Woodfall Primary & Nursery School

E-SAFETY POLICY

May 2019

In Consultation with		
Date Agreed	**Name**	**Position**
	Helen Hough	Headteacher
14.05.19		
	Duncan Haworth	Chair of Governors
Date for Review: 2021		

CONTENTS

Section

1.0 Rationale

The internet and other digital technologies permeate all aspects of life in a modern technological society. Internet use is part of the statutory National Curriculum and is a necessary tool for both staff and pupils. It is the entitlement of every pupil to have access to the internet and digital technologies in order to enrich and enhance his/her learning.

Scope

This policy applies to all pupils, all teaching staff, all support staff, all governors and all volunteers.

This policy should be read in conjunction with the Safeguarding Policy, Acceptable Use Policy, Social Networking Policy, GDPR Policy and Computing Policy.

2.0 Aims

Our aims are to ensure that all pupils, including those with special educational needs:

- will use the internet and other digital technologies to support, extend and enhance their learning;
- will develop an understanding of the uses, importance and limitations of the internet and other digital technologies in the modern world, including the need to avoid undesirable material;
- will develop a positive attitude to the internet and develop their Computing capability through both independent and collaborative working;
- will use existing, as well as up and coming, technologies safely.

3.0 Internet Use

3.1 Internet use will support, extend and enhance learning.

- Pupils will be given clear objectives for internet use.
- Internet content will be subject to age-appropriate filters applied by networking and machine use in school.
- Internet use will be embedded in the curriculum.

3.2 Pupils will develop an understanding of the uses, importance and limitations of the internet.

- Pupils will be taught how to effectively use the internet for research purposes.
- Pupils will be taught to evaluate information on the internet. They will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught how to report inappropriate web content.
- Pupils will develop a positive attitude to the internet and develop their ICT capability through both independent and collaborative working.

- Pupils will use the internet to enhance their learning experience.
- Pupils have opportunities to engage in independent and collaborative learning using the internet and other digital technologies.

4.0 Managing Internet Access

4.1 Authorised Internet Access

- Staff will read and sign the Acceptable Use Policy before using any school ICT resource.
- Parents will read and sign an internet access consent form before their children are given access to internet resources. These are signed before the children start at the school.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- Pupils will be taught to use the internet responsibly and to report any inappropriate content to a responsible adult.

4.2 Security System

- School ICT systems and security will be reviewed regularly by our IT Technician.
- Virus protection will be installed on every computer and will be set to update automatically.
- Staff and pupils are required to enter their login details and password to access the school server.
- The Securus security system is installed on all pupil computers. Misuse or unacceptable behaviour is reported in an incident log located in the Headteacher's office.

5.0 E-mail

- Pupils and staff may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a member of staff if they receive unacceptable e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone.
- Staff to pupil email communication (as part of the curriculum) must only take place via a school email address and will be monitored.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- Staff must inform the Headteacher if they receive an offensive or inappropriate e-mail.

6.0 Publishing

6.1 Published content and the school website

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.

6.2 Publishing photographs, images and work

- Pupils' full names will not be used on the school website, including via social media, particularly in association with photographs.
- Written permission from parents or carers is always obtained before photographs or images of pupils are published.
- Parents should be clearly informed of the school policy on image taking and publishing.
- Staff will not keep images of children on personal devices e.g. memory sticks, or use them for any use other than in school.

7.0 Social networking and personal publishing

- All users will be advised to never give out personal details of any kind which may identify them or their location.
- Pupils, parents and staff will be advised on the safe use of social network spaces.
- Pupils will be advised to use nicknames and avatars when using social networking sites.
- Staff will be advised that they should consider the consequences and possible repercussions of any information that they make available online, for example on a social network site. Particular care should be taken in the posting of photographs, videos and information related to the school, school life, staff and pupils.

8.0 Managing filtering

- The school will work in partnership with the local authority to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable online materials, the site must be reported to a member of staff.
- The school will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

9.0 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed, as per local authority policy and the job description of our IT Technician.

10.0 Other Devices

- Mobile phones and associated cameras will not be used during lessons or formal school time.
- Mobile phones are not permitted to be used on the school premises by pupils.
- Pupil's mobile phones are stored by the class teacher in their rooms.
- Staff mobiles are on silent/or switched off and away from use.
- The sending of abusive, offensive or inappropriate material is forbidden.
- Staff should not share personal telephone numbers with pupils and parents (a school phone is provided for staff where contact with parents is required).

11.0 Data Protection

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation 2018 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.

Please cross reference with our School GDPR Policy.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- It has clear and understood arrangements for the security, storage and transfer of personal data.
- Data subjects have rights of access and there are clear procedures for this to be obtained.
- There are clear and understood policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from information risk incidents.
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- 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.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected.
- the device must be password protected.
- the device must offer approved virus and malware checking software.

- the data must be securely deleted from the device, once it has been transferred or its use is complete.

12.0 Handling E-Safety complaints and misuse

- Complaints of Internet misuse by children will be dealt with by a senior member of staff.
- Staff will be trained so they are able to deal with E-Safety incidents. They must log incidents reported to them (that have occurred in school or out of school) using an incident log stored in the Headteacher's office. These will be monitored by the school's Designated Safeguarding Leader and discussed in the termly Online Safety meetings.
- Pupils and parents will be informed of the consequences of internet and digital technology misuse.
- Any complaint about staff misuse must be referred to the Headteacher and will be dealt with through the Governing body complaints procedure if required.
- Complaints of a child protection nature must be referred to the Designated Safeguarding Lead (DSL) and dealt with in accordance with school child protection procedures.

