E SAFETY POLICY

This Policy should also be read in conjunction with any relevant Trust documentation/policies. Please ask if you need further information.

This policy applies to all people using school equipment. This includes teaching staff, administration staff, ancillary staff, site managers, students, pupils, parents and visitors. Wordsworth Primary School will ensure that every person to whom this policy applies is aware of its contents.

When staff, pupils etc leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment. Parents will be requested to sign an e–Safety/internet agreement as part of the Home School Agreement. Any e-Safety issues or concerns will be taken to the ICT co-ordinator, Head teacher or the designated Child Protection Coordinator.

Wordsworth Primary School aims to foster an e-safe culture in which issues of e-safety are discussed openly and honestly. We alert our users of potential risks and we encourage the children to develop their own sets of safe and responsible behaviour through computing and ICT sessions, circle times and by demonstrating positive behaviour both inside and outside school. We appreciate that e-safety is primarily a safeguarding issue for which all staff are responsible.

Teaching and Learning

Why the Internet and digital communications are important

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems. Access to the Internet is a necessary tool for staff and an entitlement for pupils to give them experience of developments in Technology in the world around them.

Benefits of using the Internet in education include:

- Access to world-wide educational resources including museums and art galleries
- Inclusion in government initiatives
- Educational and cultural exchanges between pupils world-wide
- Access to experts in many fields for pupils and staff
- Professional development for staff through access to national developments educational materials and effective curriculum practice
- Collaboration across networks of schools, support services and professional associations
- Access to learning wherever and whenever convenient
- Exchange of curriculum and administration data with SCC and DCSF
- Provide opportunities for publishing and displaying work on a school web page

The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.

How Internet use enhances learning

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use

- Staff should guide pupils to on-line activities that will support the learning outcomes planned for the pupils' age and maturity and educate them in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation, at an age appropriate level
- Internet access will be planned to enrich and extend learning activities.
- Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- The school's internet access will be designed expressly for pupil use and will include filtering appropriate to the age of the pupils

How will pupils learn how to evaluate Internet content?

- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of on-line materials is a part of teaching/learning in every subject.
- If staff or pupils discover unsuitable sites, the URL(address), time, date and content must be reported to the ICT co-ordinator to pass on to the internal IT technician and where appropriate to the school's safeguarding officer.

Managing Internet Access

Information system security

- Virus protection will be updated regularly.
- The security of the school information systems and users will be reviewed regularly.
- The ICT co-ordinator / network manager will review system security regularly.
- The school uses Broadband with its firewall and filters.

E-mail

- Pupils may only use approved e-mail accounts on the school system
- Pupils may send e-mail as part of planned lessons where whole-class or group e-mail addresses set up by the ICT Manager or Technician will be used. Pupils will not be given individual e-mail accounts
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission from an adult.
- In-coming e-mail should be treated as suspicious and attachments not opened unless the author is known
- Formal e-mails sent to an external organisation should be written carefully and where staff deem appropriate a senior member of staff should be copied in.
- The forwarding of chain messages is not permitted.

Published content and the school's website

The contact details on the website should be the school address, office, email and telephone number. Staff or pupils' personal information must not be published. .

Publishing pupil's images and work

- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images of pupils are electronically published outside of the schools intra net.

Social Networking, Social Media and Personal Publishing

- The schools will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- The school has an expectation that use of any social networking sites (e.g. Facebook, Twitter, Myspace) by staff does not bring the name of the school or any of its staff into disrepute. All staff are advised to set security and privacy filters on such sites appropriately to avoid making private details public. Staff should not accept contact from pupils via social networking sites. It is worth remembering that a pupil remains as such until the age of 18.

Managing filtering

- If staff or pupils discover unsuitable sites, the URL must be reported to the IT Coordinator.
- Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP.
- The school's broadband access will include filtering appropriate to the age and maturity of pupils.

