- I understand that inappropriate use of personal and other non-school based ICT facilities can have implications for my employment at the school where this becomes known and where activities undertaken are inconsistent with expectations of staff working with children.

The school may exercise its right to monitor the use of the school's ICT systems and accesses, to intercept email and to delete inappropriate materials where it believes unauthorised use of the school's ICT systems may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, images or sound

I have read and understand the Policy for Staff Acceptable Use of ICT and understand that inappropriate use may be considered to be misconduct or gross misconduct and may, after proper investigation, lead to a disciplinary sanction or dismissal. I understand that if I need any clarification regarding my use of ICT facilities, I can seek such clarification from any member of the Senior Leadership Team.

SIGNED: ……

DATE:…….

NAME (PRINT): ……

Cliddesden Primary School – Use of Allocated School Laptops Appendix 2

Staff may be provided with laptops for the performance of their role. Where provided, staff must ensure that:

1. Their school laptop is not accessible by others when in use at home.

2. The laptop is not used inappropriately by themselves or others. (Please see Cliddesden School Staff Acceptable Use of IT Policy for further details).

3. They bring the laptop in as required for updating of software licences, virus protection and inventory purposes.

4. The laptop has appropriate controls set to prevent unauthorised access to confidential material.

Please sign below to agree to the above:

Date Laptop Received:	
Make & Model:	
Serial Number:	
Name (printed):	
Signature:	
Date:	

Responsible Internet Use **Appendix 3**

Dear Parents

As part of your child's curriculum and the development of ICT Skills, Cliddesden Primary School is providing **supervised** access to the Internet. We believe that the use of the World Wide Web and e-mail is worthwhile and is an essential skill for children as they grow up in the modern world. Please would you read the attached Rules for Responsible Internet Use and sign and return the consent form so that your child may use the Internet at school.

Although there have been concerns about pupils having access to undesirable materials, we are taking positive steps to deal with this risk in school. Our school Internet provider operates a filtering system that restricts access to inappropriate materials.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the school cannot be held responsible for the nature or content of materials accessed through the Internet. The School will not be liable for any damages arising from your child's use of the Internet facilities.

Also along similar lines, we need your written consent in order to publish children's work or to publish photographs on our school web site. As can be seen with the attached consent form and conditions of use, guidance has been sought from Hampshire County council.

The attached written consent forms will last for the duration of your child's schooling at Cliddesden Primary School unless you request otherwise.

This is an important and sensitive area and I do hope that you will support the school in its efforts to use ICT in the fullest sense and to promote our web site. Our web site address is: www.cliddesden.hants.sch.uk

Should you wish to discuss any aspect of Internet or web site use please do come and see us.

Yours sincerely
Kenneth Davies
Headteacher

Cliddesden Primary School

Responsible Internet Use

Pupil (name):

Pupil's Agreement

I have read and understand the school Rules for Responsible Internet Use. I will use the computer system and Internet in a responsible way and obey these rules at all times

Signed: .**Date:**

Parent's Consent for Internet Access

I have read and understood the school Rules of Responsible Internet Use and give permission for my child to access the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature of content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from the Internet facilities.

Signed: **Date:**

Please print name:

Rules for Responsible Internet Use

We use the school computers and Internet connection for learning. These rules will help us to be fair to others and keep everyone safe.

- I will ask permission before entering any Web site, unless my teacher has already approved that site.
- On a network, I will use only my own login.
- I will not look at or delete other people's files.
- I will not bring CDRom/Memory sticks/removable hard drive etc into school without permission.
- I will only e-mail people I know, or my teacher has approved.
- The messages I send will be polite and sensible.
- When sending e-mail, I will not give my home address or phone number, or arrange to meet someone.
- I will not use Internet chat.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- I know that the school may check my computer files and may monitor the Internet sites I visit.

I understand that if I deliberately break these rules, I could be stopped from using the Internet or computers. The school may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web-sites, the interception of e-mail and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be used for criminal purposes or for storing text or imagery which is authorised or unlawful.