13.0 Whole-School Responsibilities for Internet Safety

13.1 Headteacher

- Responsible for e-safety issues within the school but may delegate the day-to-day responsibility to a Senior Leader such as the Computing subject leader.
- Ensure that the Computing subject leader is given appropriate time, support and authority to carry out their duties effectively.
- Ensure that any developments at Local Authority level are communicated to the Computing subject leader.
- Ensure that the Governing Body is informed of e-safety issues and policies.

13.2 Online Safety/Computing Subject Leader

- Primary responsibility: establish and maintain a safe ICT learning environment
- Establish and maintain a school-wide e-safety programme
- Create and adapt, where necessary, an e-safety policy and procedures.
- Respond to e-safety policy breaches in an appropriate and consistent manner in line with protocols set out in policies, and maintain an incident log.
- Develop an understanding of relevant legislation and take responsibility for their professional development in this area.

13.3 Governing Body

- Support the Headteacher and/or designated e-safety co-ordinator in establishing and implementing policies, systems and procedures for ensuring a safe ICT learning environment.

- Ensure that appropriate funding is authorised for e-safety solutions, training and other activities as recommended by the Headteacher and/or designated e-safety/Computing coordinator.
- Promote e-safety to parents and provide any updates/changes on e-safety policies within the school.

13.4 Schools ICT support

- Provide a technical infrastructure to support e-safety practices.
- Ensure that appropriate processes and procedures are in place for responding to the discovery of illegal materials, or suspicion that such materials are, on the school's network (School's firewall systems).
- Develop an understanding of relevant legislation.
- Report network breaches of acceptable use of ICT facilities to the Headteacher and/or the Computing subject leader.
- Maintain a professional level of conduct in their personal use of technology, both within and outside school.
- Take responsibility for their professional development in this area.

13.5 Teaching and Support Staff

- Contribute to the development of e-safety policies.
- Adhere to acceptable use policies.
- Take responsibility for the security of data.
- Develop an awareness of e-safety issues, and how they relate to pupils in their care.
- Model good practice in using new and emerging technologies.
- Include E-safety regularly in the curriculum.
- Deal with E-Safety issues they become aware of.
- Maintain a professional level of conduct in their personal use of technology, both within and outside school.
- Take responsibility for their professional development in this area.

13.6 Wider School Community

- This group includes: non-teaching staff; volunteers; student teachers; other adults using school internet or other technologies.
- Contribute to the development of e-safety policies.
- Adhere to acceptable use policies.
- Take responsibility for the security of data.
- Develop an awareness of e-safety issues, and how they relate to pupils in their care.
- Model good practice in using new and emerging technologies.
- Know when and how to escalate e-safety issues.
- Maintain a professional level of conduct in their personal use of technology, both within and outside school.
- Take responsibility for their professional development in this area.

13.7 Parents and Carers

- Contribute to the development of E-Safety policies.

- Are encouraged to read acceptable use policies and encourage their children to adhere to them via eg. School newsletters, the School website and organised E-Safety Workshops for Parents.
- Must adhere to acceptable use policies when using the school internet.
- Are encouraged to discuss E-Safety issues with their children, support the school in its E-Safety approaches and reinforce appropriate behaviours at home.
- Are encouraged to take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Should model appropriate uses of new and emerging technologies.
- Are encouraged to liaise with the school if they suspect, or have identified, that their child is conducting risky behaviour online.
- Are encouraged to actively monitor their children's use of the internet, Apps, Games and age appropriate material via eg. School newsletters, the School website and organised E-Safety Workshops for Parents.

14.0 Communicating E-Safety

14.1 Communication of the E-Safety Policy to pupils

- Appropriate elements of the E-Safety Policy will be shared with pupils.
- E-safety rules will be posted in each room where a computer is used.
- Pupils will be informed that internet and usage will be monitored.
- E-Safety will be included in the curriculum and regularly revisited.

14.2 Communication of the E-Safety Policy to staff

- The E-Safety and Acceptable Use policies will be given to all new members of staff as part of the staff induction.
- The E-Safety and Acceptable Use policies will be signed by all staff and discussed with them at least annually.
- Staff will be informed that internet and usage will be monitored.

14.3 Communication of the E-Safety policy to parents/carers

- The policies will be available on the school website.
- The school website will include a list of E-Safety resources and information for parents to access.
- Parents will be asked to sign a Home-School Agreement when their children join the school. This will include Acceptable Use policies relating to the internet and other digital technologies.
- The school will communicate and publicise E-Safety issues to parents through the school newsletter, website and Workshops/parents meetings/individual meetings where necessary.
- Parents and carers will be reminded that they must not publish any images of or comments about performances and other school events on social media.

15.0 Evaluation and Review

This policy was written by the computing subject leader in conjunction with the revised orders of the National Curriculum and has the approval of staff and governors. It will be reviewed initially by the subject leader and ultimately by the whole staff every two years.

Written by: C. Boot