

Oak Hill C of E Primary School

Internet E-safety / Acceptable Use Policy

This policy was written in consultation with staff and governors

Agreed by Governors: 12 March 2018

Review Date: March 2020



The school policy for Internet E-Safety reflects the consensus of opinion of the whole teaching staff and has the full agreement of the Governing Body.

Introduction

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.

Internet use includes accessing the World Wide Web and the use of email. The school encourages the use of the Internet, together with the development of appropriate skills to analyse and evaluate resources found on it.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Aims

Access to life-long learning and employment increasingly requires the use of a range of information technologies and pupils need to develop life skills for their use. The internet, as an open, public communications channel is just one aspect of this. This policy relates to the school's Internet environment and is part of a suite of e-safety documents and strategies developed to ensure pupils are provided with as safe and secure Internet environment as is possible, and are educated to be aware of, and respond responsibly, to any risks.

The policy identifies the measures in place in our school

- to protect children from undesirable content on the Internet
- to protect children from the risk of radicalisation
- to protect them from undesirable contacts over the Internet,
- to prevent unacceptable use of the Internet by children or adults
- to address issues of copyright for materials published on the Internet

Roles and responsibilities

E-safety is a whole-school responsibility dependent on all stakeholders e.g. staff, governors, advisers, parents and, where appropriate, pupils themselves taking responsibility for the use of the Internet and other forms of communication. Of major importance in creating a safe e-learning environment is the internet safety education which occurs in the classroom itself, initiated by the teacher or teaching assistant. The Head Teacher has overall responsibility for e-safety issues.

Staff may review files and communications stored in User Areas to ensure that users are using the system responsibly. Users should not expect that files stored on servers or disks would always be private.

E-learning technologies

Internet access is supplied by Gloucestershire County Council and SWGfL which provides an effective and safe e-learning environment including Internet access and e-mail service. To safeguard against risks and unacceptable materials and activities these services include filtering and content control, firewall and virus protection, and monitoring systems. All new Internet technologies will only be made accessible to the school e-community when they have been assessed for their nature, content, educational benefit, safety and security.

Permission to use the Internet

The Internet can provide pupils and all stakeholders with opportunities to experience and use a wide range of activities, resources, and information to support and enhance the learning and teaching across the whole school curriculum. All pupils will be expected to access the Internet unless parents have indicated otherwise at the time their child is admitted to school. Access is a privilege, not a right and that access requires responsibility. Unauthorised use of the Internet or use of unauthorised websites will not be tolerated. Parents will be asked to discuss with their children the e-safety agreement and sign the agreement. Without this being signed pupils will not be allowed to access the Internet.

Pupils will be informed by staff of their rights and responsibilities as users. Pupils will not be allowed undirected use of the Internet. Staff will provide pupils with links to sites which have been reviewed and evaluated prior to use. Staff must remain vigilant when their pupils are using the Internet in order to ensure that offensive or irrelevant materials are not accessed.

Individual users of the Internet in school are responsible for their own behaviour and communications over the Internet.

Social Networking

The use of personal social networking sites will not be permitted in school. Sending messages by e-mail or by any other means will only be undertaken as part of a whole class or group project, with the knowledge and supervision of the class teacher. Staff should not invite or accept pupils onto social networking sites and professional boundaries should be maintained.

Accessing and using the Internet

In lessons the majority of access to the Internet will be by the teacher, by adult demonstration or through carefully supervised access to specific approved on-line materials. Pupils will be taught how to use the internet safely and responsibly as an integral part of e-learning across the curriculum and supported by the school's e-safety scheme of work. In the spirit of Every Child Matters pupils will be taught how to be safe while online at home as well as at school.

The school's Internet home page will default to a recognised children's search engine as its Home page.

E-safety – Content

Unintentional exposure of children to Inappropriate Content

It is the School's policy that every reasonable step should be taken to prevent exposure of children to undesirable materials on the Internet. It is recognised that this can happen not only through deliberate searching for such materials, but also unintentionally when a justifiable Internet search yields unexpected results.

To protect children from such occurrences, the School has adopted the following position:

In-school protection by:

- adult supervision of pupils' Internet activity, with no accessing or searching of the Internet allowed without a suitable adult present in the room
- Pupils will be encouraged to explore the latest e-safety websites e.g www.thinkuknow.org and www.SafenSavvy.co.uk
- the 'caching' of Internet sites whenever possible in advance by staff to verify the site and its content
- children will be taught to become critical and discriminating users of materials they find online, through questioning the source and reliability of any content they access and by being aware of ways to minimise risks
- if any users discover undesirable sites, the URL (address) and content must be reported to the Head Teacher who will inform the ISP as soon as possible
- the use of the accredited County Council Broadband Service which provides protection by maintaining a list of approved sites
- filtering, such as blocking strategies, allowed lists, dynamic filtering, rating systems, flagging systems and monitoring
- the imposition of a 'banned list' of undesirable sites
- the filtering of sites by language content with prohibition of sites with unacceptable vocabulary
- 'live' anti-virus protection

Intentional access of undesirable content by children

Children should never intentionally seek offensive material on the Internet. In such instances these steps will be followed. Any such incident will be treated as a disciplinary matter, and the parents of a child or children will be informed.

