School Improvement and Curriculum Committee 25/03/15 – Approved
Governing Body Ratification 13/05/15

E-Safety Policy

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles that connect to the Internet on a daily basis. The purpose of Internet use at Walnuts School is to raise educational standards, to promote pupil achievement and facilitate social and leisure opportunities. The internet also supports the professional work of staff and enhances the school's communication and management functions. Internet use is part of the statutory curriculum and is a necessary tool for learning. The exchange of ideas, social interaction, leisure activities and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger. This is particularly true of those who have difficulty with communication and social interaction. E-Safety encompasses not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology. E-safety is covered in the Milton Keynes Model Child Protection Policy for Schools.

EU kids online have produced useful grids analysing risk and opportunity of internet use which it is valuable for all members of the school community to mindful of, these grids will be displayed in ICT suites and on staff information boards.

Benefits	**Education and Learning**	**Participation and civic engagement**	**Creativity**	**Identity and social connection**
Content (What is found on the web) "Child as recipient"	Educational resources	Global information	Diversity of resources	Advice (personal/ health/ sexual etc)
Contact (Someone else making contact) "Child as participant"	Contact with others who share one's interests	Exchange among interest groups	Being invited or inspired to participate in creative processes	Social networking, shared experiences with distant others
Conduct (Child contacts someone) "Child as actor"	Self-initiated and collaborative forms of learning and education	Concrete forms of civic engagement	User-generated content creation	Expression of identity

Risks	Commercial	Aggressive	Sexual	Values
Content (What is found on the web) "Child as recipient"	Advertising, exploitation of personal information	Violent web content	Problematic sexual web content	Biased information, racism, blasphemy, health "advice"
Contact (Someone else making contact) "Child as participant"	More sophisticated exploitation, children being tracked by advertising	Being harassed, stalked, bullied	Being groomed, arranging for offline contacts	Being supplied with misinformation
Conduct (Child contacts someone) "Child as actor"	Illegal downloads, sending offensive messages to peers	Cyberbullying someone else, happy slapping	Publishing porn	Providing misinformation

[Table developed by the EUKids Online project and referenced in paragraph 1.3 of the Byron Review]

The School e-Safety Coordinators are:

Eleanor Attridge (Hazeley)/Rachel Cross (Infants).

Policy approved by Head Teacher:

Nick Jackman Date: .....

Policy approved by Governing Body:

Carol Head (Chair of Governors) Date: .....

The date for the next policy review is March 2015

E-Safety Policy

Teaching and Learning

Pupils at the Walnuts School may be particularly vulnerable to risks when using the internet technology due to poor social understanding and therefore must be taught explicit and unambiguous rules and reminders of how to keep safe online.

- 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, particularly as part of the PHSE programme.
- E-safety will also be taught explicitly at least once a year as part of the ICT curriculum, using a range of materials and approaches appropriate to the age, need and ability of the students.
- Safe and responsible use of the Internet and technology in school, home and the community, will be reinforced across the curriculum.
- Pupils may only use approved e-mail accounts for school purposes.
- Pupils will be involved in designing the pupils' acceptable use policy and e-safety rules and where appropriate, students should be expected to sign the policy (appendix 1). Where this document is not fully understood by pupils parents will be asked to read and sign on their behalf (appendix 2).
- Pupils should be under staff supervision appropriate to their need when using the Internet.

Staff

- All staff will read and sign the School Acceptable Use Policy before using any school ICT resources (appendix 3).
- All teachers will complete the 'Keeping Children Safe Online' online training materials from the NSPCC.
- The e-safety officers will additionally attend accredited e-safety training.
- Staff will only use official school email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team.
- Images of a pupil should not be used without reference to the Photo policy.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. – Please refer to the Data Protection Policy.
- The security of the school information systems and users will be reviewed regularly.

Incident Procedures

- 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 possible to guarantee that access to unsuitable material will

never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use

- The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- Any breaches in e-safety must be reported to one of the two named e-safety coordinators via email – any offensive emails that have been received should not be deleted (or accessed) as they constitute evidence that may later be required if the incident is of a serious nature.
- The e-Safety coordinators will record any incident in the School e-Safety incident log and in any other relevant areas e.g. Bullying or Child Protection log.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Police or Child Exploitation and Online Protection Centre
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list, via the E2bn.
- The Designated Child Protection Coordinator will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Area Children's Officer or the County e-Safety Officer.
- The school will manage e-Safety incidents in accordance with the school discipline/ behaviour policy where appropriate.
- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Any complaint about staff misuse will be referred to the head teacher.
- Cyber bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.

Parental Engagement

The Walnuts school will offer parents information to support them to plan appropriate supervised use of the internet at home and educate them about the risks and benefits to their child.

- The e-safety guidance will be shared with parents.
- Parents will be requested to read and sign acceptable use policy with their child where appropriate.
- Advice on useful resources and websites will be made available to parents.

E-Safety Contacts and References

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

Childline: www.childline.org.uk

Childnet: www.childnet.com

Internet Watch Foundation (IWF): www.iwf.org.uk

Think U Know website: www.thinkuknow.co.uk

EU kids online report- http://eprints.lse.ac.uk/24368/1/D3.2_Report-Cross_national_comparisons-2nd-edition.pdf

Byron report –

Safer Children in a Digital World - The Report of the Byron Review
http://www.cybersentinel.co.uk/media_documents/Byron%20Report.pdf

The Walnuts School

Pupil Acceptable Use Agreement

E-Safety Rules

In the modern world there are many useful, fun and interesting resources available online. At school we know that the internet provides educational activities which are of great benefit to the children and teenagers. However there are potential risks of using the online world as we do not always know who we are talking to and if they are being kind and truthful towards us. These risks include but are not limited to, access to inappropriate content, contact from strangers and inappropriate or illegal behaviours such as cyberbullying. We would like you to read and sign these rules and think about how you keep yourself safe when using the internet and other technology.