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.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Staff internet responsibilities

- A member of staff who flouts security advice, or uses email or the Internet for inappropriate reasons risks dismissal.
- Staff will not use any personal technology to take images of children.

Policy Decisions

Authorising internet access

- At Key Stage 1, and during the Early Years Foundation Stage, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- At Key Stage 2 access to the internet will be more frequent, but will be more supervised by the class teacher.
- All staff, administration staff, ancillary staff, site managers, students, parents and visitors must read and sign the "E safety policy" before using any school ICT resources.

Community use of the Internet

- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

Management of Cyber bullying

- Cyber bullying (along with all forms of bullying) will not be tolerated in school. Cyber bullying will be dealt with in accordance to the Behaviour Policy.
- All incidents of cyber bullying reported to the school will be recorded.

Below, we have identified a number of e-safety risks and issues. We aim to avoid these risks and achieve e-safety for our children and staff in three ways. Firstly, through effective policy and practice outlined in this document (including the Social Networking Policy and E Safety home school agreement). Secondly, by a secure and reliable technical infrastructure, and thirdly, through education and training for all ICT users. Details of these are set out below.

E-Safety Risks and Issues

- The school will audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.
- 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. Neither the school nor JET can accept liability for the material accessed, or any consequences resulting from Internet use.
- The use of the computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

We have identified the following examples of risks and issues which may arise to threaten the e-safety of our children and staff:

Content

- Exposure to age-inappropriate material
- Exposure to inaccurate or misleading information
- Exposure to socially unacceptable material such as that inciting violence, hate or intolerance
- Exposure to inappropriate lifestyle material, such as that including pro-anorexia, self-harm etc.
- Exposure to illegal material, such as images of child abuse
- Downloading of copyrighted materials, e.g. music and films
- Plagiarism

Contact

- Grooming using ICT, leading to sexual assault and/or child prostitution
- Grooming using ICT, leading to extremism, terrorism or the support of terrorism (PREVENT 2015)
- Bullies using ICT (e-mail, mobile phones, chat rooms etc.) as a way to torment their victims
- Children and young people self-publishing information – sometimes inappropriate – about themselves and therefore putting themselves at risk

Commerce

- Exposure to inappropriate commercial advertising
- Exposure to online gambling services
- Commercial and financial scams

Infrastructure and Network Practice

Within Jefferys Education Trust, firewall and virus protection are provided for all computers and iPads connected to the school's network. Our anti-viral software is checked by our ICT technician and is regularly updated on all machines to maintain protection.

Filtering and content control is similarly provided by Jefferys Education Trust for all computers and iPads connected to the city network using Smoothwall. This uses a nationally approved database of keywords and URLs which it filters. If concerns are raised about particular keywords and URLs, these can be forwarded to our ICT Technician via the school emailing facility.

This technical infrastructure is further secured by good network practice by all users. This includes the following safeguarding procedures:

- Each member of staff has their own personal log-in and password
- Passwords should be strong (a minimum of 7 characters including both numbers and characters) and changed on a regular basis
- Unattended workstations should be logged off/locked
- All removable media and e-mail attachments must be virus checked before being used/viewed on the network

Education and Training

All members of staff are aware of the need for good network practice and have read and agreed to the school's E Safety and Social Networking Policies. All staff will take part in annual training sessions regarding e-safety as required and the e-safety coordinator will keep staff informed of new developments. Staff are fully informed as to how they should respond to e-safety incidents as outlined below.

All children must agree to an e-safety contract which consists of the following statements:

- I will not bring any USB sticks, digital cameras or memory devices into school and use them without permission.
- I will tell a teacher straight away if I see anything on the internet I am not happy with or worried about or if I receive a message I am not happy with.
- I will only use internet sites my teacher approves and only use the internet with permission.
- I will not use internet chat rooms or give away any personal information over the internet.
- I will only send and open emails to and from people I know, or who my teacher has approved. All messages I send will be polite, kind, sensible and considerate.
- I understand that the school can check my files and the internet sites I visit and any irresponsible use may result in loss of network or internet access.
- If I am in Year 6 and need to bring a mobile phone into school for safety reasons, I will hand it straight in to my teacher at the beginning of the day and collect it at the end of the day.
- I agree that I will use all ICT resources in a responsible way at all times.
- I know that network and internet access may be monitored and that irresponsible use may result in the loss of network or internet access.