In the event of children being exposed to undesirable materials, the following steps will be taken:

- Pupils will notify a teacher or teaching assistant immediately

- The e-safety coordinator (the Head Teacher) will be notified by the teacher.
- The incident will be recorded in a central log, located in the school office, by which the school may reliably report the frequency and nature of incidents to any appropriate party
- The County approved forensic monitoring software will be used to investigate as appropriate
- Parents will be notified at the discretion of the Headteacher according to the degree of seriousness of the incident (for example, exposure to materials that include common profanities might not be notified to parents, but exposure to materials that included pornographic images would be notified)
- The Headteacher will regularly notify Governors of any incidents involving inappropriate or unacceptable use of school internet / ICT facilities.

Intentional access to undesirable content by adults

Deliberate access to undesirable materials by adults is unacceptable, and will be treated as a disciplinary issue. If abuse is found to be repeated, flagrant or habitual, the matter will be treated as a very serious disciplinary issue. The Governors will be advised and the LA will be consulted.

Risks associated with Contact

The Internet as a means to contact people and organisations is an extremely valuable tool, encouraging the development of communications skills and transforming the learning process by opening up extra possibilities. However, just as in the real world, children may get involved in inappropriate, antisocial or illegal behaviour while using new technologies e.g. cyber bullying, identity theft, and arranging to meet people they have met online. Whilst children will, at times, use emails as part of their learning across the curriculum, the school does not use chat rooms or instant messaging. Children will however be made aware of the risks involved in all of these and ways of avoiding them, as part of their e-safety and digital literacy skills development.

If a member of staff has a concern of a safeguarding concern they are to refer to the school's Child Protection policy.

Receiving and sending of e-mails by children

It is recognised that e-mail messages received by children can contain language or content that is unacceptable and that some people may try to use e-mail to identify and contact children for unacceptable reasons. If any member of staff believes that a child has been targeted with e-mail messages by parties with criminal intent, the messages will be retained, the incident recorded, and the Governors and the child's parents informed. Advice will also be taken regarding possible further stops, including investigation using forensic monitoring software.

To avoid these problems the school has adopted the following practice:

- The use of the accredited County e-mail service which includes filtering all incoming and outgoing messages for inappropriate content and spam
- Pupils read e-mail messages when a member of staff is present, or the messages have been previewed by the teacher

- Children are taught not to open or respond to emails from a previously unknown source, but to tell the member of staff present in the room so that appropriate action can be taken
- Steps are taken to verify the identity of any school or child seeking to establish regular e-mail with this school
- Pupils save their emails / messages to Draft for the teacher or teaching assistant to approve before being sent (as they would with a conventional letter)
- To avoid children revealing their identity within e-mail messages, only the child's forename is revealed: when appropriate 'internet aliases' are used for each child: the child's personal address is never revealed, and information is never given that might reveal the child's whereabouts.

Other use of the Internet / other technologies and email facilities

School staff have access to the Internet for preparation of materials and the exchange of information for professional purposes. The school will provide a secure e-mail address for professional use to all members of staff.

All users of the network must be aware that their user area, including their Internet use history, may be accessed by network administrators and files may be removed. The school internet / e-mail facilities should only be used only for educational purposes during teaching and learning time. Staff are advised not to, but if they do choose to use school internet facilities for personal purposes, such as online banking or purchasing of items for personal use, this will be at their own risk.

Inappropriate use will be subject to similar procedures as those listed above.

Staff should be mindful of unsolicited emails from people they do not know and use the Spam reporting facility as appropriate.

Staff should not use personal mobile phones within the classroom for any purposes. Any photographs taken should be on school cameras.

Publishing of Content on the Internet

It is recognised that staff and children may at some time produce and publish materials on an Internet Website associated with the School or the County.

The school has its own website hosted through its recognised reputable ISP. Materials produced as part of children's learning may be published on it unless parents have indicated otherwise at the time their child is admitted to school.

No materials will be published on the Internet which contains any unacceptable images, language or content. Infringement of this rule will be taken as a serious disciplinary issue.

Use of the school's Internet facility by visitors and guests

Members of school staff are expected to take responsibility for the actions of any adult guests or visitors who they allow or encourage to use the school Internet facilities. The essential 'dos and don'ts' are explained to such visitors and guests prior to their use of the Internet.

Unacceptable use will lead to the immediate withdrawal of permission to use the school Internet facility.

Copyright Issues

It is recognised that all materials on the Internet are copyright, unless copyright is specifically waived. It is the school's policy that the copyright of Internet materials will be respected.

Where materials are published on the Internet as part of the teacher's professional duties, copyright will remain with the County Council. Internet published materials will contain due copyright acknowledgements for any third party materials contained within them.

Related documents and guidance

School e-safety awareness materials

- Pupil / parent user agreement and information leaflets
- E-safety education programme (for all year groups – Hectors World)
- E-safety posters