E-Safety Policy

(Policy for E-Safety and Acceptable Usage)

Introduction

Name of School	Ocker Hill Infant School
Date of Policy	December 2018
Co-ordinator	Michelle Bailey
Policy Consultation	Curriculum
Review Date	December 2019

SAFEGUARDING AND PROMOTING THE WELFARE OF CHILDREN

Section 175 of the Education Act 2002 places a duty on local authorities and the governors of maintained schools to make arrangements to ensure that their functions are carried out with a view to safeguarding and promoting the welfare of children.

Section 157 of the same act and the Education (Independent Schools Standards) (England) Regulations 2003 require proprietors of independent schools (including academies) to have arrangements for safeguarding and promote the welfare of children who are pupils at the school. "Keeping Children Safe in Education", issued to schools in September 2018, details statutory guidance, placing a duty on schools to promote the welfare of children. The definition of safeguarding children as detailed in the document "Working Together to Safeguard Children" is as follows:

- *Protecting children from maltreatment*
- *Preventing impairment of children's' health or development*
- *Ensuring that children grow up in circumstances consistent with the provision of safe and effective care and*
- *Taking action to enable all children to have the best outcomes*

Safeguarding children is consequently more than contributing to the protection of individual children and the school is committed to the development of policy and practice that supports children and their families to be safe, healthy, enjoy and achieve, contribute positively and achieve economic wellbeing. These principles and the documents above have supported the writing of this E-Safety Policy.

In today's society children, young people and adults interact with technologies on a daily basis such as, mobile phones, games consoles and the internet. The exchange of ideas, social interaction and learning opportunities are beneficial but can occasionally place children, young people and adults in danger.

New technologies have revolutionised the movement, access and storage of information with important implications for all schools. At Ocker Hill Infant and Nursery School, we recognise that learning is a lifelong process and that e-learning is an integral part of it. We hope to empower and educate children, young people and adults with the skills to make safe and responsible decisions as well as feel able to report concerns. The school is committed to the continuing development of our ICT infrastructure and embracing new technologies so as to maximise the opportunities for all pupils, staff, parents and the wider community to engage in productive, cooperative and efficient communication and information sharing.

However, as in any other are of life, children are vulnerable and may expose themselves to danger, whether knowingly or unknowingly, when using the internet and other technologies. Additionally, some young people may find themselves involved in activities which are inappropriate, or possibly illegal. E-safety seeks to address the issue around using these technologies safely and promote an awareness of the benefits and risks.

This policy sets out clearly our expectations on pupils, staff, parents and members of the wider community to ensure best practice.

Teaching and Learning

Why is Internet use important?

- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- Pupils use the internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- 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 functions.
- Internet access is an entitlement for pupils who show a responsible approach to its use.
- Internet use will enable pupils to cover and understand computer science, digital imagery and information technology.

How can Internet use enhance learning?

- The school's Internet access will be designed to enhance and extend education.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The schools will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright laws.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

How will pupils learn to evaluate Internet content?

- Pupils will use age-appropriate tools to research Internet content.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole school requirement across the curriculum.

How will published material be managed?

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.
- The head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.
- Pupils will learn about safety content including the CEOP button use.

Physical Safety:

- All electrical equipment in the school is tested annually to ensure that it is safe to use. Pupils are taught about the dangers of electricity as part of the science and PSHE curriculum. We expect pupils to behave appropriately near electrical sockets and appliances.
- Workstations are cleaned and sanitised regularly. Pupils are taught to avoid taking food and liquids anywhere near the computers. We expect all users to refrain from eating and drinking when working at a computer.
- Health and safety guidance states that it is not healthy to sit at a computer for too long without breaks. Pupils are taught correct posture for sitting at a computer and that sitting for too long at a computer can be unhealthy. We expect all users to take responsibility for their own physical well-being by adopting good practices.
- Computers and other ICT equipment can be easily damaged. Pupils are taught the correct way to use ICT equipment. We expect pupils to respect ICT equipment and take care when handling and using.
- Staff users are expected to ensure that devices are closed down when not in use and stored away safely at the end of the day. Devices should not be left in cars.

Network Safety:

- All users need to log on using a username and password. Pupils are taught that they should only access the network using that particular log in. We expect all users to only log on using their username.
- On the network there are 'shared resource' areas where many different groups of users can save work so that it is available to others. Pupils are taught how to access and save to these shared resource areas. We expect pupils to respect the contributions of others, not to delete or alter others'

work and to ensure that they only save work to shared areas with permission.

