



## **THE WHARTONS PRIMARY SCHOOL** **(Excellence, Enjoyment and Achievement for All)**

### **SAFEGUARDING – ONLINE SAFETY POLICY**

#### **Rationale**

- In recognising the essential role of ICT in supporting learning, school improvement and school organisation, it is imperative that we also recognise the inherent safety issues that need to be planned for and managed through a measured and strategic approach.
- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- The evolving nature of current and emerging technologies will necessitate the development of online safety as a core principle within our ICT strategy.

#### **What is online safety?**

Online safety encompasses Internet technologies and electronic communications such as mobile phones, laptops, tablets and PC's as well as collaboration tools, personal publishing and social networking applications. It highlights the need to educate pupils about the benefits and risks of using this technology and provides safeguards and awareness for users to enable them to control their online experience. The use of new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content,
- Unauthorised access to / loss of / sharing of personal information,
- Child Sexual Exploitation and the risk of being subject to grooming by those with whom they make contact on the internet,
- The sharing / distribution of personal images without an individual's consent or knowledge,
- Inappropriate communication / contact with others, including strangers,
- Online bullying,
- Access to unsuitable video / internet games,
- An inability to evaluate the quality, accuracy and relevance of information on the internet,
- Plagiarism and copyright infringement,
- Illegal downloading of music or video files,
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this online safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

#### **Aim of this online safety policy**

- To support pupils to develop effective learning habits and skills within an online safe environment,
- To ensure that pupils develop a strong awareness of the type of dangers that exist when using technology,

- To ensure that pupils develop a strong awareness of the type of dangers associated with internet and email linked technologies
- To ensure that adults in our school community, including staff, parents, governors and other stakeholders develop a strong awareness of the type of dangers associated with internet and email linked technologies
- This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

#### **The Governors:**

- Are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy.
- Receive regular information about online safety incidents and monitoring reports.
- Have appointed a member of the Governing Body to take on the role of 'Child Protection Governor'. This governor will be responsible for matters relating to online safety.

#### **The Child Protection Governor:**

- Has regular meetings with the Head teacher/Deputy Head/ICT Leader
- Regularly monitors the school Online safety incident logs
- Reports to the relevant Governors committee.

#### **The Head teacher:**

- Is responsible for ensuring the safety (including online safety) of members of the school community
- Is responsible for ensuring that the ICT Leader and other relevant staff receive suitable CPD to enable them to carry out their online safety roles
- Is aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of the school community
- Will liaise with the Local Authority regarding any serious online safety concerns.

#### **The Computing/Online Safety Leader:**

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies,
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place,
- Provides training and advice for staff,
- Liaises with the Local Authority,
- Receives details of any online safety incidents and creates a log of incidents to inform future online safety developments,
- Meets regularly with online safety Governor to discuss current issues and review incident logs,
- Reports to Senior Leadership Team/Governors

#### **The ICT Technician:**

- Ensures that the school's ICT infrastructure is secure and is not open to misuse or malicious attack,
- Ensures that the school meets the online safety technical requirements and Local Authority online safety policies and guidance

- Ensures that staff users can only access the school's networks through a properly enforced password protection policy
- Keeps up to date with online safety technical information in order to effectively carry out his online safety role and to inform and update others as relevant,
- Regularly monitors the use of the Network and school email accounts, in order that any misuse or attempted misuse can be reported to the Head teacher or online safety Leader for investigation / action / sanction,
- Implements and updates monitoring software and systems as agreed in school policies.

#### **The Class Teachers:**

- Have all read and signed the Acceptable Use Policy (see appendix), a copy of which is kept in their staff file,
- Have an up to date awareness of online safety matters and of the current school online safety policy and practices,
- Report any suspected misuse or problem to the Head teacher or online safety leader for investigation / action / sanction,
- Communicate with pupils on a professional level and only using official school systems,
- Embed online safety issues in all aspects of the curriculum and other school activities,
- Ensure that pupils understand and follow the school online safety policy and online safety agreements whilst in school,
- Ensure that pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations (age appropriate),
- Monitor ICT activity in lessons and extracurricular school activities,
- Are aware of online safety issues related to the use of mobile phones, cameras and hand held devices and implement current school policies with regard to these devices,
- Ensure that when using the Internet in school, pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in any internet searches.

#### **The Designated Teacher for Child Protection:**

Is trained in online safety issues and aware of the potential for serious child protection issues arising from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers and Child Sexual Exploitation
- Potential or actual incidents of grooming
- Online-bullying

#### **Other visitors to the school**

- All visitors are made aware of online safety issues related to the use of mobile phones, cameras and hand held devices and are required to follow school policies with regard to these devices
- Adults teaching in our school such as supply teachers and students are able to access the network using a generic visitor log in and password
- All regular members of staff are required to read and sign the staff Acceptable Use Policy.
- All visitors to the school are made aware of the child protection designated members of staff.

