



Osmaston Primary School

E-Safety Policy

Teaching and learning

Why Internet and digital communications are 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 is provided through Derby City Council
- 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
- Pupils will be shown how to publish and present information appropriately to a wider audience.

Pupils will be taught how to evaluate Internet content

- The school will seek to ensure that the use of Internet derived material by staff and by pupils complies with copyright law
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy
- Pupils will be taught how to report unpleasant Internet content using the CEOP Report Abuse icon.

Managing Internet Access

- Information system security- only designated staff will be allowed access the school's information system (e1)
- School ICT systems security will be reviewed regularly
- Virus protection will be updated regularly

E-mail

- Pupils and staff may only use approved e-mail accounts on the school system i.e. addresses ending with @osmaston.derby.sch.uk
- Pupils must immediately tell a teacher if they receive an 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

- Staff to pupil email communication must only take place via a school email address or from within the learning platform and will be monitored
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known
- The school will consider how e-mail from pupils to external bodies is presented and controlled
- The forwarding of chain letters is not permitted.

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 Staff and pupil personal information will not be published
- The Head Teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupils' images and work

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Social networking and personal publishing on the school learning platform

- The school will not allow access to social networking sites, but will consider how to educate pupils in their safe use e.g. use of passwords and privacy settings
- Newsgroups will be blocked unless a specific use is approved
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils must not place personal photos on any social network space provided in the school learning platform
- Pupils will be advised to use nicknames and avatars when using social networking sites

Managing filtering

- If staff or pupils come across unsuitable on-line materials, the site must be reported to the E-safety Coordinator. (Mr M Gard)
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Screen shots will be taken through the use of XXXX

Managing video-conferencing

- Pupils should ask permission from the supervising teacher before making or answering a video-conference call.
- Video-conferencing will be supervised and will be appropriate for the pupils' age.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed

- Mobile phones and associated cameras will not be used during lessons or formal school time except as part of an educational activity. The sending of abusive or inappropriate text messages is forbidden. Mobile phone cameras must not be used to photograph pupils
- Games machines including the Sony PlayStation, Microsoft Xbox and others have Internet access which may not include filtering. Care will be taken with their use within the school
- Staff will use a school phone where contact with pupils is required.

Protecting personal data

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

Policy Decisions

Authorising Internet access

- All staff must read and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems
- Pupils must apply for Internet access individually on entry to the school by agreeing to comply with the Responsible Internet Use statement published in their planner
- Any person not directly employed by the school will be asked to sign an 'acceptable use of school ICT resources' before being allowed to access the Internet from the school site.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor DCC can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate and effective.

Handling E-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff
- Any complaint about staff misuse must be referred to the Head Teacher
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures
- Pupils and parents will be informed of the complaints procedure.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Community use of the Internet

- All use of the school Internet connection by community and other organisations shall be in accordance with the school E-safety Policy.

Communications Policy

Introducing the E-safety policy to pupils

- Appropriate elements of the E-safety policy will be shared with pupils
- E-safety rules will be posted in all networked rooms.
- Pupils will be informed that network and Internet use will be monitored.
- Curriculum opportunities to gain awareness of E-safety issues and how best to deal with them will be provided for pupils, Staff and the E-safety policy
- All staff will be given the School E-safety Policy and its importance explained
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

Enlisting parents' support

- Parents and carers will from time to time be provided with additional information on E-safety
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.