Vernon Primary School

Acceptable Use Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers and visitors) who have access to and are users of the school's ICT systems, both in and out of our setting.

Contents

1 The benefits of Internet access for education

Most curricula at European level require pupils to demonstrate that they can effectively locate, retrieve and exchange information using ICT. Access to the Internet offers pupils and teachers vast, diverse, and unique resources. The Internet opens up opportunities to initiate cultural exchanges between pupils from all over the world, while at the same time providing access to educational, social and leisure resources.

The main reason that we provide Internet access to our teachers and pupils is to promote educational excellence by facilitating resource sharing, innovation, and communication. However, for pupils and teachers, Internet access at school is a privilege and not an entitlement.

Unfortunately as there is the possibility that pupils will encounter inappropriate material on the Internet, the school will actively take all reasonable precautions to restrict student access to both undesirable and illegal material.

Teachers are responsible for guiding pupils in their on-line activities, by providing clear objectives for Internet use. Teaching staff will also ensure that pupils are only too aware of what is regarded as acceptable and responsible use of the Internet. The main goal is to utilise Internet access to enrich and extend those learning activities that reflect the curriculum requirements and the age and maturity of the pupils.

Pupils will access websites from bookmarks within the 'Favourites' folder in their browser. These will have been previewed and approved by their teacher.

The free use of search engines is permitted only when another teacher or member of staff is present. Child friendly search engines, for example yahooligans.com can filter most websites with inappropriate content and will be used as a first option. Other search engines intended for use by pupils offer a filtered list of links.

All Internet access is filtered through a proxy server to screen out undesirable sites at source

2 Whole-school network security strategies

Infrastructure, equipment, filtering and monitoring

The school will be responsible for ensuring that the infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- All users will have clearly defined access rights to school's ICT systems
- All users will be provided with a username and password. Users will be required to change their password regularly
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- In the event of the filtering system needing to be switch off for any reason, or for any user, this must be logged and carried out by a process that is agreed by Headteacher

- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager
- An appropriate system is in place for users to report any actual / potential safety incident to SLT
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school's systems and data
- Personal use of the school's ICT systems should be limited to what may be deemed reasonable. The services are provided predominantly for education purposes
- Neither staff nor pupils should install programmes or other software on workstations, portable devices or servers, without the prior express, written permission of the school's Network Manager
- The school's ICT infrastructure and individual workstations are protected by up to date virus software
- Personal data (as defined by the Data Protection Act) cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured by password or other means
- Where staff have email accounts and other data on their phone or other mobile device they must ensure that the device is locked with a password.

Hardware and software infrastructures

The school has invested in the following hardware and software infrastructures to reduce risks associated with the Internet.

Proxy server – in conjunction with a web management system

Filtering software

Firewall – that has been configured to prevent access to inappropriate websites.

Classroom management structures

Individual pupil logins will allow teachers to trace and monitor student access and usage of the Internet.

Ensure that computers are positioned in such a way that monitors are easily observed by teachers.

3 Risk assessment and management of Internet content

The school has taken and will continue to take all reasonable precautions to ensure that pupils access appropriate material only. However, it is not possible to guarantee that a student will never come across unsuitable material while using a school networked computer. The school, however, cannot accept liability if such material is accessed nor for any consequences resulting from Internet access.

All pupils are taught effective online research techniques, including the use of subject catalogues and search engines. Receiving information over the web or in e-mail or text messages presupposes good information-handling skills.

Key online information-handling skills include:

- Ensuring the validity, currency and origins of the information accessed or received;
- Using alternative sources of information for comparison purposes;

- Identifying an author’s name, date of revision of the materials, and possible other links to the site;
- Respecting copyright and intellectual property rights.

Pupils will be made fully aware of the risks to which they may be exposed while on the Internet. They will be shown how to recognise and avoid the negative areas of the Internet such as pornography, violence, racism and exploitation of children.

However, if they encounter such material they will know that they should switch off the monitor, not the computer, and report the incident to the nearest teacher or the school's ICT co-ordinator who will deal with it according to the school AUP.