1. I will only use ICT in school for school purposes.
2. I will only use my own school email address when emailing.
3. I will only open email attachments from people I know, or who my teacher has approved.
4. I will not tell other people my passwords.
5. I will only open/delete my own files.
6. I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
7. I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher or parents immediately.
8. I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
9. I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
10. I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my E - Safety.

Name _____ **Class** _____

Signed _____ **Date** _____

Pupil ICT Acceptable Use Agreement (Parent)

Internet use is part of the statutory curriculum and is a necessary tool for learning. The exchange of ideas, social interaction, leisure activities and learning opportunities available are greatly beneficial to all, but can occasionally place children, young people and adults in danger. This is particularly true of those who have difficulty with communication and social interaction. E-Safety encompasses not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology.

The Walnuts School recognises the importance of ICT in education and the needs of pupils to access the computing facilities available within the School. To protect your child and the resources of the school we ask that all parents sign a copy of this 'Acceptable Use Policy' before children and young people use the School's ICT facilities, discussing where appropriate the acceptable use of technology with your child.

Please read this document carefully and sign and date it in order to indicate your acceptance of the Policy on your child's behalf and your permission for them to use these facilities.

- **Children and young people look after all equipment to the best of their ability;**

This includes, making sure that there is no damage to hardware or changes to software. We understand that many young people at the Walnuts are highly ICT literate however it is unacceptable for software changes to be made e.g. downloading games to the network without permission from the ICT technician as these may pose a risk to our network.

- **Printers are available across the network**

Printers are provided across The Walnuts School for use by pupils. Pupils will be encouraged to only print a single copy of a document. They will also be encouraged not to print documents that are unnecessary or offensive. Excessive printing or printing of offensive materials may result in printer credits being temporarily suspended from your child's login. This would be clearly discussed with yourself and your child if necessary.

- **The Internet**

The internet is a rich source of information and provides educational activities which are of great benefit to the children. However there are potential risks due to the interconnected nature of the internet, these include but are not limited to, access to inappropriate content, contact from strangers and inappropriate or illegal behaviours of children such as cyberbullying or illegally downloading materials. For more information please visit https://www.thinkuknow.co.uk/parents/

To protect your child in school The Walnuts provides several layers of internet filtering, including the filtering services provided by the E2bN schools broadband which are designed remove controversial, offensive or illegal material that would cause your child to be upset. However despite this the constantly changing nature of the internet means that we cannot guarantee that no inappropriate materials will pass the filter. To additionally protect children at the Walnuts access to the Internet is supervised by adults and e-safety is taught

throughout the school in a range of ways. E-safety lessons will include the way children present themselves online and they will be expected to act in a way that is safe and respectful of themselves, their friends and the wider school community in all their activity on the internet including social networking. For reasons of safety and security your child should not use his/her mobile phone, social networking or any other technology in a way that is likely to damage the reputation of the school or risk the welfare of other pupils or adults that work within the school.

Social Contact

Where we encourage children and young people at the Walnuts to have social contact outside of school this must be done in an appropriate and respectful way. Any acts of cyberbullying will be dealt with in accordance with the schools behaviour policy. If inappropriate material is sent to a pupil, it please reported to your child's Head of Department. Appropriate communication with members of staff within the school is via their school provided email address or phone numbers that are provided by the school. It is not appropriate for members of staff to have social networking communication with pupils.

Systems

Whilst every effort is made to ensure that the systems, both hardware and software are working correctly, the school will not be responsible for any damages or loss incurred as a result of system faults, malfunctions or routine maintenance. These damages include loss of data as a result of delay, non-deliveries, mis-deliveries or service interruptions caused by the system or elements of the system, or your errors or omissions.

- -

Required Signature

PARENTS / CARERS

I have read this Acceptable Use Policy and I have discussed this with my child.

I agree for my child _____ Class _____

to use the Internet and related technologies in accordance with the school guidelines.

Signed _____ Parent/Carer

Signed _____Pupil

Date: _____

Please return this slip to The Walnuts School.

Staff ICT Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

- I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, PDAs, digital cameras, email and social media sites.

- School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

- I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

- I will respect system security and I will not disclose any password or security information. I will use a 'strong' password.

- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the ICT technician.

- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1988. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or

accessed remotely. Any images or videos of pupils will only be used as stated in the school image use policy and will always take into account parental consent.

- I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones). I will protect the devices in my care from unapproved access or theft.

- I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.

- I will respect copyright and intellectual property rights.

- I have read and understood the school e-Safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces

- I will report all incidents of concern regarding children's online safety to the Designated Child Protection Coordinator (Nick Jackman) and/or the e-Safety Coordinator (Eleanor Attridge – Hazeley/Rachel Cross – Infants) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the e-Safety Coordinator.

- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this to the ICT technician (Steven Bell) as soon as possible.

- My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team.

- My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the school AUP and the Law.

- I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the County Council, into disrepute.

- I will promote e-Safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

- If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the e-Safety Coordinator (Rachel Cross) or a member of the Senior Management Team.

- I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agreed to comply with the Staff ICT Acceptable Use Policy.

Signed:..... Date: .....

Print Name: .....

Accepted by:..... Print Name: .....