METROPOLITAN BOROUGH OF CALDERDALE
Woodhouse Primary School
Daisy Road, Brighouse, West Yorkshire. HD6 3SX

Tel: 01484 714750
Fax: 01484 720347
Email:admin@woodhouse.calderdale.sch.uk
www.woodhouse.calderdale.sch.uk

Headteacher: Mrs Shirley Stoker ***Deputy Headteacher: Mrs Lynn Daveney***

E - SAFETY POLICY
FEBRUARY 2010

	Date	Chair of Governors	Headteacher
Adopted	February 2010		
Reviewed	September 2011		
Reviewed			
Reviewed			
Reviewed			

WOODHOUSE PRIMARY SCHOOL

CURRICULUM AND ASSESSMENT DOCUMENTATION

E – SAFETY POLICY – FEBRUARY 2010

1. Introduction

National guidance suggests that it is essential for schools to take a leading role in e-safety. Becta in its "Safeguarding Children in a Digital World" suggested:

> *"That schools support parents in understanding the issues and risks associated with children's use of digital technologies. Furthermore, Becta recommends that all schools have acceptable use policies, and ensure that parents are aware of the procedures for e-safety within the school. Recognising the growing trend for home-school links and extended school activities, Becta recommends that schools take an active role in providing information and guidance for parents on promoting e-safety messages in home use of ICT, too."*

The Byron Review "Safer Children in a Digital World" stressed the role of schools:

> *"One of the strongest messages I have received during my Review was about the role that schools and other services for children and families have to play in equipping children and their parents to stay safe online. To empower children and raise the skills of parents, I make recommendations to Government in the following areas: delivering e-safety through the curriculum, providing teachers and the wider children's workforce with the skills and knowledge they need, reaching children and families through Extended Schools and taking steps to ensure that Ofsted holds the system to account on the quality of delivery in this area."*

The development and expansion of the use of ICT, and particularly of the internet, has transformed learning in schools in recent years. Children and young people will need to develop high level ICT skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment. There is a large body of evidence that recognises the benefits that ICT can bring to teaching and learning. Schools have made a significant investment both financially and physically to ensure these technologies are available to all learners. The benefits are perceived to "outweigh the risks." However, schools must, through their e-safety policy, ensure that they meet their statutory obligations to ensure that children and young people are safe protected from potential harm, both within and outside school. The policy will also form part of the school's protection from legal challenge, relating to the use of ICT.

2. Rationale

The use of exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement.

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

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games

- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

3. Aims

- To ensure Internet use provides effective learning.
- To enrich and extend learning activities as an integrated aspect of the curriculum.
- To provide children with access to the Internet.
- To educate children in the safe and responsible use of the Internet.
- To develop a partnership approach to Internet learning with parents, including Internet Access Guidelines.
- To develop use of the Internet in the wider community.
- To use email to discover, connect and create

4. Scope of the Policy

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

4.1 Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Safeguarding Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety within the Safeguarding Committee.

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator.
- The Headteacher and another member of the Senior Management Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The Headteacher will receive reports of e-safety incidents and create a log of incidents to inform future e-safety developments.

E-Safety Coordinator:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents.

- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- monitors ICT activity in lessons, appropriate extra curricular and extended school activities.
- provides training and advice for staff.
- liaises with the Local Authority.
- liaises with school E – Learning mentor.
- attends relevant meeting with the Safeguarding committee and Governing Body.
- reports regularly to Senior Leadership Team.

E-Learning Mentor:
The E-Learning Mentor is responsible for ensuring:
- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- that the school meets the e-safety technical requirements outlined in the YHGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance.
- that users may only access the school's networks through a properly enforced password protection policy.
- that YHGfL is informed of issues relating to the filtering applied by the Grid.

Teaching and Non- teaching Staff:
Teachers and non-teaching staff are responsible for ensuring that:
- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
- they have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP).
- they report any suspected misuse or problem using the appropriate proforma (found in the school's staff handbook), which is then handed directly to the Headteacher.
- digital communications with pupils (email / Virtual / voice) should be on a **professional** level and only carried out using official school systems and equipment.
- 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
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

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

Pupils:

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems. (nb. at KS1 it would be expected that parents / carers would sign on behalf of the pupils)
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers:

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through newsletters, letters, website and information about national / local e-safety campaigns / literature through appropriate training.

