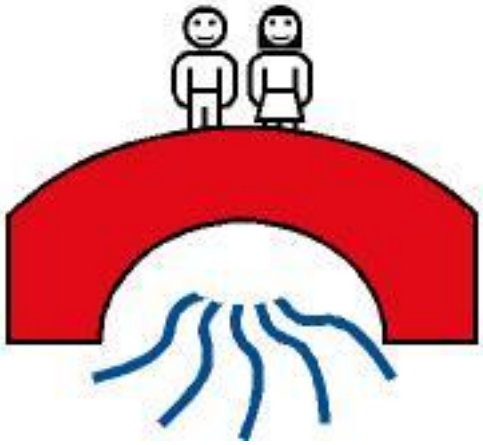
Loddon Primary School



E- Safety Policy

Author: Amy Routh

Committee responsible: Curriculum Committee

Date of last review: March 2017

Date of next review: March 2018

Authorised on 8 March 2017

_____	Sarah Phillips	Headteacher
_____	John Brady	Committee Chair

e-Safety

E-Safety encompasses all technologies including the Internet, mobile phones, ipads, digital cameras as well as collaboration tools and personal publishing. It highlights the need to educate staff and pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their technology experiences.

This e-Safety Policy is written to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole.

The school's e-Safety policy will operate in conjunction with other policies including those for Behaviour, Disciplinary, Anti- Bullying, Curriculum, Data Protection and ICT Security.

Our e-Safety Policy has been written by the school, following guidance from Wokingham Borough Council, Kent County Council and government guidance. It has been agreed by senior management and approved by the governors and PTA.

End to End e-Safety

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by **all staff and students**. This is implemented through in-house training and made explicit through published policies.
- Sound implementation of e-Safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the SEGfL including the effective management of Web filtering.
- National Education Network standards and specifications.

1. Roles and Responsibilities

Governors

Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. There should be a member of the governing body whose responsibility includes:

- Regular meetings with the e-Safety Co-ordinator
- Regular monitoring of e-safety incident logs
- Reporting to relevant Governors committees
- Keeping up to date with school e-Safety matters

This is reported through the Governor representative on the ICT strategy group

Headteacher and SLT

The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community. However, the day to day responsibility for e-safety may be delegated to the ICT Subject Leader or another appropriate member of staff, if necessary. The Head Teacher and SLT will ensure the following:

- Ensuring that such staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues when necessary.
- The Senior Leadership Team receive regular monitoring reports regarding e-safety.
- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The School Business Manager, under the direction of the Headteacher, ensures that the Information Commissioner's Office, ICO, registration is kept up to date on an annual basis.

E-Safety co-ordinator

The role of the e-safety co-coordinator falls to the ICT lead unless the e-safety issue becomes a child protection matter, in which case it falls to the Head teacher (Child Protection Officer).The e-safety co-ordinator takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents. The e-safety co-ordinator will also:

- Ensures that all staff, including parent helpers, are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- Provides materials, training and advice for staff about integrating e-safety within the curriculum and monitors that e-safety is being taught regularly.
- Liaises with the Local Authority
- Liaises with school ICT technical staff
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-Safety developments (kept in the safeguarding file)
- Meets regularly with Safeguarding Governor to discuss current issues, review incident logs and filtering/change control logs
- Attends relevant committee meetings of Governors
- Reports regularly to the Senior Leadership Team
- Reminds class teachers to display e-Safety rules in the classroom at all times and discuss with pupils at the start of each school year in order to form part of a signed class agreement.
- Ensures all staff, pupils and parents sign AUP annually

ICT Technician and ICT Subject Leader

In co-operation with the school's technical support provider they are responsible for ensuring that:

- The school's ICT infrastructure is secure and is not open to misuse or malicious attack
- The school meets the e-Safety technical requirements outlined in any relevant Local Authority Safety Policy and guidance
- Users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- The school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- They keep up to date with e-Safety technical information in order to effectively carry out their e-Safety role and to inform and update others as relevant
- The use of the network, learning platform and pupil email is regularly monitored in order that any misuse/attempted misuse can be reported to the e-safety co-ordinator for investigation and action
- Appropriate steps are taken to protect personal information , including the encryption of removable devices including laptops and external storage devices, and the provision of secure access to the school network from home using VPN technologies
- E-safety reminder cards are displayed on all computers
- E-Safety rules are displayed at all ICT access points

Staff

All staff are responsible for ensuring that:

- They are familiar with current e-safety matters and of the school e-safety policy and practices

- They have read, understood and signed the school Staff Acceptable Use Policy (AUP) annually
- They report any suspected misuse or problem to the ICT Subject Leader for investigation and action. The ICT Subject Leader will inform the e-safety co-ordinator if necessary.
- Digital communications with pupils (email/Virtual Learning Environment (VLE)/voice) should be on a professional level and only carried out using approved school systems
- E-safety issues are embedded in all aspects of the curriculum and other school activities.
- Pupils understand and follow the school e-safety and acceptable use policy
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations in relation to their age
- They monitor ICT activity in lessons, extra-curricular and extended school activities
- They are aware of e-safety issues related to the use of mobile phones, cameras, ipads and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- In lessons where internet use is pre-planned students/pupils should be guided to sites checked as suitable for their use and that they are aware of the procedure for dealing with any unsuitable material that is found in internet searches

Child Protection Officer (CPO)

The CPO should be trained in e-safety issues and be aware of child protection matters that may arise from:

- Sharing or loss of personal data
- Access to illegal/inappropriate materials
- Inappropriate on-line contact with adults/strangers
- Potential or actual incidents of grooming
- Cyber-bullying

Data Protection Officer

Responsibilities include:

- Maintaining registration with the Information Commissioner's Office
- Keeping abreast of regulatory requirements and recommendations as outlined on their website at www.ico.gov.uk
- Informing staff and the Senior Leadership Team of these recommendations so that school policies may be updated. See Appendix 1 – School and the Data Protection Act for further information and the School Data Protection policy

2. E-Safety within learning and teaching

Why new technology use is important

- The Internet and the use of other ICT resources are an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality access to new technology as part of their learning experience.
- New technology use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use to enhance learning

- The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- The school will work with Wokingham Borough Council, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Addressing E-safety

- Key e-safety messages are reinforced as part of a planned programme of assemblies (2 a year), Computing lessons (1 per half term), PSHE activities or other curriculum opportunities where appropriate
- Pupils are taught, in all appropriate lessons, to be critically aware of the materials/content they access online and be guided to validate the accuracy of information
- Pupils should be helped to understand the need for the AUP (Acceptable Use Policy) and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices **both within and outside school**
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of computers are displayed in all rooms and displayed next to fixed site computers
- Staff should act as good role models in their use of ICT, the internet and mobile devices
- Staff will be kept up to date through annual training in e-Safety

Staff Training

- Staff will be kept up to date through regular e-safety training
- Staff should always act as good role models in their use of ICT, the internet and mobile devices.
- Staff will be provided with suitable and relevant e-safety resources for teaching and learning to ensure progression and coverage of themes across the school.

Parental Support

The support of, and partnerships with, parents is encouraged. This will include the following:

- Awareness of the school's policies regarding e-safety and internet use.
- Practical demonstrations and training including advice and guidance on: filtering systems, educational and leisure activities and suggestions for safe internet use at home. This will be delivered through parent workshops delivered by the parent support worker, ICT co-ordinator and where possible external professionals. (2-3 per year)

3. Network Security

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented by those responsible.

The ICT subject leader and ICT technician review Loddon Primary School's ICT systems capacity and security regularly. Virus protection through Sophus is updated daily and additional technical support is provided by independent ICT companies (currently Capita and Waterman Solutions). Security strategies are reviewed, discussed and updated on the advice of Wokingham Borough Council ICT advisors.