4 Regulation and guidelines

The school’s Internet access incorporates a software filtering system to block certain chat rooms, newsgroups, and inappropriate websites. The filtering system used on the school network aims to achieve the following:

- Access to inappropriate sites is blocked.
- The content of web pages or web searches is dynamically filtered for unsuitable words.
- A rating system is used to rate web pages for inappropriate content and that the web browsers are set to reject these pages.
- Records of banned Internet sites visited by pupils and teachers are logged.

The school's ICT subject leader regularly assesses the effectiveness of the filtering system. The school’s filtering strategy depends on the age and curriculum requirements of each class.

The school will immediately report the details of any inappropriate or illegal Internet material found to Computeam so it can be blocked in future.

Similarly, the school will request of IT support that 'allow' access be made of certain banned sites and provide the educational reasons behind the request.

4.1 E-mail accounts

- Pupils may only use their approved Google Classroom account/s on the school network during school time.
- Pupils shall immediately report any offensive messages that they receive to their class teacher.
- Access in school to external, Web-based, personal e-mail accounts is denied for network security reasons.
- It is forbidden to distribute chain letters or to forward a message without the prior permission of the sender.
- Pupils may not reveal their own or other people’s personal details, such as addresses or telephone numbers or arrange to meet someone outside school via Google Classroom.
- Sending and receiving e-mail attachments is subject to permission from the teacher.

4.2 The school's website

Individual teachers will add their own contributions to webpages. The Assistant Headteacher and website coordinator ensures that the content on the site is accurate, up to date and appropriate. The website will comply with the Department for Education's guidelines.

The copyright of all material produced by the school for display on the school's web pages belongs to the school. Permission to reproduce any other material will be sought and obtained, from the copyright owner.

The contact details for the school will include only the school's postal address, e-mail address and telephone number. No information about teachers' home addresses or the like will be published.

The school will not publish any material produced by pupils without the agreed permission of their parents. In addition, photographs of pupils will not be published without a parent or carer's written permission. A student's full name will not be used in association with photographs without permission, and first names only in this instance.

Website photographs which include pupils will be carefully selected.

4.3 Moderated mailing lists, newsgroups and chat rooms

The school may use/uses an e-mail distribution list to send messages to selected groups of users.

Teachers will moderate other collaboration tools such as newsgroups and chat rooms if used on the school network for learning purposes.

Pupils will be denied access to public or unmoderated chat rooms.

4.4 Other communication technologies

Pupils are not allowed to use mobile devices during lessons or formal school time. Pupils who bring in phones will need to hand them in at the start of the day to be returned for the end of the day. They are not to be used on school grounds. It is forbidden to send abusive or otherwise inappropriate text messages using the facilities provided by the school network.

5 Communicating the school's AUP

5.1 Informing pupils

'Code of Practice' will be displayed each time a staff member/student/visitor logs in and uses a laptop for them to agree too before use. Pupils will be informed that their Internet use is monitored and be given instructions on safe and responsible use of the Internet. The school has created separate Rules for Acceptable and Responsible Internet Use for primary. Pupils must read and understand the rules.

5.2 Informing staff

All staff will be provided with a copy of the School's Acceptable Use Policy. Teachers are aware that Internet traffic can be monitored and traced to an individual user. Staff will be consulted regularly about the development of the school's Acceptable Use Policy and instructions on safe and responsible Internet. Teachers will also sign the relevant part of the Acceptable Use Policy' document.

To avoid misunderstandings teachers will contact the ICT subject leader regarding any doubts that arise concerning the legitimacy of any given instance of Internet use. Teachers will be provided with information on 'copyright and the Internet' issues that apply to schools.

5.3 Informing parents / carers

Parents' attention will be drawn to the School AUP on the school's website. Advice that accords with acceptable and responsible Internet use by pupils at home will be made available to parents. Safety issues will be handled sensitively.

The school will obtain parental consent before publication of pupils' work or photographs.

Policy Date: Sept 2021
Review Date: Sept 2024
Ratified by Governors: Sept 2021