Parents and carers will be responsible for:

- endorsing (by signature) the Student / Pupil Acceptable Use Policy
- accessing the school website in accordance with the relevant school Acceptable Use Policy.

Community Users

Community Users who access school ICT systems / website as part of the Extended School provision will be expected to sign an Acceptable Use Guidelines before being provided with access to school systems.

4.2 Guidelines for Learning and Teaching

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

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

- A planned e-safety programme should be provided as part of PSHCE and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.
- Key e-safety messages should be reinforced as part of a planned programme of lessons and assemblies and pastoral activities.
- Students / pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils should be helped to understand the need for the pupil AUP 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 ICT systems / internet will be posted in all rooms and displayed on log-on screens
- Staff should act as good role models in their use of ICT, the internet and mobile devices.

Education – parents / carers
Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

"There is a generational digital divide". (Byron Report).

The school will therefore seek to provide information and awareness to parents and carers through:
- Letters, newsletters, web site,
- Parents training sessions led by Calderdale E-safety Officer

Education - Extended Schools
The school will offer family learning courses in ICT, media literacy and e-safety so that parents and children can together gain a better understanding of these issues. Messages to the public around e safety should also be targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

Education & Training – Staff
It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings and INSET days when necessary.
- The E-Safety Coordinator will provide advice, guidance and training as required to individuals as required

Training – Governors
Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in ICT / e-safety / health and safety / child protection. This will be delivered by the E-Safety Coordinator.

4.3 Technical – infrastructure / equipment, filtering and monitoring

The school will be 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. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the YHGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling are securely located and physical access restricted.

Access to the school ICT systems

- All users will have clearly defined access rights to school ICT systems (AUPs).
- **Pupil access:** All year groups will use a general password and username relating to their cohort.
- **Staff access:** All staff users will have a personal username and password, users will be made responsible for the security of their username and password must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- **Temporary access:** A general username and password will be made available for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system. This password will be changed regularly.
- The e-learning mentor will have access using the "administrator" passwords for the school ICT system; this must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe).

Filtering and monitoring

- The school maintains and supports the managed filtering service provided by YHGfL
- In the event of the e-learning mentor needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher.
- Any filtering issues should be reported immediately to YHGfL.
- Requests from staff for sites to be removed from the filtered list will be considered by the e-learning mentor and the Headteacher. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Committee
- School ICT technical staff may monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Any ICT/ e-safety incident should be logged on the relevant proforma and handed directly to the Headteacher.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- The appropriate AUP allows staff forbids staff from installing programmes on school workstations / portable devices.

4.4 Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

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

- Where pupils are allowed to freely search the internet, e.g. using search engines, this should only be done under staff supervision and staff should be vigilant in monitoring the content of e websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the e-learning mentor (with the Headteacher's permission) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

4.5 Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Staff / pupils must not take, use, share, publish or distribute images of others without their permission
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

4.6 Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Personal data is kept on the school G drive which prevents staff being able to take information off the school site unless safely encrypted or otherwise secured. When personal data is required in the case of offsite residential trips, this will be removed on an encrypted memory stick.

Staff must ensure that they:

- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.
- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

4.7 Communications

- Users need to be aware that email communications may be monitored.
- Users must immediately report, to the Headteacher using the afore mentioned proforma, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents / carers (email, chat, etc) must be professional in tone and content.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

4.8 Unsuitable / inappropriate activities (Acceptable use of the internet and other ICT communications)

This applies to all School employees, contractors, temporary staff and third parties provided with access to the School's information assets.
The internet is an unregulated environment. Although the LA has implemented pro-active filtering the School or LA will not be liable for any material viewed or downloaded.

The School's internet and e-mail facilities remain the School's property at all times, and the School may intercept communications for the purpose of monitoring or for keeping a record of communications relevant to the School's business. Where misuse of these facilities is suspected, detailed investigations will be undertaken.

Failure to comply with this policy may constitute gross misconduct and could lead to dismissal. Suspected illegal activities may also be reported to the police.

RED (Do not engage in these activities)

- DO NOT use the internet and e-mail facilities for personal purposes in works time, UNLESS usage is in compliance with the Green – acceptable use section below.
- DO NOT use e-mail to engage in gossip.
- DO NOT make libellous statements about individuals or other organisations.

