Oak Farm Junior School

Online Safety Policy

Last reviewed: September 2017
Current review: September 2017
Next review: Sept 2018

Introduction

This school is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

The purpose of this policy is:

- To ensure that all staff, parents, governors and children understand and agree the school's approach to online safety. The policy relates to other policies including computing curriculum, Internet Access, MLE Policy, Bullying, Child Protection and Health and Safety.
- Establish the ground rules we have in school for using the Internet.
- Demonstrate the methods used to protect the children from sites containing unsuitable material.

The school believes that the benefits to pupils from access to the resources of the Internet far exceed the disadvantages. Ultimately, the responsibility for setting and conveying the standards that children are expected to follow, when using media and information resources, is one the school shares with parents and guardians.

Writing and reviewing the online safety policy

The school's Computing coordinator is currently responsible for coordinating online safety. The Online Safety Policy, Rules for Responsible Computer and Internet Use and Acceptable Use Policy for staff (AUP) have all been written building on the LGfL exemplar policies and Becta guidance.
It will be reviewed on an annual basis.

Teaching and Learning

The importance of internet and digital communications

- Access to the Internet is a necessary tool for staff and students; it helps to prepare students for their on-going career and personal development needs.
- It is a requirement of the statutory curriculum orders for Computing and is implied in other subject orders.
- The Internet is a part of everyday life for education, business and social Interaction.
- The school has a duty to provide students with quality Internet access as part of their learning experience.

Internet use enhances learning

- Internet access is currently provided by Hillingdon Grid for Learning (HGfL) and designed for pupils. This includes filtering appropriate to the content and age of pupils.
- 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 planned to enrich and extend learning activities.
- Access levels are reviewed to reflect the curriculum requirement.
- Pupils are given clear objectives for Internet use and sign 'Rules for Responsible Computer and Internet Use'.
- Pupils are taught how to take responsibility for their own Internet access.
- Where appropriate, staff will guide pupils to online activities that will support the learning outcomes planned for the pupils' age and maturity.
- The schools will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.

Pupils are taught how to evaluate Internet content

- Pupils need to learn how to evaluate Internet information and to take care of their own personal safety and security whilst online. The evaluation of online materials is a part of teaching and learning in every subject.
- Pupils will be taught ways to be critically aware of materials that they read and to validate information before accepting that it is necessarily accurate.
- Pupils will be taught to respect copyright when using Internet material in their own work.
- Pupils will be made aware that the writer of an e-mail or the author of a Web page might not be the person claimed.
- Pupils are encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Managing Internet Access

Information System Security

- The school's ICT system capacity and security is reviewed regularly by the ICT technician.
- Virus protection is updated regularly.
- Security strategies are discussed with the Local Authority.
- Unapproved software will not be allowed in pupils' work areas or attached to email.

E-mail

- Pupils may only use approved email or blogging accounts
- Pupils must tell a teacher immediately if they receive offensive email.
- In emails, pupils are taught that they must not reveal their personal details, those of others or arrange to meet anyone without specific permission.
- Pupils are taught not to open suspicious incoming email or attachments.
- Emails sent to an external organisation should be written carefully and authorised before sending.
- The forwarding of chain letters is not permitted.
- Whole class or teacher email addresses will be used in Oak Farm for communication by children.
- Access in school to external personal email accounts may be blocked.

Published content and the school web site

- The school website complies with the school's guidelines for publications.
- All material must be the author's own work or where permission to reproduce has been obtained, it is clearly marked with the copyright owner's name.
- The contact details on the website should be the school's address, email and telephone number and are for school administration purposes only.
- The head teacher and website coordinator take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupils' images and work on the school website

- Children's photographs should not be accompanied by their full names and photographs must not identify individual pupils. Where possible, group shots should be used in preference to individual 'passport' style images.
- Children's photographs will only be allowed to go on the website once written permission has been obtained from the child's parents.
- Still and moving images and sounds add liveliness and interest to a website, particularly when pupils can be included. Nevertheless the security of staff and pupils is paramount.
- Pupils' full names will not be used anywhere on the website in association with a photograph.

Social networking and personal publishing

- HGfL blocks / filters access to social networking sites as far as possible.
- Pupils and parents will be advised that use of social networking sites outside of school is inappropriate for primary-aged children. Guidance for parents and pupils will be published on the website and updated regularly.
- Children will have access to approved child-friendly networking sites at school and be taught how to use them safely. There will be opportunities to use forums / chat rooms in teacher moderated, closed communities.
- Pupils will not be allowed to access public chat rooms without supervision.
- Although primary age pupils should not use Facebook, Instagram, Twitter, Snapchat or similar sites, pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.
- No member of staff should use social networking sites or personal publishing sites to communicate with students, past or present.
- Staff need to be aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status. Examples include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chatrooms, instant messenger and many others.
- Teachers cannot under any circumstances mention any references to their working lives on any social media.
- The school will control access to social media and social networking sites. Pupils will be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location.
- Staff are advised not to run social network spaces for pupil use on a personal basis.