All parents must agree to an e safety contract also which consists of the following:

- I agree to support the school by encouraging my child to follow the E safety rules and will talk to my child about safe use of ICT when appropriate.
- I agree that I will not use my mobile phone in the school building.
- I agree not to use my mobile phone or any other camera to take photographs, unless it is a special occasion such as Christmas Performances or Sports Day and I have permission. In this instance I

agree they will be for my own private use and I will not publish any such photos on any website/ social networking site.

Each year group will learn about the risks and issues surrounding e-safety in an age-appropriate way. They will take part in lessons and circle times where e-safety in the key focus. Teachers will deliver e-safety lessons in accordance with the scheme of work.

All of the school's computers are in public areas and the ICT suite is open access to ensure a staff member can easily monitor use at all times. Any tablets or iPads are also only used under close supervision. Unsupervised access to the internet is not allowed.

Due to the strong emphasis on home access to the internet as well as increased use made of electronic communication, we recognise that parents must be made aware of the importance of e-safety. Parents are encouraged to discuss the e-safety contract with their children before signing and enforce those rules which apply at home as well as in school. Through our annual workshop, parents are made aware of agencies and websites which they may find useful when learning about e-safety or in tackling the issue with their children.

Children should not bring mobile phones into school unless agreed by the head teacher for valid reasons. This is to prevent the possibility of pupils' access to internet sites that may be unsafe. If they are granted permission to have a mobile phone in school it needs to be handed in to the teacher on arrival.

Responding to E-safety Incidents

Responses to e-safety incidents will differ depending on

1. The severity of the incident and
2. The person or persons concerned (staff member, child or parent).

Minor incidents involving misuse of ICT by pupils should be closely monitored, such as an incident such as using another child's login and password. The class teacher or e-safety coordinator should react proactively to any emerging trends. In the first instance, the pupil will receive a verbal warning and the incident will be documented. Further infractions will be recorded, parents may be notified and other appropriate action may be taken.

Online content is filtered by Jefferys Education Trust's Smoothwall. However, such software is never 100% effective. There remains a small possibility that children may inadvertently or deliberately have access to age-inappropriate materials. All children understand that when such e-safety incidents occur, they must immediately seek help from a trusted adult. It will be a disciplinary matter if a child has deliberately accessed, printed or shared such inappropriate material. The child's parents will be contacted and access to the internet may be restricted. The e-safety coordinator will monitor and keep a record of such incidents. Some records will be kept in our safeguarding file. Where incidents are reported to individual teachers, teachers should take immediate steps to ensure that the content cannot be viewed by other children. This may include closing a laptop or switching off a monitor. As soon as possible, the URL must be recorded and passed to the e-safety coordinator to be reported to the ICT Technician.

In the event of a serious incident occurring in school, including the discovery of illegal or indecent material, the police will be contacted. The computer(s) concerned should remain untouched until advised by the police.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with under the School's Complaints Procedure.
- Any complaint about staff misuse must be referred to the Headteacher.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary and child protection procedures.
- All e–Safety complaints and incidents will be recorded by the school — including any actions taken.

How will the policy be introduced to pupils?

- All users will be informed that network and Internet use will be monitored.
- A review of E safety Education will take place annually.

How will the policy be discussed with staff?

- The e–Safety Policy will be formally provided to and discussed with all members of staff.
  Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

How will parents' support be enlisted?

- Parents' attention will be drawn to the School e–Safety Policy in newsletters, the school brochure and on the school website. Parents will be asked to sign the E safety rules and talk through them with their children.

Policy written: November 2015

Review Due: November 2016