- DO NOT make statements purporting to represent Woodhouse Primary School when they are personal views.
- DO NOT make derogatory remarks or express derogatory opinions regarding the school.
- DO NOT knowingly infringe copyright or intellectual property rights.
- DO NOT knowingly send or receive anything which is illegal or fraudulent.
- DO NOT knowingly view, send or receive material which is obscene, sexually explicit, offensive, defamatory, racist or homophobic in nature, or any material which is intended to cause the receiver or anyone who sees the material harassment, alarm or distress.
- DO NOT use the facility to pursue personal business interests, for gambling or for political purposes not directly related to your job.
- DO NOT allow anyone else to use your user name and password to gain Internet access or access your e-mail account or disclose your password to another person.
- DO NOT knowingly engage in any activity which threatens the integrity or availability of the school's systems.
- DO NOT attempt to gain unauthorised access to (hack) any server/facility whether inside or outside the school.
- DO NOT install any unauthorised programs, such as screen savers, on the School's information assets.

The Acceptable Use Policy for Pupils states the activities which are deemed suitable and unsuitable. See Appendix 1
A full policy for Acceptable use of the Internet for staff can be found in Appendix 2.

Responding to incidents of misuse
It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Incidents of misuse will be dealt with through normal behaviour / disciplinary procedures. However, failure to comply with this policy may constitute gross misconduct and could lead to dismissal. **Suspected illegal activities may also be reported to the police.**

5. Monitoring and evaluation:
The school will monitor the impact of the policy using:
- Logs of reported incidents
- YHGfL monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- When appropriate, the use of surveys / questionnaires of:
  - pupils (e.g. Ofsted "Tell-us" survey / CEOP ThinkUknow survey)
  - parents / carers
  - staff

6. Success Criteria
All staff aware of procedures;
Incidents dealt with in line with the policy;
All staff and pupils are aware of how to be safe while using ICT and the internet inside and outside of school.

7. Equal Opportunities and Inclusion
The school is committed to working towards equality of opportunity in all aspects of school life. Our aim is to ensure that no child is discriminated against by being treated less favourably or

by failure of staff to make reasonable adjustments to in recognition of pupils' needs and abilities.

8. Relationships with other School Policies

Due to the ever changing nature of Information and Communication Technologies, this policy will be reviewed annually in November by the Safeguarding Team and, if necessary, more frequently in response to any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place and in relation to the aims and content of other school policies such as:

- Equal Opportunities Policy
- Protecting and Safeguarding Children Policy
- Health and Safety Policy
- Professional Development Policy
- Inclusion Policy
- SEN Policy
- Induction Policy

Appendix 1 - Pupil guidelines for acceptable Internet use:

The following are **not** permitted within the school environment:

1. Sending or displaying offensive messages or pictures.
2. Using obscene language.
3. Harassing, insulting or attacking others.
4. Damaging computers, computer systems or computer networks.
5. Violating copyright laws.
6. Using others' passwords or accounts.
7. 'Hacking' into others' folders, work or files for any reason.
8. Intentionally wasting limited resources, including printer ink and paper.

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety and the safety of the school:

- I know I must have my parent's / carer's permission before using the internet.
- I know I must have a supervising teacher or member of staff with me at all times when using the internet.
- I will not disclose any password or login name to anyone, other than the persons responsible for running and maintaining the system.
- I will only access the school system using my class password.
- Under no circumstances will I view, upload or download any material which is likely to be unsuitable for children. This applies to any material of a violent, dangerous or inappropriate context. If you are unsure ask the supervisor.
- I will always respect the privacy of files of other users. I will not deliberately move, look at or delete other files.
- I will use the computers only for school work, homework or as part of an approved extra-curricular club.
- I will not put CDs or memory sticks (flash drives) into school computers unless I have permission.
- I will ensure that any messages / emails I send will be polite and sensible.
- I will only e-mail people I know, or my teacher has approved and I will inform the teacher if I receive an e-mail from someone I don't know.
- I will **never** give out my home address or phone number, or arrange to meet someone over the internet.
- I will keep all login details and passwords safe.
- If I see anything I am unhappy with or I receive messages I do not like, I will turn off the computer screen (but not shut the system down) and tell a teacher or supervising adult.
- I understand that the school may check my computer files and may monitor the Internet sites I visit.
- I will not upload photos of anyone (staff or pupils) without their permission.
- I will only use my personal hand held / external devices (mobile phones / USB devices etc) in school if I have permission. I understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community.
- I will not use internet chat in school time unless specifically directed by a teacher when accessing the school's Learning Platform.
- When using the school's Learning Platform, I will not let anyone else have access to my login details and password.
- I will follow these rules at school and when using the school's Learning Platform at home.

