West Earlham Infant and Nursery School
Online Safety policy

1. At West Earlham Infant and Nursery school we acknowledge the positive impact and educational benefits that can be achieved through appropriate use of the Internet and associated communications technologies. We are also aware that inappropriate or misguided use can expose both adults and young people to unacceptable risks and dangers. Therefore, we aim to educate pupils about the benefits and risks of using technology and provide safeguards and awareness for users to enable them to control their online experience.

2. The purpose of this policy is to:

a. Set out the key principles expected of all members of the school community at West Earlham Infant and Nursery school with respect to the use of technologies.

b. Safeguard and protect the children and staff.

c. Assist school staff working with children to work safely and responsibly with technologies and to monitor their own standards and practice.

d. Set clear expectations of behaviour and/or codes of practice relevant to responsible use of technologies for educational, personal or recreational use for the whole school community.

e. Have clear structures to deal with online abuse such as online bullying

f. Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

g. Minimise the risk of misplaced or malicious allegations made against adults who work with students.

3. The main areas of risk for our school community can be summarised as follows:

a. Content
- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

b. Contact
- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

c. Conduct
- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

4. Scope

This policy applies to all members of West Earham Infant and Nursery School community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school technologies, both in and out of West Earlham Infant and Nursery School

5. Communication

The policy will be communicated to staff/pupils/community in the following ways:

a. Policy to be posted on the school website

b. Policy to be part of school induction pack for new staff, including information and guidance where appropriate

c. All staff must read and sign the 'Staff Digital Code of Conduct' before using any school technology resource

d. Regular updates and training on online safety for all staff, including any revisions to the policy

6. Handling Concerns

a. The school will take all reasonable precautions to ensure online safety is in line with current guidance from the Department for Education (DfE)
b. Staff and pupils are given information about infringements in use and possible sanctions.
c. Designated Safeguarding Lead (DSL) acts as first point of contact for any safeguarding incident whether involving technologies or not
d. Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the concern is referred to the Chair of Governors

7. Pupil online safety curriculum

This school:

a. has a clear, progressive online safety education programme as part of the Computing curriculum/PSHE and other curriculum areas as relevant. This covers a range of skills and behaviours appropriate to their age and experience
b. ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright
c. ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights

Assessing risks

a. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor LEA can accept liability for the material accessed, or any consequences of internet access.
b. The school will audit computing provision to establish if the online safety policy is adequate and that its implementation is effective.

8. Staff and governor training

This school:

a. makes regular up to date training available to staff on online safety issues and the school's online safety education program
b. provides, as part of the induction process, all staff [including those on university/college placement and work experience] with information and guidance on the Online Safety Policy.

9. Parent/Carer awareness and training

This school:

a. provides information for parents/carers for online safety on the school social media pages, website and in newsletters
b. runs a rolling programme of online safety advice, guidance and training for parents
c. parents/carers are issued with up to date guidance on an annual basis

10. Incident management

In this school:

a. there is strict monitoring and application of the online safety policy, including the ICT Code of Conduct and a differentiated and appropriate range of sanctions
b. support is actively sought from other agencies as needed (i.e. the local authority, UK Safer Internet Centre helpline, CEOP, Police, Internet Watch Foundation) in dealing with online safety issues
c. monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school
d. parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible
e. the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law
f. we will immediately refer any suspected illegal material to the appropriate authorities – i.e. Police, Internet Watch Foundation and inform the LA
g. And incidents will be recorded

11. Internet access, security and filtering

a. In this school we follow guidelines issued by the Department for Education to ensure that we comply with minimum requirements for filtered broadband provision
b. Pupils in key stage 1 will not have individual logins and class logins will be used instead.

12. Information system security

a. School computing systems capacity and security will be reviewed regularly in consultation with NetCentral who manage our online systems.
b. Virus protection is refreshed every 4 hours through the school's server.

13. Social networking and personal publishing

a. The school will filter access to social networking sites.
b. Pupils will be advised never to give out personal details of any kind that will identify them or their location.

14. Managing filtering

a. The school will work with the Local Authority, DFE and the Internet Service Provider to ensure that systems to protect pupils are reviewed and improved.
b. If the staff or pupils discover an unsuitable site, it will be reported to the computing co-ordinator who is responsible for online safety or the designated safeguarding lead where appropriate.
c. The computing co-ordinator will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

15. E-mail

a. This school

I. Provides staff with an email account for their professional use, e.g. nsix.org.uk and makes clear personal email should be through a separate account
II. We use anonymous e-mail addresses, for example head@, office@
III. Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
IV. Will ensure that email accounts are maintained and up to date

b. Pupils email:

I. We use school provisioned pupil email accounts that can be audited
II. Pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home.

c. Staff email:

I. Staff will use LA or school provisioned e-mail systems for professional purposes
II. Never use email to transfer staff or pupil personal data unless it is protected with secure encryption. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.
III. Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. Use of teacher laptops at home is the teacher's responsibility and must be used appropriately.

16. School website

- The school web site complies with statutory DfE requirements
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- Photographs of pupils published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;

17. Digital images and video

In this school:

a. We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school (or annually)

b. We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs
c. Staff sign the school's Digital Code of Conduct/AUP and this includes a clause on the use of personal mobile phones/personal equipment

18. Removable controls and home working

a. The school will encrypt all school-owned devices for personal use, such as laptops and tablets, to ensure that they are password protected. If any portable devices are lost, this will prevent unauthorised access to personal data.
b. Pupils and staff are not permitted to use their personal devices where the school shall provide alternatives, such as work laptops unless instructed otherwise by the head teacher
c. The Wi-Fi network at the school will be password protected and will only be given out as required. Staff and pupils are not permitted to use the Wi-Fi for their personal devices, such as mobile phones or tablets, unless instructed otherwise.

19. Protecting personal data

a. Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations Act 2018. *(Refer to General Data Protection Regulations Policy)*

Further related Policies:

- Computing Policy
- General Data Protection Regulations Policy
- Safe Use of Images Policy
- Social Media Policy
- Anti-Bullying Policy
- Behaviour Policy
- Safeguarding children incorporating Child Protection Policy
- Safer Recruitment Policy

Approval

This policy has been reviewed in line with the 2010 Equality Act and Public Sector Equality Act. Due regard has been given to Equality.

This policy will be adopted in ***February 2019***. The date of the next formal review will be ***February 2020*** and every year thereafter, unless statutory legislation changes.

Policy approved by the Head Teacher of West Earlham Infant and Nursery School.