- The network software prevents changes being made to computer settings. Pupils are taught that making changes may prevent the computer from working properly. We expect all users to make no attempt to alter the way the computer is set up.
- Only the network administrators are permitted to install software on to computers. Pupils are taught that the network or an application may not function properly if programmes are installed. We expect all users to make no attempt to load or download any programme on to the network.
- All users of the network can be monitored remotely by the network administrators. Pupils are taught that their use of the network can be monitored. We expect all users to understand that their use is subject to monitoring. We use the Sonic Wall package.

Internet Safety:

- The school's broadband access will include filtering using the package Sonic Wall to ensure that it is appropriate to the age and maturity of pupils.
- If staff or pupils discover unsuitable sites, the URL will be reported to the school E-Safety Coordinator who will then record the incident and escalate the concern as appropriate.
- The school Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Police or CEOP.
- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- Parents have access to the E Safety Policy on the school website and are encouraged to discuss it with their child at Induction Evenings.
- Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.
- When considering access for vulnerable members of the school community (such as children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).
- When using a network workstation all access to the Internet is protected by a number of different filters. These filters are designed to prevent accidental or deliberate access to unsuitable materials. In addition, the network administrators can manually add site addresses which are considered to be unacceptable. However, no system is 100% safe and we expect users to behave responsibly. Pupils are taught that the Internet contains many websites that are useful but that there are also websites that are unpleasant, offensive, not child-friendly or can damage your

computer. We expect pupils to make no attempt to access a website that they know to be unsuitable for children and/or containing offensive language, images, games or other media.

- Pupils accessing the Internet at home are subject to the controls placed upon them by their parents. However, any home use of the Internet made in connection with the school or school activities: any of its staff, pupils and governors or any partnership organisation will be subject to this policy and any breach dealt with as if the event took place at school. We expect all members of our school community to behave as positive ambassadors of the school in all school related activities made through the Internet.

Email:

- Staff will only use official school provided email accounts to communicate with professionals related to school business and parents, as approved by the Senior Leadership Team.
- The forwarding of chain messages is not permitted.
- In KS1 pupils can create a class email (not individual) to learn more about emailing.

Digital Images:

- Images or videos that include pupils will be selected carefully and will not provide material that could be reused.
- 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/videos of pupils are electronically published annually.
- Written consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.
- The school will have a policy regarding the use of photographic images of children which outlines policies and procedures.
- Digital still and video cameras are used for recording special events as well as being essential tools for everyday learning experiences across the curriculum. As part of pupil induction and on an annual basis in September parents are asked to sign a consent form for images of their children to be used for school purposes. See GDPR policy.

Cyber bullying:

- Cyberbullying (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.
- There are clear procedures in place to support anyone in the school community affected by cyberbullying.

- All incidents of cyberbullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of cyberbullying.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate. This may include identifying and interviewing possible witnesses and contacting the service provider and the police if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's E-Safety ethos.

Sanctions for those involved in cyberbullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
- Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the school's Anti-bullying or Behaviour policy..
- Parents/carers will be informed.
- The police will be contacted if a criminal offence is suspected.

The school takes bullying very seriously and has robust procedures for identifying and dealing with it. E-bullying is the use of any communication medium to offend, threaten, exclude or deride another person or their friends, family, gender, race, culture, ability, disability, age or religion. <u>We expect all members of our community to communicate with each other with respect and courtesy. Bullying of any type will not be tolerated by the school and will be dealt with under the procedures within the whole school policy on Behaviour and Anti-Bullying.</u>

<u>Learning Platform:</u>

- SLT and staff will regularly monitor the usage of the LP by pupils and staff in all areas.
- Pupils/staff will be advised about acceptable conduct and use when using the LP.
- Only members of the current pupils and staff community will have access to the LP.
- All users will be mindful of copyright issues and will only upload appropriate content onto the LP.
- When staff, pupils etc leave the school their account or rights to specific school areas will be disabled.

Any concerns about the content on the LP may be recorded and dealt with in the following ways:

- The user will be asked to remove any material deemed to be inappropriate or offensive.
- The material will be removed by the site administrator if the user does not comply.
- Access to the LP will be suspended.
- The user will need to discuss the issues with a member of the SLT before reinstatement.
- A pupil's parent/carer may be informed.

Personal Devices:

Staff use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school phone where contact with pupils or parents/carers is required.
- Mobile phone and devices will be switched off or switched to silent mode, Bluetooth communication should be hidden or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the Senior Leadership Team in emergency circumstances.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Communication

- All users will be informed that network and Internet use will be monitored.
- An E-Safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils and staff.
- Pupil instruction regarding responsible and safe use will precede Internet access.
- An E-Safety module will be included in the PSHE, Citizenship and Computing programmes covering both safe school and home use.
- E-Safety training will be part of the transition programme across the Key Stages and when moving between establishments.
- E-Safety rules will be posted in all rooms with internet access.

- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.
- Particular attention to E-Safety education will be given where pupils are considered to be vulnerable.

<u>Copyright:</u>

- Though there are lots of free to use resources on the Internet, the majority of image, sound and music files are covered by copyright laws. Some can be used for educational reasons without permission provided that the source is stated and that they are not made available outside the school. Some cannot be used under any circumstances, this is particularly so for music but can apply to other types of file eg photographic images. Care therefore needs to be taken with multi-media work which incorporates anything downloaded from the internet or any other published source that it is not uploaded onto the school's website or broadcast through any other technology. Pupils are taught that the people who put their work on the Internet may not always want people to copy or use their work and that they should check whether they have permission. <u>We expect all users to respect copyright laws.</u>
- It is important to know what work is original and when chunks of text have been copied from other sources such as the Internet. Pupils are taught that they should not present the work of others as their own work.

<u>Social media, social networking and personal publishing:</u>

- The school will control access to social media and social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications.
- Staff and governors to follow the protocol set out in the Staff Code of Conduct.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Concerns regarding pupils' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning pupils' underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the Staff Code of Conduct.
- Continual and regular checking for any changes in Social Media.

How will the school respond to any incident of concern?

- All members of the school community will be informed about the procedure for reporting E-Safety concerns.
- The E-Safety Coordinator will record all reported incidents and actions taken in the school E-Safety incident log and other in any relevant areas eg Bullying or Child protection logs.
- The Designated Safeguarding Lead will be informed of any E-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage E-Safety incidents in accordance with the school discipline/behaviour policies where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguarding Team or E-Safety officer and escalate the concern to the police.
- 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.

E-Safety complaints:

- Complaints about Internet misuse will be dealt with under the school's complaints procedure.
- Any complaint about staff misuse will be referred to the headteacher.
- All E-Safety complaints and incidents will be recorded by the school, including any action taken.
- Pupils and parents/carers will be informed of the complaints procedure.
- Parents/carers and pupils will need to work in partnership with the school to resolve issues.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- Discussions will be held with the local police safer schools partnership coordinators and/or Children's safeguard team to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.

E-Safety Rules displayed and shared with children all around school:

- Only use a computer when an adult is nearby.
- Never arrange to meet someone whom you have met through the Internet even if you think you know them well or they seem really nice.
- Never send a picture of yourself to a person that you don't know or haven't met.
- Don't fill out forms online without asking your parents or teacher first.
- Tell your parents or the teacher right away if you come across anything that upsets you or makes you feel uncomfortable.
- Check before downloading anything.
- Being unkind to someone online is a form of bullying.

Detailed rules for Email, Games, Friend Sites and Chatting online are also shared with the children.

Ocker Hill Infant and Nursery School

Social Media

Protocol for Staff and Governors

Introduction

'Social Media' is the term commonly given to websites and online tools which allow users to interact with each other in some way – by sharing information, opinions, knowledge and interests. Examples include social networking websites (such as facebook, Instagram, snapchat, twitter, bebo and MySpace) content sharing websites (such as flickr and You Tube), blogs (inc. Twitter) Chat facilities (inc. MSN), podcasts and message boards.

The growing popularity of social media has opened up new opportunities for communication. The following principles are intended to provide you with a framework to make responsible decisions about the use of these communication tools in relation to your role as a school employee or governor.

Whether or not you choose to create or participate in any of the media listed in the introduction above is your own decision. However it is important to be aware that posting information about any matter relating to your school can not be isolated from your role as a member of staff or governor.

Principles

These principles apply to your online participation and set out the standards of behaviour expected as a school employee or governor at Ocker Hill Infant and Nursery School.

- Be responsible; remember that you are an ambassador for our school.
- Stay within the legal framework and be aware that libel, defamation, copyright and data protection laws apply.
- If you are an employee and you are not using the sites/tools to support you directly in your job you should always access the sites/tools in your personal time.
- Do not make personal comments about individual children, parents or colleagues. Do not refer to incidents in school, this may be viewed as cyber bullying.
- Staff must not sign up pupils, parents, or ex- pupils as 'friends' on social networking sites.

- Protect your own privacy. Never give out personal details like home address and phone numbers. Make sure your settings are set as ‘Friends only’.

- Know and follow our school’s Employee Code of Conduct. Ensure that you present yourself as a respectable member of the community. Consider photographs that are on and ensure your use of language would not be perceived inappropriately by the community.

- Always remember that participation online results in your comments being permanently available and open to being forwarded on to or accessed by people that you may not have originally intended to read them. Your comments can be viewed much more widely and much more easily than through any other type of media.

Please note: inappropriate use of social media can breach confidentiality and damage the reputation of the school, which can lead to disciplinary action against staff members or suspension in the case of a governor.