I understand that if I deliberately break these rules, I could be stopped from using the internet or computers.

I have read and understand the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment (both in and out of school)
- I use my own equipment in school (when allowed) e.g. mobile phones, PDAs, cameras etc
- I use my own equipment out of school in a way that is related to me being a member of this school e.g.. communicating with other members of the school, accessing school email and website etc.

Name of Pupil:

Class:

Signed: Date:

Appendix 2 - Staff (inc. Volunteers and community users) guidelines for acceptable Internet use:

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety and the safety of the school:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, etc) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

- **I will not** disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- **I will not** use the internet and e-mail facilities for personal purposes in works time, unless I have prior permission.
- **I will not** use e-mail to engage in gossip.
- **I will not** make libellous statements about individuals or other organisations.
- **I will not** make statements purporting to represent Woodhouse Primary School when they are personal views.
- **I will not** make derogatory remarks or express derogatory opinions regarding the school.
- **I will not** knowingly infringe copyright or intellectual property rights.
- **I will not** knowingly send or receive anything which is illegal or fraudulent.
- **I will not** knowingly view, send or receive material which is obscene, sexually explicit, offensive, defamatory, racist or homophobic in nature, or any material which is intended to cause the receiver or anyone who sees the material harassment, alarm or distress.
- **I will not** use the facility to pursue personal business interests, for gambling or for political purposes not directly related to your job.
- **I will not** knowingly engage in any activity which threatens the integrity or availability of the school's systems.
- **I will not** attempt to gain unauthorised access to (hack) any server/facility whether inside or outside the school.
- **I will not** install any unauthorised programs, such as screen savers, on the school's information assets.

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

- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website /) it will not be possible to identify by full name, or other personal information, those who are featured.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in this policy (**4.6**). Where personal data is transferred outside the secure school network, it must be encrypted.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

Use of Social Networking Sites:

When using Social Networking Sites:

- I will not bring myself or the school into disrepute.
- I will not mention staff, school or school business.
- I will have the highest privacy settings on my site, including disabling the 'search' function so my page is unable to be found through a search tool.
- I will not be friends with any pupils, past or present.
- I will make the E-Safety Coordinator aware of any pupils (present, therefore under the legal age) who have a page on a social networking site.

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

User Name: **Signed:** **Date:**

Appendix 3 - Parent / Carer/ guidelines for acceptable Internet use:
The school will try to ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

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

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

- I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of ICT – both in and out of school.
- I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
- I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.
- I understand that my child (who is under the age of 13years) should not be legally accessing a Social Networking Site, and if the school discover that to be the case, they will contact me and support me in ensuring my child is aware of the dangers posed.
- I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Permission Form

Parent / Carers Name:	
Student / Pupil Name:	

Signed:		Date:	

Appendix 4: Legislation

Schools should be aware of the legislative framework under which this E-Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.
It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994
This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988
It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. You Tube).

Telecommunications Act 1984
It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994
This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they: -

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964
Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998
This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006
Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

Appendix 5: Links to other organisations or documents

Child Exploitation and Online Protection Centre (CEOP)
http://www.ceop.gov.uk/

ThinkUKnow
http://www.thinkuknow.co.uk/

CHILDNET
http://www.childnet-int.org/

INSAFE
http://www.saferinternet.org/ww/en/pub/insafe/index.htm

BYRON REVIEW ("Safer Children in a Digital World")
http://www.dcsf.gov.uk/byronreview/

Becta
Website e-safety section - **http://schools.becta.org.uk/index.php?section=is**
Developing whole school policies to support effective practice:
http://publications.becta.org.uk/display.cfm?resID=25934&page=1835
Signposts to safety: Teaching e-safety at Key Stages 1 and 2 and at Key Stages 3 and 4:
http://publications.becta.org.uk/display.cfm?resID=32422&page=1835
"Safeguarding Children in a Digital World"
http://schools.becta.org.uk/index.php?section=is&catcode=ss_to_es_tl_rs_03&rid=13344