#### **The Role of the Pupil**

Pupils in our school are encouraged and supported to:

- Be responsible for using the school ICT systems in accordance with the Pupil Online Safety Agreements, which they are expected to sign to be given access to school systems. (NB. at KS1 parents / carers will sign on behalf of the pupils).
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations (age appropriate),
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so,
- Know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They also know and understand school policies related to online-bullying,
- Understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school if related to their membership of the school.

### **Online safety Education**

- A planned online safety programme is provided as part of our computing and PHSCE curriculum (through the use of 'Switched On Computing' and 'Jigsaw PSHE'. This is regularly revisited and covers the use of ICT and new technologies in and outside school,
- Key online safety messages are reinforced during assemblies, PHSCE lessons, whole school events, information evenings, school newsletters and school information screens,
- Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information (age appropriate),
- Pupils are helped to understand the need for the Pupil Online safety Agreements and are encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school,
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet (age appropriate),
- Rules for use of ICT and Internet are displayed throughout the school,
- Staff act as good role models in their use of ICT, the internet and mobile devices.

### **To secure effective achievement of these aims, the school...**

- The Head teacher and deputy head have strategic leadership; this role encompasses online safety in the context of procedures and infrastructures needed to minimise online safety risks and to deal with online safety issues that arise,
- The ICT leader has ICT Curriculum leadership; this role encompasses online safety in the context of the teaching and learning needed to develop pupils', staff and the wider school communities' awareness of how to recognise, understand and deal with online safety,
- Involves the relevant individuals and organisations when dealing with online safety awareness and issues
- Involves the relevant organisations at the earliest opportunity when responding to any suspected criminal activity/child protection issues,
- Has an online safety policy written by the school
- Accesses and delivers regular online safety staff training,
- Ensures that all new staff receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and the pupil online safety agreements,
- Manages School ICT systems in ways that ensure that the school meets the online safety technical requirements,
- Ensures that servers, wireless systems and cabling are securely located and physical access restricted
- Reviews this online safety policy and its implementation annually.

### Online bullying

- Online bullying can be defined as “the use of Information and Communications Technology (ICT), particularly mobile phones and the internet, to deliberately upset someone else. It can be an extension of face-to-face bullying, with technology providing the bully with another route to harass their target. However, it differs in several significant ways from other kinds of bullying: the invasion of home and personal space; the difficulty in controlling electronically circulated messages; the size of the audience; perceived anonymity; and even the profile of the person doing the bullying and their target.” (DCSF definition)
- Bullying (and this includes online bullying) is never acceptable. The school community has a duty to protect all its members and provide a safe, healthy environment. Education and discussion around the responsible use of technologies and online safety are key to preventing online bullying and helping pupils deal confidently with any problems that might arise, whether in or out of school. Technology can have a positive role in learning and teaching practice, and there is a need for staff to be confident about ICT and to respond to incidents of online bullying appropriately.
- Online bullying is included in our online safety education for all pupils,
- If an online bullying incident is identified, it is important that, as in other cases of bullying, sanctions are applied. Steps will be taken to change the attitude and behaviour of the bully, as well as ensuring access to any help that they may need. See our Anti bullying policy for more information.

### E-mail

- Staff may only use approved school e-mail accounts on the school system,
- Staff must immediately tell the Headteacher if they believe something may be wrong with their email account,
- Pupils must immediately tell a teacher if they receive an offensive e-mail,
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission,
- E-mails sent to an external organisation should be written carefully, in the same way as a letter

### Published content and the school website

- The contact details on the Website are the school address, e-mail and telephone number. Staff or pupils' personal information will not be published,
- The head teacher takes overall editorial responsibility and ensures that content is accurate and appropriate.

### Publishing pupil's images and work

- The school will allow staff to take digital / video images to support educational aims, but they must follow school policies concerning the sharing, distribution and publication of those images. Those images will only be taken on school equipment, **the personal equipment of staff will not be used for such purposes,**
- Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs,
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site,

### Social networking and personal publishing

- Pupils and staff are not permitted to use social networking sites in school and the network filters will block any attempts to do so,
- Pupils will be advised never to give out personal details of any kind on line which may identify them or their location,
- Pupils and parents are advised that the use of social network sites outside school is inappropriate for primary aged pupils,

### **Managing filtering**

- The school will work with ConnectUp to ensure systems to protect pupils are reviewed and improved,
- If staff or pupils discover an unsuitable site, it must be reported to the online safety leader or Headteacher.

### **Procedure to follow if an inappropriate or unsuitable site is accessed**

- **Do not** turn the computer off or log out
- **Switch the monitor and/or projector off**
- Contact the Head Teacher/Deputy
- A decision will then be made on the level of response needed and if any other individuals or organisations need to be involved.