Passwords

- All staff have an individual password. Pupils may have a group password or older pupils may be given individual passwords for accessing the network.
- It may be necessary to have a username with limited access whose password is known to more than one member of staff.
- All users have an individual log on to the Learning Platform and Bug Club when using either a fixed or mobile piece of ICT.
- Users must log off computers or platforms when no longer in use
- Users leaving a computer temporarily should lock the screen.
- No individual should tell another their password

Security

- Servers, and communications cabinets should be securely located and physical access restricted.
- Wireless systems should be secured to at least WPA level (Wi-fi protected access)
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the ICT Technician.
- The "administrator" passwords for the school ICT system, used by the ICT Technician are also available to the ICT Subject Leader and School Business Manager and stored securely in school.
- School ICT staff may monitor and record the activity of users on the school ICT systems and users are made aware of this through the Acceptable Use Policy.
- The school keeps a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- Pupil access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Pupils will not access the Internet without an adult present.
- Parents are asked to sign and return a consent form, (Pupil AUP).

Filtering

- The school maintains and supports the managed filtering service provided by SEGfL.
- Changes to network filtering should be approved by the ICT Subject Leader and ICT technician.
- Any filtering issues are to be reported immediately to SEGfL.

4. School password protocol

- All passwords used by adults should follow the guidelines in this policy.
- No individual should log on using another individual's password, unless they are a member of staff logging on as a child.
- No individual should tell another individual their password.
- Once a computer has been used, users must remember to log off so that others cannot access their information. Users leaving a computer temporarily should lock the screen.

- Passwords must meet complexity requirements. A security setting determines whether passwords meet these requirements. These requirements are enforced when passwords are changed or created. The minimum requirements are that a password must:
    - Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
    - Be at least six characters in length
    - Contain characters from three of the following four categories:
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Base 10 digits (0 through 9)
    - Non-alphabetic characters (for example, !, $, #, %)
- Passwords must not be easily guessable by anyone.
- If a password is identified as insecure then it is essential that the password is changed immediately.

5. Loading software

- Only the ICT Subject Leader or those acting specifically on their behalf such as the ICT Technician are allowed to load software on to any school computer. The School Business Manager may load administration Software.
- For the purpose of this policy, software relates to all programs, images or screensavers, which can be downloaded or installed from other media.
- Images and video clips may be downloaded as long as the teacher in charge is satisfied that they are not breaching copyright.
- Software loaded on to any school system must be
    - Properly licensed.
    - Free from viruses.
    - Authorised by the ICT Subject Leader

6. Virus Protection and Transferring and downloading files

All computer systems, including staff laptops, are protected by the Sophus antivirus product which is administered centrally and automatically updated.
Great care, by all staff and pupils, should be taken when copying files from one computer to another as there is considerable risk of viruses infecting the school computers. This includes downloading files from the internet where only dependable sources should be used.

7. Security of Sensitive Data

Sensitive data is any data which links a child's name to a particular item of information. Examples include:

- SEN records such as IPPs and Annual Review records.
- Marksheets and assessments.
- Reports and Open Evening comments.
- Personal data stored on the School Information Management System, SIMS.
- Photographic or video material.
- Name, address and contact information

Non Sensitive data thus includes

- General teaching Plans.
- Curriculum materials.
- General correspondence of a non-personal nature.
- All users are responsible for only accessing, altering and deleting their own personal files. They must not access, alter or delete files of another user without permission.
- Data may be encrypted through full hard-drive encryption sing Truecrypt.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Sensitive data
    - Must be encrypted on laptops or memory sticks. All teachers have access to these.
    - Should not be emailed between staff.
    - Should not be put on a USB stick, CD or any other removable media unless it is encrypted.
    - Should be deleted from laptops at the end of an academic year.
    - Staff should take care not to leave printed documents with sensitive information open to view
    - Safe and secure procedures for disposal of any data or images from devices.

