

E-Safety Policy

Codsall Middle School

Codsall Middle School



E-Safety Policy

Introduction

The Internet is regarded as an essential resource to support teaching and learning. The curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail and mobile learning. Computer skills are vital to access life-long learning and employment; indeed Computing is now seen as an essential life-skill. ICT skills and resources are used daily to support and enhance the learning of the children at Codsall Middle.

Young people have access to the Internet from many places, home, school, friends' homes, libraries and in many cases mobile phones. Schools have a number of services to help ensure that curriculum use is safe and appropriate, however, access out of school does not usually have these services and has a range of risks associated with its use. This policy is designed to ensure safe internet use by pupils in school and give them the skills and awareness to remain safe while on-line at home.

Rationale

The purpose of this policy is to:

- set out the key principles expected of all members of the school community at Codsall Middle School with respect to the use of ICT-based technologies.
- safeguard and protect the children and staff of Codsall Middle School.
- assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- have clear structures to deal with online abuse such as cyber-bullying which are cross referenced with other school policies.
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- minimise the risk of misplaced or malicious allegations made against adults who work with students.

Our whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities
- E-Safety teaching is embedded into the school curriculum.

Technical and Hardware Guidance

School Internet provision:

The school use a Staffordshire approved content filter to ensure that as far as possible, only appropriate content from the Internet finds its way into school. Whilst this filtering technology is robust and generally effective at blocking unsuitable material, it is still possible for unsuitable material to occasionally get past the filter.

- All pupils and staff have been issued with clear guidelines on what to do if this happens, and parents will be informed where necessary.
- Pupils or staff who deliberately try and access unsuitable materials will be dealt with according to the rules outlined elsewhere in this document.
- Pupils and parents sign and agree an internet use policy in the school planner and are informed of pertinent e-safety messages as necessary via the school newsletter.

Downloading files and applications:

The Internet is a rich source of free files, applications, software, games and other material that can be downloaded and installed on a computer. Whilst we are protected by highly efficient internet filtering and blocking system, the nature of some content may remain unpredictable.

- Pupils are therefore, not allowed to download any materials from the internet unless directed to do so by an appropriate member of staff.

Portable storage media:

- Staff and pupils are allowed to use their own portable media storage (USB Keys etc). If use of such a device results in an anti-virus message they should remove the device and immediately report to the ICT teacher or a member of Concero support staff

Teaching and Learning

We think it is crucial to teach pupils how to use the Internet safely, both at school and at home, and we use the Kidsmart safety code to support our teaching in this area:

Kidsmart has been developed by the Childnet charity, and is endorsed by the DfES
<http://www.kidsmart.org.uk>

The main aspects of this approach include the following five SMART tips:

Safe - Staying safe involves being careful and not giving out your name, address, mobile phone no., school name or password to people online...

Meeting someone you meet in cyberspace can be dangerous. Only do so with your parents'/carers' permission and then when they are present...

Accepting e-mails or opening files from people you don't really know or trust can get you into trouble - they may contain viruses or nasty messages...

Remember someone online may be lying and not be who they say they are. If you feel uncomfortable when chatting or messaging end the conversation...

Tell your parent or carer if someone or something makes you feel uncomfortable or worried...

Why Internet use is important

The Internet is an essential element in 21st century 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 is a part of the statutory curriculum and a necessary tool for staff and pupils.

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff will guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity and educate them in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate Internet content

- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the school ICT teacher or support staff from Concerro
- Staff will ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

Information system security

- The security of the school information systems will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- The school uses broadband with its firewall and filters.

E-mail

- Pupils may only use approved e-mail accounts on the school system. Children are not allowed access to personal e-mail accounts or chat rooms whilst in school.
- Pupils must immediately tell a teacher if they receive 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.

Published content and the school web site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- 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 photographs of pupils are published on the school website.
- All parents / carers are asked for permission for their children's photograph to be taken and uploaded to the school website. At no point will a photograph be uploaded online with a child's name.

Social networking and personal publishing

- Social networking sites and newsgroups will be blocked unless a specific use is approved.
- Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples include real name, address, mobile or landline phone numbers, school, e-mail address, names of friends, specific interests and clubs etc.
- Pupils and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged pupils.

Mobile phones

- Those children who choose to bring a mobile phone to school hand them in to the Office where they are kept in a secure place until they are collected at the end of the school day.
- The use of mobile phones is only permitted within school by members of staff for specific learning activities (e.g. taking pictures of art work, recording a voice memo for a radio interview etc.) They are then returned to the school office after use.
- If a pupil does not hand in their mobile phone and they are found in possession of it then it will be kept securely at the school office until a responsible adult comes to collect it.

Managing filtering

- The school will work in partnership with the service provider to ensure filtering systems are as effective as possible.
- If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the school E-Safety leader.

Protecting personal data

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

To be reviewed October 2021