'A brighter tomorrow'

Wood End Primary School
E-Safety Policy

School Aims:

- Ensure every child has the opportunity to achieve their full potential – intellectually, educationally, physically, emotionally, morally and spiritually;
- Develop positive attitudes and approaches to learning and social awareness which enables pupils to make appropriate choices for success throughout their lives;
- Work in partnership with parents and community to enable pupils to make a positive contribution to society;
- Provide a safe, stimulating and creative environment in which pupils are all encouraged to learn;
- Deliver a broad and balanced curriculum which motivates pupils to aspire for lifelong learning;
- Set challenging yet achievable targets for individual and school improvement in order to raise standards;
- Work towards ensuring that our pupils will become self-confident, sympathetic, open-minded and well balanced members of society.

Policy approved by Governors June 2017 ……(Chair of governors)…… date

To be reviewed May 2018

Aims:

Wood End Primary School:

- believes that online safety (e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles.
- identifies that the Internet and information communication technologies are an important part of everyday life, so children must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online.
- has a duty to provide the community with quality Internet access to raise education standards, promote achievement, support professional work of staff and enhance management functions.
- identifies that there is a clear duty to ensure that all children and staff are protected from potential harm online.

The purpose of this e-safety policy is to:

- Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use technology to ensure that Wood End Primary School is a safe and secure environment.
- Safeguard and protect all members of the school's community online.
- Raise awareness with all members of the school's community regarding the potential risks as well as benefits of technology.
- To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

- This policy applies to all staff including the governing body, teachers, support staff, external contractors , visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as children and parents/carers. (amend staff roles as appropriate to the setting)
- This policy applies to all access to the Internet and use of information communication devices, including personal devices, or where children, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets or mobile phones.
- This policy must be read in conjunction with other relevant school policies:
  safeguarding and child protection
  anti-bullying
  discipline and behaviour
  e-learning curriculum
  acceptable use (see appendix)
  confidentiality
  relevant curriculum policies including; computing, Personal Social and Health Education (PSHE), Sex and Relationships Education (SRE).

Roles and Responsibilities:

The key responsibilities of the school management and leadership team and the subject leader are:

- Developing, owning and promoting the online safety vision and culture to all stakeholders, in line with national and local recommendations with appropriate support and consultation throughout the school community.
- Ensuring that online safety is viewed by the whole community as a safeguarding issue and proactively developing a robust online safety culture.
- Supporting the Designated Safeguarding Lead (DSL) by ensuring they have sufficient time and resources to fulfil their online safety role and responsibilities.
- Ensuring there are appropriate and up-to-date policies and procedures regarding online safety including an Acceptable Use Policy which covers appropriate professional conduct and use of technology.
- To ensure that suitable and appropriate filtering and monitoring systems are in place to protect children from inappropriate content which meet the needs of the school community whilst ensuring children have access to required educational material.
- To work with and support technical staff in monitoring the safety and security of school/setting systems and networks and to ensure that the school/setting network system is actively monitored.
- Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.
- Ensuring that online safety is embedded within a progressive whole school/setting curriculum which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.
- To be aware of any online safety incidents and ensure that external agencies and support are liaised with as appropriate.
- Receiving and regularly reviewing online safeguarding records and using them to inform and shape future practice.
- Ensuring there are robust reporting channels for the school/setting community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.
- To ensure a member of the Governing board is identified with a lead responsibility for supporting online safety.
- Auditing and evaluating current online safety practice to identify strengths and areas for improvement.

The key responsibilities of the Designated Safeguarding Lead are:

- Acting as a named point of contact on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate.
- Work with the school lead for data protection and data security to ensure that practice is in line with current legislation.
- Maintaining a record of online safety concerns/incidents and actions taken as part of the school's safeguarding recording structures and mechanisms.
- Monitor the school/settings online safety incidents to identify gaps/trends and use this data to update the school/settings education response to reflect need
- To report to the school management team, Governing Board and other agencies as appropriate, on online safety concerns and local data/figures.
- Liaising with the local authority and other local and national bodies, as appropriate.
- Working with the school leadership and management to review and update the online safety policies, Acceptable Use Policies (AUPs) and other related policies on a regular basis with stakeholder input.
- Ensuring that online safety is integrated with other appropriate school policies and procedures.