LONDON GRID FOR LEARNING
http://cms.lgfl.net/web/lgfl/365

KENT NGfL
http://www.kented.org.uk/ngfl/ict/safety.htm

NORTHERN GRID
http://www.northerngrid.org/ngflwebsite/esafety_server/home.asp

NATIONAL EDUCATION NETWORK
NEN E-Safety Audit Tool: **http://www.nen.gov.uk/hot_topic/13/nen-e-safety-audit-tool.html**

CYBER-BULLYING
DCSF - Cyberbullying guidance
http://publications.teachernet.gov.uk/default.aspx?PageFunction=productdetails&PageMode=spectrum&ProductId=DCSF-00658-2007
Teachernet
http://www.teachernet.gov.uk/wholeschool/behaviour/tacklingbullying/cyberbullying/
Teachernet "Safe to Learn – embedding anti-bullying work in schools"
http://www.teachers.gov.uk/wholeschool/behaviour/tacklingbullying/safetolearn/
Anti-Bullying Network - **http://www.antibullying.net/cyberbullying1.htm**
Cyberbullying.org - **http://www.cyberbullying.org/**

East Sussex Council – Cyberbullying - A Guide for Schools:
https://czone.eastsussex.gov.uk/supportingchildren/healthwelfare/bullying/Pages/eastsussexandnationalguidance.aspx

References to other relevant anti-bullying organisations can be found in the appendix to the DCSF publication "Safe to Learn" (see above)

SOCIAL NETWORKING
Home Office Task Force - Social Networking Guidance -
http://police.homeoffice.gov.uk/operational-policing/crime-disorder/child-protection-taskforce

Digizen – "Young People and Social Networking Services":
http://www.digizen.org.uk/socialnetworking/

Ofcom Report:
http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/socialnetworking/summary/

MOBILE TECHNOLOGIES
"How mobile phones help learning in secondary schools":
http://partners.becta.org.uk/index.php?section=rh&catcode=_re_rp_02_a&rid=15482

Mobile phones and cameras:
http://schools.becta.org.uk/index.php?section=is&catcode=ss_to_es_pp_mob_03

DATA PROTECTION AND INFORMATION HANDLING
Information Commissioners Office - Data Protection:
http://www.ico.gov.uk/Home/what_we_cover/data_protection.aspx

BECTA - Data Protection:
http://schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_saf_dp_03

PARENTS GUIDES TO NEW TECHNOLOGIES AND SOCIAL NETWORKING:
http://www.iab.ie/

Resources

Links to other resource providers:
BBC Chatguides: **http://www.bbc.co.uk/chatguide/index.shtml**

Kidsmart: **http://www.kidsmart.org.uk/default.aspx**

Know It All - **http://www.childnet-int.org/kia/**

Cybersmart - **http://www.cybersmartcurriculum.org/home/**

NCH - **http://www.stoptextbully.com/**

Chatdanger - **http://www.chatdanger.com/**

Internet Watch Foundation: **http://www.iwf.org.uk/media/literature.htm**

Digizen – cyber-bullying films: **http://www.digizen.org/cyberbullying/film.aspx**

London Grid for Learning: **http://cms.lgfl.net/web/lgfl/safety/resources**

Appendix 6: Glossary of terms

AUP Acceptable Use Policy – see templates earlier in this document

Becta British Educational Communications and Technology Agency (Government agency promoting the use of information and communications technology)

CEOP Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.

CPD Continuous Professional Development

CYPS Children and Young Peoples Services (in Local Authorities)

DCSF Department for Children, Schools and Families

ECM Every Child Matters

FOSI Family Online Safety Institute

HSTF Home Secretary's Task Force on Child Protection on the Internet

ICO Information Commissioners Office

ICT Information and Communications Technology

ICTMark Quality standard for schools provided by Becta

INSET In-Service Education and Training

IP address The label that identifies each computer to other computers using the IP (internet protocol)

ISP Internet Service Provider

ISPA Internet Service Providers' Association

IWF Internet Watch Foundation

JANET Provides the broadband backbone structure for Higher Education and for the National Education Network and RBCs.

KS1 Key Stage 1 (2, 3, 4 or 5) – schools are structured within these multiple age groups e.g. KS3 = years 7 to 9 (age 11 to 14)

LA Local Authority

LAN Local Area Network

Learning Platform A learning platform brings together hardware, software and supporting services to support teaching, learning, management and administration.