8. Email and messaging guidance

- Staff may use school computers in child free zones (e.g. Staff room) for personal use during break and lunch times, but must be vigilant when opening emails from personal accounts.
- Pupils and staff will be informed that the use of school e-mail or messaging accounts will be monitored
- Pupils should immediately tell a teacher if they receive an offensive e-mail or message or find an inappropriate web page.
- Pupils should not reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone via an e-mail or message.
- Emails sent by pupils to an external organisation should be authorised by a member of staff before sending.
- The forwarding of chain letters, jokes etc. is not allowed. Nor is the sending of defamatory or obscene material either internally or externally.
- Pupils may only use approved e-mail or message accounts on the school system.
- Information of a sensitive nature should not be sent by unencrypted email and on no account to personal staff email, any US based email service or drop box type cloud storage environment. They are not considered to be secure under UK data handling laws.

9. Confidential Information on Laptops

In addition to the information above the following security measures should be taken with staff laptops:

- Laptops must be out of view and preferably locked away overnight particularly when left at school
- Windows should be locked when a teacher user leaves their computer (Windows key + L)
- Staff and school laptops should never be left in a parked car, even in the boot.
- At home, the families of members of staff should not use a school laptop perhaps allowing access to confidential information. If others are to use the laptop, they should logon as a separate user without staff privileged access.

10. Confidential Information on Paper

Staff should take care not to leave printed documents with sensitive information open to view eg by not collecting them promptly from printers, or leaving such documents on open desks. Sensitive information should be held in lockable storage when office staff are not present.

11. Backing up of data

- The school has a secure on-site and remote backup regimes which will enable recovery of key systems and data within a reasonable timeframe should a data loss occur.
- Data held on individual curriculum systems is liable to be overwritten without notice during the process of ghosting the computers. It is essential that no data is stored on the C drive of any curriculum computer.
- Staff are responsible for backing up their own data on staff laptops if they decide not to use automatic synchronise option. They may copy files to the server for automatic backing up.
- Backup methods are regularly tested by renaming and then retrieving sample files from the backup.
- Loddon Primary School has a whole school ICT disaster recovery plan which would take effect when severe disturbance to the schools ICT infrastructure takes place, to enable key school systems to be quickly reinstated and prioritised, including who would be involved in this process and how it would be accomplished.

12. The School Learning Platform

- The school Learning Platform includes the school address, school email, telephone and fax number.
- Staff or pupils' home information should not be published.
- Photographs of children are only shown with parental approval (see appendix 3).
- Pupils' full names are not used on the learning platform in conjunction with photographs.
- The copyright of all material posted must be held by the school or be clearly attributed to the owner where permission to reproduce has been obtained or given eg danosongs.com.
- The headteacher takes overall editorial responsibility and ensure that content is accurate and appropriate.
- The learning platform provides information and guidance concerning e-safety.

13. World Wide Web

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.
- All pupils using the World Wide Web must be made aware of the school's e-Safety Guidelines. These are posted next to all computer access points and frequent reminders are given through lessons and assemblies.
- Instruction in responsible and safe use will precede Internet access on a regular basis (at least once each term).
- Pupils and staff will be informed that Internet access will be monitored.
- Filtering will be carried out by RM (Research Machines) as part of the managed service.

- The school audits ICT provision to establish if the e-Safety policy is adequate and that its implementation is effective through 'stop-check' questioning around the school.
- Staff are able to access some filtered websites (e.g. You Tube) to access content for learning via the staff proxy. This is username and password protected and cannot be accessed by the children. Staff must check content before downloading for use in lessons.