The key responsibilities for all members of staff are:

- Contributing to the development of online safety policies.
- Reading the school Acceptable Use Policies (AUPs) and adhering to them.
- Taking responsibility for the security of school systems and data.
- Having an awareness of a range of different online safety issues and how they may relate to the children in their care.
- Modelling good practice when using new and emerging technologies
- Embedding online safety education in curriculum delivery wherever possible.
- Identifying individuals of concern and taking appropriate action by following school safeguarding policies and procedures.
- Knowing when and how to escalate online safety issues, internally and externally.
- Being able to signpost to appropriate support available for online safety issues, internally and externally.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site.
- Demonstrating an emphasis on positive learning opportunities.
- Taking personal responsibility for professional development in this area.

In addition to the above, the key responsibilities for staff managing the technical environment are:

- Providing a safe and secure technical infrastructure which support safe online practices while ensuring that learning opportunities are still maximised.
- Taking responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team.
- To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices.
- Ensuring that the schools filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the DSL.
- Ensuring that the use of the school/setting's network is regularly monitored and reporting any deliberate or accidental misuse to the DSL.
- Report any breaches or concerns to the DSL and leadership team and together ensure that they are recorded and appropriate action is taken as advised.
- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
- Report any breaches and liaising with the local authority (or other local or national bodies) as appropriate on technical infrastructure issues.

- Providing technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Ensuring that the school's ICT infrastructure/system is secure and not open to misuse or malicious attack.
- Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.
- Ensure that appropriately strong passwords are applied and enforced for all but the youngest users.

The key responsibilities of children and young people are:
- Contributing to the development of online safety policies.
- Reading the school/setting Acceptable Use Policies (AUPs) and adhering to them.
- Respecting the feelings and rights of others both on and offline.
- Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.

At a level that is appropriate to their individual age, ability and vulnerabilities:
- Taking responsibility for keeping themselves and others safe online.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

The key responsibilities of parents and carers are:
- Reading the school/setting Acceptable Use Policies, encouraging their children to adhere to them, and adhering to them themselves where appropriate.
- Discussing online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.
- Role modelling safe and appropriate uses of technology and social media.
- Identifying changes in behaviour that could indicate that their child is at risk of harm online.
- Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.
- Contributing to the development of the school's online safety policies.
- Using school systems, such as learning platforms, and other network resources, safely and appropriately.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

Rationale

E-safety encompasses Internet technologies and electronic communications such as mobile phones, tablets and laptops as well as collaboration tools and personal publishing. It highlights the need to educate pupils and the school community about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

Our E-Safety Policy has been written by the school, building on the guidelines from BECTA and recent documentation and good practice.

The schools has an E-Safety subject leader (J Staffiere) who works closely with the Designated Safe Guarding Lead.

Managing the school/setting website

Wood End Primary School will ensure that information posted on the school website meets the requirements as identified by the Department for Education (DfE).
The contact details on the website will be the school address, email and telephone number. Personal

information will not be published.
The head teacher will take overall editorial responsibility for online content published and will ensure that information is accurate and appropriate.
The school will post information about safeguarding, including online safety, on the school website for members of the community.

Managing email

Pupils may only use school provided email accounts for educational purposes.
All members of staff are provided with a specific school email address to use for any official communication.
The use of personal email addresses by staff for any official school business is not permitted.
The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using secure and encrypted email.
Access to school email systems will always take place in accordance to data protection legislation and in line with other appropriate school policies e.g. confidentiality.
Members of the community must immediately tell a designated member of staff if they receive offensive communication.
Staff will be encouraged to develop an appropriate work life balance when responding to email, especially if communication is taking place between staff and pupils and parents.
The deputy head teacher and/or the head teacher must always be copied in (cc'd) when members of staff communicate via email with parents or pupils.
Excessive social email use can interfere with teaching and learning and will be restricted. Access in school to social networking sites will be blocked.
Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
The school will have a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff.
School email addresses and other official contact details will not be used for setting up personal social media accounts.

Official videoconferencing and webcam use for educational purposes

Wood End Primary School acknowledges that videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
All videoconferencing equipment will be switched off when not in use and where appropriate, not set to auto answer.
Videoconferencing contact details will not be posted publically.
Video conferencing equipment will be kept securely and, if necessary, locked away when not in use.
Staff will ensure that external videoconference opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access events are appropriately safe and secure.

Users
Pupils will always ask permission from a teacher before making or answering a videoconference call or message.
Videoconferencing will be supervised appropriately for the pupils' age and ability.
Unique log on and password details for the educational videoconferencing services will only be issued to members of staff and kept secure.

Appropriate and safe classroom use of the Internet and any associated devices

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

Internet use is a key feature of educational access and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum.

Access levels to the Internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.

All members of staff are reminded that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential.

Supervision of pupils will be appropriate to their age and ability.

All school owned devices will be used in accordance with the school Acceptable Use Policy and with appropriate safety and security measure in place.

Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

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 use age appropriate search tools (schools should list search tools suggested for staff and pupils to use such as SWGfL Squiggle, Dorling Kindersley find out, Google Safe Search or CBBC safe search) as decided by the school following an informed risk assessment to identify which tool best suits the needs of our community.

The school will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information.

Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

The school will use the Internet to enable pupils and staff to communicate and collaborate in a safe and secure environment.

If pupils encounter material they feel is distasteful, uncomfortable or threatening, they should report the address of the site to a member of staff.

Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

Management of school learning platform

Leaders/managers and staff will regularly monitor the usage of the Learning Platform (LP) in all areas, in particular discussion and communication tools and publishing facilities.

Pupils/staff will be advised about acceptable conduct and use when using the LP.

Only members of the current pupil and staff community will have access to the LP.

All users will be mindful of copyright issues and will only upload appropriate content onto the LP.

When staff, pupils' etc. leave the school their account or rights to specific school areas will be disabled.

Any concerns about content on the LP will be recorded and dealt with in the following ways:

a) The user will be asked to remove any material deemed to be inappropriate or offensive.

b) The material will be removed by the site administrator if the user does not comply.

c) Access to the LP for the user may be suspended.

d) The user will need to discuss the issues with a member of leadership before reinstatement.

e) A pupil's parent/carer may be informed.

Information system security

School computing systems capacity and security will be reviewed regularly in line with the Wolverhampton LA Guidelines and SLA.
Virus protection will be updated regularly.
Security strategies will be discussed with the e-learning support team and on site technician as appropriate.
Use of USB sticks will be reviewed. Personal USB sticks may not be brought into school.
Backup procedures are in place where all essential office data is backed up off site.

Social Media

Expectations regarding safe and responsible use of social media will apply to all members of Wood End Primary School community and exist in order to safeguard both the school and the wider community, on and offline. Examples of social media may include blogs, wikis, social networking sites, forums, bulletin boards, multi-player online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.
All members of the school community will be encouraged to engage in social media in a positive, safe and responsible manner at all times.
All members of the school community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
School will control, limit and supervise accordingly pupil and staff access to social media and social networking sites whilst on site and when using school provided devices and systems.
The use of social networking applications during contact times in school hours for personal use is not permitted.
Any concerns regarding the online conduct of any member of the school community on social media sites should be reported to the leadership team and will be managed in accordance with policies such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.
Any breaches of school policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be accordance with relevant policies, such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.

Staff personal use of social media

The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school Acceptable Use Policy.
All members of staff are advised not to communicate with or add as 'friends' any current or past children/pupils or current or past pupils' family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead and/or the headteacher.
If ongoing contact with pupils is required once they have left the school roll, then members of staff will be expected to use existing alumni networks or use official school provided communication tools.
All communication between staff and members of the school community on school business will take place via official approved communication channels (such as an official setting provided email address or phone numbers)
Staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher.
Any communication from pupils/parents received on personal social media accounts will be reported to the schools designated safeguarding lead.

Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members, colleagues etc. will not be shared or discussed on personal social media sites.
All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.
All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with schools policies (safeguarding, confidentiality, data protection etc.) and the wider professional and legal framework.
Members of staff will be encouraged to manage and control the content they share and post online. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis.
Members of staff will notify the Leadership/Management Team immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the school/setting.
Members of staff are encouraged not to identify themselves as employees of Wood End Primary School on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members and the wider community.
Members of staff will ensure that they do not represent their personal views as that of the school on social media.
School email addresses will not be used for setting up personal social media accounts.

Staff official use of social media

If members of staff are participating in online activity as part of their capacity as an employee of the school, then they are requested to be professional at all times and to be aware that they are an ambassador for the school.
Staff using social media officially will disclose their official role/position but always make it clear that they do not necessarily speak on behalf of the school.
Staff using social media officially will be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
Staff using social media officially will always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.
Staff must ensure that any image posted on any official social media channel have appropriate written parental consent.
Staff using social media officially will be accountable and must not disclose information, make commitments or engage in activities on behalf of the school/setting unless they are authorised to do so.
Staff using social media officially will inform the Designated Safeguarding Lead and the head teacher of any concerns such as criticism or inappropriate content posted online.
Staff will not engage with any direct or private messaging with children or parents/carers through social media and will communicate via official communication channels.
Staff using social media officially will sign the school social media Acceptable Use Policy.

Pupils' use of social media

Safe and responsible use of social media sites will be outlined for children and their parents as part of the Acceptable Use Policy.
Personal publishing on social media sites will be taught to pupils as part of an embedded and progressive education approach via age appropriate sites which have been risk assessed and approved as suitable for educational purposes.