Managing filtering

- The school works in partnership with parents, the LEA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- The school's broadband access includes filtering appropriate to the age and maturity of pupils.
- Checks will take place to ensure that the filtering methods selected are effective in practice.
- If staff or pupils discover unsuitable sites, the URL address and content must be reported to the Internet Service Provider via the Computing coordinator.
- Pupils are not allowed to bring mobile phones into school. Under certain circumstances exceptions can be discussed with the Head teacher, so that pupil mobile phones can be kept in the school office.

Managing video conferencing and webcam use

- Video conferencing will always be appropriately supervised and pupils must ask permission before accepting or making any calls.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and the Head teacher in consultation with staff will give permission for appropriate use
- Current and emerging technologies used in school and (more importantly in many cases) outside of school by children include:
    - The internet
    - Email
    - Instant messaging often using single web-cams
    - Blogs
    - Podcasting
    - Social networking sites (www.facebook.com www.twitter.com, Instagram, musical.ly)
    - Video broadcasting sites (www.youtube.co.uk)
    - Chat rooms (www.teenchat.com , www.habbohotel.co.uk)
    - Gaming sites (www.neopets.com , www.miniclip.com/games , www.clubpenguin.com)
    - Music download sites (www.apple.com/itunes , spotify)
    - Mobile phones with camera and video functionality
    - Mobile technology (e.g. games consoles) that are 'internet ready'
    - Smart phones with email, web functionality and Office applications
    - Mobile phones must not be used during lessons. The sending of abusive or inappropriate text messages is forbidden. Cameras in mobile phones are not to be used by pupils.
    - Only school cameras are used by both staff and children for educational purposes.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Staff must not keep confidential information on removable devices such as USB devices unless suitably security protected.
- Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals.

Policy Decisions

Authorising Internet access

- The school will maintain a record of all staff and children who have access to the school's ICT systems.
- Please see acceptable use policy relating to staff, pupils and volunteers

Assessing risks

- The school takes all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network.
- Neither the school, nor HGfL, can accept liability for any material accessed, or any consequences of Internet access. The school's online safety policy and its implementation will be monitored and reviewed on a regular basis.

Handling online safety complaints

- Complaints of internet misuse must be referred to the head teacher and / or Computing coordinator.
- Any complaint about staff misuse must be referred to the head teacher. If the complaint is about the Head of School this should be reported to the Chair of Governors.
- Complaints of a child protection nature must be dealt with in accordance with the school's child protection policy.
- Pupils and parents are informed of the complaints procedure.
- Pupils and parents are informed of the consequences for pupil misuse of the Internet.
- All Online Safety complaints and incidents will be recorded by the school — including any actions taken.
- Discussions will be held with the local Police Safer Schools Partnership Coordinators and/or Children's Safeguards Unit to establish procedures for handling potentially illegal issues.

Community use of the Internet

- The school liaises with local organisations to establish a common approach to Online Safety.
- The school recognises that children can access the internet outside of school and offers support and advice to parents on internet safety though information sent home with children and through advice on the website.

Cyberbullying

- Cyberbullying (along with all forms of bullying) will not be tolerated in

School. All incidents of cyberbullying reported to the school will be recorded.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify bullying behaviour, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Parent/carers will be informed and the Police will be contacted if a criminal offence is suspected.

Communication Policy

Introducing the Online Safety policy to pupils

- The children will be taught about Online Safety in Computing and as part of every subject whenever pupils are using the Internet.
- All users are informed that network and Internet use will be monitored.
- Pupil instruction in responsible and safe use should precede Internet access every time they go online.
- Safe and responsible use of the internet and technology will be reinforced across the curriculum. Particular attention will be given where pupils are considered to be vulnerable.

Staff and the Online Safety policy

- The Online Safety Policy will be formally provided to and discussed with all members of staff and published on the school Learning Platform.
- Staff are informed that network and Internet traffic can be traced to an individual user.
- Discretion and professional conduct is essential at all times.
- Staff will always use a child friendly safe search engine when accessing the web with pupils.

Enlisting parents' and carers' support

- Parents' attention will be drawn to the School Online Safety Policy in newsletters, the school brochure, year group meeting and on the school website.
- The school has links on its website to Online Safety resources.
- The school asks all new parents to sign the pupil/parent agreement when they register their child with the school.

- The following Online Safety programmes will be used:
    - Think U Know: www.thinkuknow.co.uk
    - Childnet: www.childnet.com
    - Kidsmart: www.kidsmart.org.uk
    - Safe Social Networking: www.safesocialnetworking.com

Matt Szurgot
September 2017