14. Course of action if inappropriate content is found

- If inappropriate web content is found (ie that is pornographic, violent, sexist, racist or horrific) the user should
    - Turn off the monitor or minimise the window immediately
    - Report the incident to the teacher or responsible adult.
- The teacher should
    - Ensure the well-being of the pupil.
    - Note the details of the incident, especially the web page address that was unsuitable (without re-showing the page to the pupils).
    - Report the details of the incident to the e-safety co-ordinator
- The e-Safety co-ordinator will then
    - Log the incident and take any appropriate action.
    - Where necessary report the incident to our Internet Service Provider (RM) so that action can be taken.

15. The use of new technologies

- Pupils and staff will not be allowed access to public or unregulated chat rooms in school.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Staff and volunteer personal mobile phones may not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

16. Staff use of Social Networking

- Staff have a perfect right to use social networking sites but not during the school day on the school computers.
- Staff should ensure that any public comments they make on social networking sites are compatible with their role as a member of staff and that they show the highest standards of professional integrity.
- Staff should not post photographs of children from the school on their social networking site.
- Staff should regularly check their profile settings on social networking sites to ensure that
    - No pupil (or recent past pupil (under 16)) is able to see extra material that is not public (eg not be a friend or a contact).
    - No parent of a child at school should be able to see extra material that is not public.
    - Any changes to social networking sites and privacy settings are clearly understood.

17. Child use of Social Networking sites

- Pupils at school are regularly educated in e-Safety which includes the safe use of social networking sites.

- Pupils are able to use the learning platform at school and at home, which has some aspects of social networking. One key feature of the learning platform is the ability to control, filter and check the flow of information through the system.
- Most social networking sites are blocked at school. However, to further the pupils' education in the use of such sites they may be unblocked for specific activities on specific occasions. This is undertaken with the knowledge of the ICT subject leader and ICT Technician (who unblocks and re-blocks the sites).
- Pupils use of social networking should conform to age restrictions.

18. Use of mobile devices

- Pupils are not allowed to bring mobile phones to school unless parents make prior arrangements with the school. Pupils' personal mobile phones must be stored in the school office throughout the school day.
- Pupils are not allowed to bring in game devices which allow ad hoc networks to be established.
- Teacher/parent contact should normally be by the main school telephone and not via a mobile device except where off-site activities dictate the use of a mobile phone.
- Staff, helper and visitor mobile devices should normally be switched off or on silent during the times that children are present.
- Staff and Parent helpers in school must ensure that they do not send personal messages, either audio or text, during contact time with pupils. If an exceptional emergency arises they should arrange temporary cover whilst they make a call.
- Staff and pupils may send educational messages during lesson times if these are part of the curriculum.
- The sending of abusive or inappropriate text messages is forbidden.
- Schools should be vigilant where mobile phones are used with children in the Foundation Stage.
- No device in any of the school buildings should contain any content that is inappropriate or illegal.

19. Photography of pupils

- Parents, staff and pupils are welcome to take photographs of pupils at school under the following conditions
    - Photographs should not be distributed beyond either the school or the immediate family and friends of the child's family.
    - Photographs should not be posted on an open internet site such as
        - On a social networking page with the permissions set to public.
        - On the school learning platform on an open page without parental approval
- No photographs of pupils should be taken
    - In the toilets or wash areas.
    - Whilst pupils are getting changed.
    - In the medical room.
- The school will ensure appropriate written permissions are obtained for the taking of digital images of pupils. Use could include website, learning platform and social media. It could also include display and publicity material.
- Where parental permission has not been obtained, or it is known that a pupil should not be photographed or filmed, every reasonable effort should be made to ensure the pupil's image is not recorded.

- The only exceptions to this rule would be if photographs are being taken to illustrate a particular point for display (eg how to wash hands). In this case the Team Leader must be informed before this activity is undertaken.
- Only school photographic devices (ie cameras, Flipcams, ipads) are to be used, not personal cameras or mobiles. These devices will be checked and monitored.
- Photographic images of pupils are monitored when stored on the school network and spot check audits of school laptops will be made from time to time too.
- All devices capable of taking photographs, whether belonging to the school or personal, may be subject to scrutiny by managers if required.
- All images will be securely stored in a central location. Images on a USB, memory card or CD should only be temporary. Images of pupils who have left school will be deleted unless kept as part of a school archive.