Pupils will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and/or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, Instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs etc.
Pupils will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.
Pupils will be advised on appropriate security on social media sites and will be encouraged to use safe and passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.
Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.
Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour and discipline.
Concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, could be raised with parents/carers, particularly when concerning any underage use of social media sites.

Use of Personal Devices and Mobile Phones

The widespread ownership of mobile phones and a range of other personal devices among children, young people and adults will require all members of the school community to take steps to ensure that mobile phones and personal devices are used responsibly.
Wood End Primary School recognises that personal communication through mobile technologies is an accepted part of everyday life for children, staff and parents/carers but requires that such technologies need to be used safely and appropriately within schools/settings.

Expectations:
All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies.
Electronic devices of all kinds that are brought in on site are the responsibility of the user at all times. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
Mobile phones and personal devices are not permitted to be used on school site (except for in the staff room or head teacher's office).
The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community and any breaches will be dealt with as part of the discipline and behaviour policy.
All members of the school community should take steps to protect their mobile phones or devices from loss, theft or damage.
All members of the school community should use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen. Passwords and pin numbers should be kept confidential. Mobile phones and personal devices should not be shared.
All members of the school community should ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school/settings policies.
School mobile phones and devices must always be used in accordance with the Acceptable Use Policy and any other relevant policies.
School devices used for communication with parents and pupils must be suitably protected via a passcode/password/pin and must only be accessed and used by members of staff.

Staff use of personal devices and mobile phones

Members of staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity. Any pre-existing relationships which could compromise this will be discussed with leaders/managers.
Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and will only use work-provided equipment for this purpose.
Staff will not use any personal devices directly with children and will only use work-provided equipment during lessons/educational activities.
Members of staff will ensure that any use of personal phones and devices will always take place in accordance with the law e.g. data protection as well as relevant school policy and procedures e.g. confidentiality, data security, Acceptable Use etc.
Staff personal mobile phones and devices will be switched off/switched to 'silent' mode and stored in an appropriate place during lesson times, e.g personal locker; teacher's cupboard; staff room.
Personal mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the Leadership Team in emergency circumstances.
Staff will ensure that any content bought on site via mobile phones and personal devices are compatible with their professional role and expectations.
If a member of staff breaches the school policy then disciplinary action will be taken.
If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence then the police will be contacted.
Any allegations against members of staff involving personal use of mobile phone or devices will be responded to following the school policy.

Visitors' use of personal devices and mobile phones

Parents/carers and visitors must use mobile phones and personal devices in accordance with the school acceptable use policy.
Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with the school image use policy.
The school will ensure appropriate signage and information is displayed and provided to inform visitors of expectations of use.

Reducing online risks

At Wood End Primary School we are aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.
Emerging technologies will be examined for educational benefit and subject leader will ensure that appropriate risk assessments are carried out before use in school is allowed.
The school will ensure that appropriate filtering and monitoring systems are in place to prevent staff and pupils from accessing unsuitable or illegal content.
The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not always possible to guarantee that access to unsuitable material will never occur via a school computer or device.
Methods to identify, assess and minimise online risks will be reviewed regularly by the subject leader and school leadership team.

Publishing pupil's images and work

Photographs that include pupils will be selected carefully. When the children first start their journey at Wood End the parents will sign a consent form allowing the school to use the children's photographs around the school, work published by the school and on occasions from outside agencies that have been checked by the school. Parents, who do not want pictures taken of their children, will state this on the consent form.
Pupils' contribute to blogs and discussions through our school website which means names are available.

However, each child has an individual password and username and only the pupils' from Wood End can access our school site.
Pupil's work can only be published with the permission of the pupil and parents.

Engagement and education of children and young people

An online safety (e-Safety) curriculum will be established and embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible Internet use amongst pupils.
Pupils' input will be sought when reviewing school online safety policies and practices, including curriculum development and implementation.
All users will be informed that network and Internet use will be monitored.
Online safety (e-Safety) will be included in the PSHE, SRE and Computing programmes of study, covering both safe school and home use.
Acceptable Use expectations and Posters will be posted in identified key areas of the school site.
Safe and responsible use of the Internet and technology will be reinforced across the curriculum and within all subject areas.
External support will be used to complement and support the schools internal online safety (e-Safety) education approaches.
The school will implement peer education to develop online safety as appropriate to the needs of the pupils, e.g. Digital Ambassadors.