LSCB Local Safeguarding Children Board

MIS Management Information System

MLE Managed Learning Environment

NEN National Education Network – works with the Regional Broadband Consortia (e.g. YHGfL) to provide the safe broadband provision to schools across Britain.

Ofcom	Office of Communications (Independent communications sector regulator)
Ofsted	Office for Standards in Education, Children's Services and Skills
PDA	Personal Digital Assistant (handheld device)
PHSE	Personal, Health and Social Education
RBC	Regional Broadband Consortia (e.g. YHGfL) have been established to procure broadband connectivity for schools in England. There are 10 RBCs covering 139 of the 150 local authorities:
SEF	Self Evaluation Form – used by schools for self evaluation and reviewed by Ofsted prior to visiting schools for an inspection
SRF	Self Review Form – a tool used by schools to evaluate the quality of their ICT provision and judge their readiness for submission for the ICTMark
TUK	Think U Know – educational e-safety programmes for schools, young people and parents.
	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol
YHGfL	Yorkshire and Humberside Grid for Learning – the Regional Broadband Consortium for Calderdale and our neighbouring Local Authorities – is the provider of broadband and other services for schools and other organisations in Y and H.

Appendix 7: Ideas for schools to consider
Schools may wish to use the following prompts when determining and evaluating their policy, which are based on a document contained in the DCSF "Safe to Learn" Overview:

Discuss, monitor and review

- Do we hold discussions on e-safety and its definition, involving staff, children and young people, governors and parents?
- Do we keep a record of the incidence of e-safety incidents, according to our agreed definition, and analyse it for patterns – people, places, groups, technologies?
- Do we ask ourselves what makes an e-safe school?
- What is our school doing to ensure that our children and young people do not feel vulnerable and are safe to learn, when engaged in online activities?
- Do we celebrate our successes and draw these to the attention of parents/carers and the wider community?

Support everyone in the school community to identify and respond

- Do we work with staff and outside agencies to identify all potential forms of e-safety incidents?
- Do we actively provide systematic opportunities for developing pupils' skills to develop safe online behaviour?
- Have we considered all the opportunities where this can be addressed – through the curriculum; through corridor displays; through assemblies; through the School Council; through peer support; and through the website and parents' evenings and newsletters?
- Do we ensure that there is support for vulnerable children and young people?
- Do we train all staff to be aware of potential e-safety issues and follow school policy and procedures on e-safety?
- Do our staff feel adequately supported to be able to respond to and manage e-safety related incidents?

Ensure that children and young people are aware of how and to whom e-safety incidents should be reported and understand that all e-safety concerns will be dealt with sensitively and effectively

- Do we acknowledge and learn from the high level of skills and knowledge of children and young people in the use of new technologies? (Often referred to as the "digital natives")
- Do we regularly canvass children and young people's views on the extent and nature of e-safety issues?
- Do we ensure that young people know how to express worries and anxieties about e-safety?
- Do we ensure that all children and young people are aware of the range of sanctions which may be applied against those involved in e-safety misuse?
- Do we involve children and young people in e-safety campaigns in school?
- Do we demonstrate that we are aware of the power of peer support? Have we created and publicised schemes of peer mentoring or counselling; buddying or mediation, for example?
- Do we include the phone numbers of help-lines in the school's student planners?
- Have we made children and young people aware of "how to report abuse"?
- Do we have an e-safety notice board?
- How else do we bring e-safety messages to children and young people's attention?
- What role does our School Council already play in our e-safety work? How might that involvement be enhanced?
- Do we offer sufficient support to children and young people who have been involved in e-safety incidents?
- Do we work with children and young people who have been involved, or may be seen as being at risk?

Ensure that parents/carers are aware of e-safety issues and that those expressing concerns have them taken seriously

- Do we work with parents and the local community to address issues beyond the school gates that give rise to e-safety issues? – particularly with regard to the possible lack of filtering and monitoring of internet access by children and young people out of school and with regard to cyber-bullying incidents
- Do parents know whom to contact if they are worried about e-safety issues?
- Do parents know about our complaints procedure and how to use it effectively?

Learn from effective e-safety work elsewhere and establish effective collaboration

- Have we invited colleagues from a school with effective e-safety policies and practice to talk to our staff?
- Have we involved local authority staff or other local / regional experts in any way?
- Do we have an established link with the police?