20. Acceptable Use Policy and Agreement

- All users of the school computers (ie staff and pupils) should sign the appropriate acceptable use policy or agreement on an annual basis.
- Parents will also be asked to sign the parent / carer acceptable use agreement on an annual basis.

21. Complaints Regarding Internet Use

- The school have procedures in place for dealing with any complaint of Internet misuse.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Complaints of Internet misuse will be dealt with by the headteacher.
- Any complaint about staff misuse will be referred to the headteacher.

22. Sanctions

- The school has a system of sanctions to promote the appropriate use of technology.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. This would constitute a disciplinary matter as far as staff are concerned.

23. Parental Support

- Parents are made aware of the school's policies regarding e-Safety and Internet use via newsletters and information evenings.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents is encouraged.
- Parents' attention are informed of the school e-Safety Policy in newsletters, the school prospectus and on the school learning platform.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet is available to parents via the e-safety link on our learning platform.

Appendices

Appendix 1 – School and the Data Protection Act

Appendix 2 - Staff Code of Conduct Acceptable Use Policy

Appendix 3 – Letter to Parents including Pupil Acceptable Use Agreement and parent photo approval

Appendix 4 – Loddon Primary School Rules Pupil Internet Use posters for display in classrooms and ICT Suite

Appendix 5 – Guidelines regarding staff use of social networking websites

Appendix 6 – Child e-safety Sanctions

Appendix 1: School and the Data Protection Act

The Seventh Principle of the Data Protection Act (1998) states that:

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

This means that:

Schools must have appropriate security to prevent the personal data you hold (eg for staff, pupils and parents) being accidentally or deliberately compromised.

In particular, you will need to:

- Design and organise your security to fit the nature of the personal data you hold and the harm that may result from a security breach.
- Be clear about who in your organisation is responsible for ensuring information security.
- Make sure you have the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff.

and

- Be ready to respond to any breach of security swiftly and effectively.

Failure to comply with the Act could result in loss of reputation or even legal proceedings. Further guidance may be found at www.ICO.gov.uk

Appendix 2 – Staff Code of Conduct Acceptable Use Policy

Loddon Primary School

The Responsibility of Staff in the use of ICT

This document is written to ensure that all staff are fully aware of their professional responsibilities when using information systems. It should be read in conjunction with the e-Safety policy.

- It is understood that the information systems are school property, primarily to be used for work related purposes. However, during break times and before/after school they can be used for personal use providing professional guidelines are followed. The head teacher and governors have discretionary rights to monitor these activities. The final definition of appropriate use lies with the head teacher.
- The use of information systems will always be compatible with the professional role.
- Staff need to ensure that their use of ICT does not leave them in a vulnerable position where accusations of criminal or unprofessional behaviour could be considered.
- The school may monitor the information systems and Internet use to ensure policy compliance.
- Personal data must be kept secure and used appropriately, whether in school, taken off the school premises or accessed remotely.
- The use of personal cameras and mobile phones to take photographs is not permitted under any circumstances.
- System security will be respected and passwords or security information will not be disclosed to anyone other than the appropriate system managers.
- Software or hardware can only be installed by the system managers on school ICT resources including teacher laptops.
- Any incidents of concern regarding children's safety must be reported to the school e-Safety Coordinator and Designated Child Protection Coordinator.
- Any electronic communications with pupils will be compatible with the professional role of staff.
- Personal use of social networking internet sites, such as Facebook and Twitter, must not include comments about work. This is an expectation of your professional role.
- Parents of the school should not be part of a staff friendship group on a social network site unless that friendship was established through a non-work related connection.
- Photos of staff should not be posted on a social networking site without their prior approval.
- E-Safety will be promoted with all children and help will be given to develop a responsible attitude to system use and to the content they access or create.
- Copyright and intellectual property rights will be respected.
- Handheld devices that are taken off site must be seen and signed in and out by a member of SLT.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