Engagement and education of staff

The online safety (e-Safety) policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of our safeguarding responsibilities.
Staff will be made aware that our Internet traffic can be monitored and traced to the individual user.
Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff in a variety of ways, on a regular (at least annual) basis.
All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

Engagement and education of parents and carers

Wood End Primary School recognises that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology.
Parents' attention will be drawn to the school online safety (e-Safety) policy and expectations in newsletters, letters, school prospectus and on the school website.
A partnership approach to online safety at home and at school with parents will be encouraged. This may include offering parent workshops with demonstrations and suggestions for safe home Internet use or highlighting online safety at other well attended events e.g. parent evenings.
Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.
Information and guidance for parents on online safety will be made available to parents in a variety of formats.
Parents will be encouraged to role model positive behaviour for their children online.

Passwords

All users should not to share passwords or information with others and not to login as another user.
Staff and pupils must always keep their password private and must not share it with others or leave it where others can find it.
All members of staff will have their own unique username and private passwords to access school

systems. Members of staff are responsible for keeping their password private.
We require staff and pupils to use STRONG passwords for access into our system and change their passwords regularly.

Managing filtering

The school will work with Wolverhampton LA and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
If staff or pupils discover an unsuitable site, it must be reported to the E Safety subject leader and/or the DSL.
Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
Any material that the school believes is illegal must be reported to appropriate agencies (E Learning Support Team).

Responding to Online Incidents and Safeguarding Concerns

All members of the community should be aware of the range of online risks that are likely to be encountered including sexting, online/cyber bullying etc. This will be highlighted within staff training and educational approaches for pupils.
All members of the school community are informed about the procedure for reporting online safety (e-Safety) concerns, such as breaches of filtering, sexting, cyberbullying, illegal content etc.
The Designated Safeguarding Lead (DSL) will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded.
The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Safeguarding Children Board thresholds and procedures.
Complaints about Internet misuse will be dealt with under the School's complaints procedure.
Complaints about online/cyber bullying will be dealt with under the School's anti-bullying policy.
Any complaint about staff misuse will be referred to the head teacher.
Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
Staff will be informed of the complaints and whistleblowing procedure.
All members of the school community need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
All members of the school community are regularly reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.
The school will manage online safety (e-Safety) incidents in accordance with the school discipline and behaviour policy where appropriate.
The school will inform parents/carers of any incidents of concerns when required.
After any investigations are completed, the school leadership team will debrief, identify lessons learnt and implement any changes as required.
Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Education Safeguarding Team or Police via 101 or 999 if there is immediate danger or risk of harm.
The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the local Police.
If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Education Safeguarding Team.
If an incident of concern needs to be passed beyond the school community, then the concern will be escalated to the Education Safeguarding Team to communicate to other schools in Wolverhampton.
Parents and children will need to work in partnership with the school to resolve issues.

Appendix A

Wood End Primary School

Acceptable Internet and Email Use Agreement

For Staff

The computer system is owned by the school and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management. The school's Internet Access Policy has been drawn up to protect all parties - the students, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

- Access must only be made via the authorised account and password, which must not be made available to any other person.
- All Internet use should be appropriate to staff professional activity or education.
- Activity that threatens the integrity of the school ICT systems, or that attacks or corrupts other systems, is forbidden.
- Sites and materials accessed must be appropriate to work in school. Users will recognise materials that are inappropriate and should expect to have their access removed.
- Users are responsible for email they send and for contacts made that may result in email being received.
- The same professional levels of language and content should be applied as for letters or other media, particularly as email is often forwarded.
- Posting anonymous messages and forwarding chain letters is forbidden.
- Copyright of materials and intellectual property rights must be respected.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.

Staff requesting Internet access must sign a copy of this and return it to the e-safety coordinator for approval before access will be granted.

I have received and read a copy of the schools Internet and Email policy and agree to abide by it. I understand my accesses will be monitored.

Full name … … … … … … … … Form/post … … … … … … … … …

Signed … … … … … … … … Date … … … … … … … … … … … … …

Access granted … … … … … … … Date … … … … … … … … … … … …

Appendix B

Wood End Primary School

Rules for Responsible Internet Use

Primary Pupils

The school has installed computers and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

- I will not access other people's files.
- I will not bring any USB devices in to school unless I have permission from a teacher.
- I will only use the computers and iPads for school work and homework.
- I will only email people within the school website.
- I will make sure the comments I post on the school website and emails are sensible and appropriate.
- I will not give my home address or phone number or arrange to meet anyone.
- To help protect other pupils and myself, I will tell a teacher if I see anything I am unhappy with or I receive messages I do not like.
- I understand that the school will check my computer files and will monitor the Internet sites I visit.
- I will follow the SMART rules when using the Internet.

Full name … … … … … … … …

Signed … … … … … … … … Date … … … … … … … … … … … … …