OAKWOOD JUNIOR SCHOOL

E-Safety Policy

Review Date	Autumn 2016		
Reviewed By	Deputy Head and ICT coordinator		
Review Cycle	2 years		
Next Review Date	Autumn 2018		

Signed …….

Name ……

on behalf of the Governing Body of Oakwood Junior School

E-Safety Roles and Responsibilities

The Head and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named E-Safety co-ordinator in this school is Nicola Fray.

Senior Management and Governors are updated by the Head / E-Safety co-ordinator and all Governors are encouraged to keep an up-to-date understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, Governors, visitors and pupils is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, behaviour and discipline, anti-bullying and PSHE and to the July 2015 DfE Keeping Children Safe in Education Document:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/447595/KCSIE_July_2015.pdf

E-Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for E-Safety guidance to be given to the pupils on a regular and meaningful basis. E-Safety is embedded within our curriculum and we continually look for new opportunities to promote E-Safety.

The school has a framework for teaching internet skills in computing lessons.

The school provides opportunities within assembles, computing lessons and PSHE to teach about E-Safety.

Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the E-Safety curriculum.

Pupils are aware through the teaching of the computing units that rules which may limit what they want to do are actually there to protect them.

Pupils are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modelling and appropriate activities.

Pupils are aware of the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying.

Pupils are taught to critically evaluate materials and learn good searching skills through cross-curricular teacher models, discussions and via the computing curriculum.

E-Safety Skills Development for Staff

New staff receive information on the school's acceptable use policy as part of their induction.

All staff are made aware of their individual responsibilities relating to the safeguarding of children within the context of E-Safety.

All staff are encouraged to incorporate E-Safety activities and awareness within computing and PSHE lessons and ensure they are adequately informed with up-to-date areas of concern.

Incident Reporting, E-Safety Incident Log & Infringements

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's relevant responsible person or E-Safety Co-ordinator.

See Appendix 1: Incident Log (kept with Nicola Fray)

Misuse and Infringements

Complaints

Complaints and / or issues relating to E-Safety should be made to the E-Safety Co-ordinator or Headteacher. Incidents should be logged and the 'Flowcharts for Managing an E-Safety Incident' should be followed.

Inappropriate Material

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the relevant responsible person and an investigation by the Headteacher or other outside agencies. Depending on the seriousness of the offence, sanctions could include immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

See appendices 2, 3 and 4: Flowcharts (kept with Nicola Fray)

Internet Access

The internet is an open worldwide communication medium, available to everyone, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

Managing the Internet

The school provides pupils with supervised access to Internet resources (where reasonable) through the school's internet connectivity.

Staff will preview any recommended sites, online services, software and apps before use.

Searching for images through open search engines is discouraged when working with pupils.

If Internet research is set for homework, specific sites will be available on the homepage that have previously been checked by the teacher.

All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.

All users must observe copyright of materials from electronic resources.

Internet Use

Users must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience.

Users must not reveal names of colleagues, pupils or any other confidential information acquired through their job on any social networking site or other online application.

On-line gambling or gaming is not allowed.

It is at the Headteacher's discretion as to what internet activities are permissible for staff and pupils and how this is disseminated. For further detail, see the 'Acceptable Use Policy for Staff and Visitors' and the 'Acceptable Use Policy for Pupils'.

Infrastructure

The school is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.

Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.

If pupils discover an unsuitable site, the screen must be switched off/ concealed using the Hector Program and the incident reported immediately to the teacher.

It is the responsibility of the school to ensure that anti-virus protection is installed and kept up-to-date on all school machines.

Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility nor the ICT technician's to install or maintain virus protection on personal systems. If pupils wish to bring in work on removable media it must be given to the technician/teacher for a safety check first.

Pupils and staff are not permitted to download programs or files on school-based technologies without seeking prior permission from the ICT technician.

If there are any issues related to viruses or anti-virus software, the ICT technician should be informed.

Managing Other Online Technologies

Online technologies, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

The school denies access to social networking and online games websites to pupils within school.

Pupils are discouraged, through E-Safety teaching and discussions, from using social media websites outside of school and reminded that they should always adhere to the age restrictions.

All pupils are advised to be cautious about the information given by others on such websites, for example users not being who they say they are.

Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.

Pupils are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).

Pupils are encouraged to be wary about publishing specific and detailed private thoughts and information online.

Pupils are asked to report any incidents of cyberbullying or images / texts which make them feel uncomfortable to an adult in school.

Staff may only create blogs, wikis or other online areas in order to communicate with pupils using the school learning platform or other systems approved by the Headteacher.

When signing up to online services that require the uploading of data which could be deemed as personal or sensitive, schools should check terms and conditions regarding the location of storage.

Parental Involvement

Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school.

Parents/carers are asked to contact the school should they not wish to give consent to images of their child being taken and used in the public domain (e.g., on school website).

Parents / carers are invited to E-Safety workshops in school led by the NSPCC.

Parents / carers are given links via our school newsletter to useful E-Safety websites.

Parents/carers are expected to sign the 'Acceptable Use Policy for Pupils'

on behalf of and in discussion with their child.