	Name (capitals)	Signature	Date
Staff Member			
Headteacher			

Appendix 3: Pupil / Parent ICT Acceptable Use Agreement

Sample letter to parents

LODDON PRIMARY SCHOOL

Headteacher: Mrs S Phillips, MA ED (Open)

Silverdale Road, Earley, Reading, Berkshire, RG6 7LR
Tel: (0118) 9261449 Fax: (0118) 9266351
Email: secretary@loddon.wokingham.sch.uk

Applicable Date added here

Dear Parents
Responsible Use of the Internet

As part of pupils' curriculum enhancement and the development of ICT skills, Loddon Primary School provides supervised access to the Internet.

Our Internet based learning platform is now fully accessible by all pupils and provides opportunities to exchange electronic mail within school and through collaborative projects with other schools in the wider community. Pupils can also use it to access appropriate, reputable websites as part of their programme of learning.

Although there have been concerns about pupils having access to undesirable materials, we have taken positive steps to deal with that possibility. We have purchased our Internet access from an educational supplier that operates a filtering system restricting access to inappropriate materials. All our computer screens are in public view and, as stated above, access is always supervised.

Recently, all pupils have learned about e-Safety (keeping safe when using the Internet). A copy of the Pupil Acceptable Use Agreement and SMART code is attached to reinforce good practice when accessing the Internet at home.

Our learning platform is set up with two methods of viewing content. The public view gives parents and pupils information about the school and the curriculum. The password protected areas can only be viewed by the pupils in their associated class and Loddon Primary School staff. We have attached a form asking your permission to store photographs and work within these password protected areas to develop good home-school links and extended learning opportunities. Please note that names will not be displayed with the photographs.

There are occasions where more than one class is involved in an activity and therefore we also request your permission to add work and unnamed photographs in the public viewing areas.

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 under any circumstances for any damages arising from your child's use of the Internet facilities.

Should you wish to discuss any aspect of Internet use please contact Miss Routh.

Yours Sincerely

Mrs Sarah Phillips

Pupil ICT Acceptable Use Agreement

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

- I will not tell anyone my password.
- If I think someone knows my password I will tell a teacher straight away.
- I will not look at or delete other people's files.
- I will only use the computers at school when a member of staff is present and has said I can (given permission).
- I will not use text talk on my web pages or in emails.
- I will not send nasty or teasing messages to people.
- I will not give out my home address or any phone number or arrange to meet anyone over the internet, even a friend.
- If I see anything I am unhappy with or I receive a message I do not like I will tell a responsible adult as soon as I can.
- I will follow the SMART code when using computers at school and home.

I know that the school can check my messages, emails and web pages and my computer files.
I understand that if I deliberately break these rules, I could be stopped from using the learning platform or computers at school.

I h**ave read and agree with the e-Safety Guidelines**

Child's Signature: …… Name ……..…… Date: ……..……

Accepted for school: …….. Name ……. …….

Parent/Carer ICT Acceptable Use Agreement

- I have read and discussed the Pupil Acceptable Use rules with my child
- I understand that the school will use appropriate filtering and ensure appropriate supervision when using the school Learning Platform and the Internet. I understand that despite the filtering it is possible that inappropriate materials may be accessed and accept that the school will endeavour to deal with any incident that may arise, according to policy.
- I understand that whilst my child is using the Internet and other on-line tools outside of school, that it is my responsibility to ensure safe and responsible use with the support of the school.
- I will report any misuse of the school Learning Platform to the school as soon as I can.
- I understand that parents may take photos of the pupils at school events, such as Sports Days and performances, but that such images should only be shared with immediate family. Photos of pupils at Loddon Primary School should not be displayed without restriction on a photo sharing website (eg Facebook, Flickr, Picasa web albums etc)