### **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.

### **Protecting personal data**

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

### **Appendix 1- Pupil Online Safety Agreement**

### **Appendix 2- Staff Acceptable Use Policy**

Last Reviewed: March 2016

Next Review: March 2017

## Online Safety Agreement for Pupils



**ZIP IT**  
Keep your personal  
stuff private and think  
about what you say  
and do online.



**BLOCK IT**  
Block people who  
send nasty messages  
and don't open  
unknown links and  
attachments.



**FLAG IT**  
Flag up with someone  
you trust if anything  
upsets you or if  
someone asks to  
meet you offline.

To keep me safe whenever I use the internet or email, I promise...

- To keep my username and password private and not to use anyone else's
- To keep all personal information private
- To block unknown links and attachments by not opening anything that I do not trust
- To report any messages or internet pages that are unsuitable or upsetting
- To tell someone I trust if someone asks to meet me offline

When using computer equipment in school...

- I will only use the username and password that I have been given
- I understand that my behaviour will be checked
- I will not play games unless I have permission
- I will not open, copy, delete or change anyone else's files without their permission
- I will be polite and think carefully about how I talk to others online and what I say about them
- I will not take, copy or send pictures of anyone without their permission
- I will not try to upload, download or open any files, program or websites which are unsuitable or illegal
- I will not try to get around the filtering or security systems in place
- I will not install any program nor change the settings
- I will not use chat and social networking sites
- I will not copy other people's work and pretend it is my own
- I will not try to download copies of music, videos, games or other software
- I will check that information I use from the internet is from a trusted website
- I will always use what I have learned about online safety to keep myself safe and will tell a teacher if something makes me worried or unhappy.

If I break these rules...

- I understand that the school's behaviour guidelines will be followed

**I have read and understand this information and agree to follow it.**

Name of pupil \_\_\_\_\_

Signed \_\_\_\_\_ Date \_\_\_\_\_

**I have read and discussed this information with my child and give permission for him/her to use the school's ICT systems, including the internet.**

Parent/Carer signature \_\_\_\_\_ Date \_\_\_\_\_

## Staff Acceptable Use Policy

### **Rationale**

At The Whartons Primary School we are committed to our duty to safeguard and promote the welfare of children and young people. New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work.

All users should have an entitlement to safe internet access at all times. The school will ensure that staff have good access to ICT to enhance their work, to enhance learning opportunities for pupils' learning and will, in return, expect staff to agree to be responsible users. This policy applies to all adults working in our school.

### **This Acceptable Use Policy is intended to ensure:**

- That staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That staff are protected from potential risk in their use of ICT in their everyday work.

### **Acceptable Use Policy Agreement**

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed online safety in my work with young people.

### **For my professional and personal safety:**

- I understand that the school may monitor my use of the ICT systems, school email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops and school email) out of school.
- I understand that school ICT equipment is intended for educational use and so I will not use it for personal or recreational use.
- If I take school ICT equipment out of school, I will not allow other people to use it.
- I will not disclose my school network username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person.

### **I will ensure that when I am using school ICT systems:**

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner and I will not use aggressive or inappropriate language.



- I will ensure that when I take images of pupils I will only do so with parental permission. I will only use school equipment to take images or videos and I will not copy any images onto school staff laptops. I will not bring my own camera into school. Where images are published (eg on the school website) it will not be possible to identify by name, or other personal information, the pupils who are featured.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. I will not use personal email addresses, mobile phones or social networking sites to communicate with pupils or parents/carers (any text messages sent to parents will be sent via the school messaging service).
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- If I bring a mobile phone into school, I will not carry it on my person while I am in contact with pupils and I will store it out of their view.
- I will use a separate USB storage device for school work and will ensure that it does not contain personal files.
- On any occasion that I need to bring a laptop in to school from home, I will ensure that it is stored securely during the school day and that pupils do not have access to it. The laptop will only be used for professional purposes whilst in school. I understand that any personal ICT equipment may be monitored by the school.
- I will not access personal email accounts in the classroom during the school day.
- I will not open any files, including attachments to school emails, unless the source is known and trusted, due to the risk of viruses or other harmful programmes.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the school filtering systems.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not attempt to load software for which no licence is held.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I understand that data protection policy requires that any staff or pupil data to which I have access will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority (see also School Confidentiality Policy).
- I will not put confidential pupil data, such as addresses or safeguarding information, onto school laptops or USB storage devices.
- I understand that the school insurance policy states that school equipment, such as laptops are only insured on the school premises and in staff homes. I will never leave school equipment unattended when travelling to and from work.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

#### **When using the internet in my professional capacity:**

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies.

#### **I understand that I am responsible for my actions in and out of school:**

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of any school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.

- I understand that if I fail to comply with this Acceptable Use Policy, I could be subject to disciplinary action. This could include a warning, a suspension, a referral to Governors and/or the Local Authority and, in the event of illegal activities, the involvement of the police.

I have read and understand the Staff Acceptable Use Policy and agree to use all school ICT systems, equipment and my own devices within these guidelines:

Name

Job title

Signed

Date