Parent's signature _____ Date _____

Parent's Consent for Web Publication of Work and/or photographs

1. I agree that, if selected, my son or daughter's work and photograph may be published on the school learning platform for public view **or the school's twitter or you tube accounts. I understand the work and photographs displayed would not be identifiable by name.**

Parent's signature _____ Date _____

Please note if you signed part 1 above you do not need to sign 2 -5 below

2. I agree that, if selected, my son or daughter's work may be published on password protected areas **of the school learning platform. .**

Parent's signature _____ Date _____

3. I agree that, if selected, my son or daughter's photograph may be published on password protected areas **of the learning platform. I understand that names will not be displayed.**

Parent's signature _____ Date _____

4. I agree that, if selected, my son or daughter's photograph may be published on the school's twitter or you tube account for public view**. I understand that names will not be displayed.**

Parent's signature _____ Date _____

5. I agree that, if selected, my son or daughter's work may be published on the school twitter or you tube account for public view**. I understand that names will not be displayed.**

Parent's signature _____ Date _____

2. Appendix 4 : SMART Code

Appendix 5 : Guidelines Regarding Staff Use Of Social Networking Websites

What is meant by 'social networking'?

Whilst the most common examples of social networking applications are Facebook, Twitter, MSN and YouTube they also include any online collaborative forum such as blogs and media sharing services and virtual worlds such as Second Life.

Use of social networking sites

- Staff may choose to use social networking sites as part of their private lives.
- Social networking sites should not be used or accessed during school working hours.
- Staff may not use school equipment to access social networking sites.

How should staff conduct themselves?

- It is assumed that staff will always conduct themselves with the highest standards of professional integrity and be aware that how they as individuals are perceived in the virtual world may reflect on how the school is perceived.
- Staff should give careful consideration when posting personal information as to how this might be viewed by pupils and parents even when the postings are within a 'private' online space.

Posting of images and/or video clips

- Photographic images and/or movie clips of children at the school or past pupils, up to the age of 18, should never be posted.
- Photographic images and/or movie clips of school staff should not be posted unless specific consent has been obtained.

Who should staff be networking with?

- Staff should recognise that their existing lists of friends/contacts/followers may include people who are part of both their private and professional lives.
- Staff should never be 'friends' with children at the school or past pupils up to the age of 18.
- Staff should not create new links with parents simply because they teach their children.

Privacy

- Profile settings should be regularly checked, and updated as necessary, to ensure that posted comments and images are not publicly accessible.
- Any changes to social networking sites and privacy settings should be clearly understood.

Appendix 6 – Pupil ICT misuse sanctions

PUPIL SANCTIONS

Using the Internet

Using a search engine without adult approval/supervision – verbal warning

Continued use of a search engine without adult approval **following verbal warning** – pupil removed from the PC for the remainder of the lesson to complete an e-safety written task.
An e-safety alert form must be completed by member of staff involved and given to e-safety co-ordinator

Inappropriate use of forums/messaging – depending on the message – learning platform account suspended for between one week and four weeks – to be decided by e-safety co-ordinator.
An e-safety alert form must be completed by member of staff involved and given to e-safety co-ordinator

Using other ICT resources

Inappropriate use of digital cameras/Flipcams/ipads – depending on level of concern –
Minimum concern - resources are removed from the pupil and for the remainder of the lesson they complete an e-safety written task

Medium/Severe concern – pupil removed from the class, e-safety co-ordinator informed (e-safety alert form completed later by member of staff involved)
Sanction to be decided from one week to four weeks ban on using ICT resources.

Pupil accounts

Logging in as another user – asked to log off immediately and explain why – verbal warning given

Logging in as another user **following verbal warning** - pupil removed from the PC for the remainder of the lesson to complete an e-safety written task.
E-safety co-ordinator to decide on the length of a network access ban of between one and four weeks (for repeat offenders only)
An e-safety alert form must be completed by member of staff involved and given to e-safety co-ordinator