e-Safety Policy

A Love of Learning for Life

Ivydale Primary School and Children's Centre believes that the use of information and communication technologies brings great benefits. Recognising the e-Safety issues and planning accordingly will help to ensure appropriate, effective and safer use of electronic communications.

Why do we need an e-Safety Policy?

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

e-Safety covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children.

It is essential that we decide on the right balance between controlling access to the internet and technology, setting rules and boundaries and educating students and staff about responsible use. We are aware that children and staff cannot be completely prevented from being exposed to risks both on and offline. Children should be empowered and educated so that they are equipped with the skills to make safe and responsible decisions as well as to feel able to report any concerns. All members of staff need to be aware of the importance of good e-Safety practice in the classroom in order to educate and protect the children in their care. Members of staff also need to be informed about how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role.

We are aware of the school's legal obligations to safeguard and protect children on and offline and the accountability of these decisions will sit with the Head Teacher and the Governing body. Breaches of an e-Safety policy can lead to civil, disciplinary and criminal action being taken against staff, pupils and members of the wider school community.

This policy is essential in setting out how the school plans to develop and establish its e-Safety approach and to identify core principles which all members of the school community need to be aware of and understand. The e-Safety Policy is part of many different policies including the ICT Policy, Safeguarding Policy, Anti-Bullying and School Development Plan and should relate to other policies including those for behaviour, for personal, social and health education (PSHE) and for citizenship.

The school has appointed an e-Safety Coordinator. The e-Safety Policy and its implementation will be reviewed annually.

The importance and benefits of the Internet in enhancing learning

The rapid developments in electronic communications are having many effects on society. Internet use is part of the statutory curriculum and is a necessary tool for learning. 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. Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security. 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.

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils worldwide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of schools, support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with Southwark and DfE;
- access to learning wherever and whenever convenient.

The school's Internet access will be designed to enhance and extend education. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. The schools will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law. Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils. Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability. 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 taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work. Pupils will use age-appropriate tools to research Internet content. The evaluation of online materials is a part of teaching and learning in every subject. Pupils' internet use will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.

Security

The security of the school information systems and users will be reviewed regularly. Virus protection will be updated regularly. Personal data sent over the Internet or taken off site will be encrypted. Portable media may not used without specific permission followed by an anti-virus / malware scan. Unapproved software will not be allowed in work areas or attached to email. Files held on the school's network will be regularly checked. The network manager will review system capacity regularly. The use of user logins and passwords to access the school network will be enforced.

Email

Pupils may only use approved email accounts for school purposes. Pupils must immediately tell a designated member of staff if they receive offensive email. Pupils must not reveal personal details of themselves or others in email communication, or

arrange to meet anyone without specific permission from an adult. Children will access email via whole-class or group email addresses when communicating outside of the school. Staff will only use official school provided email accounts to communicate with pupils and parents/carers. Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.

Published content including pupils' images

The contact details on the school website should be the school address, email and telephone number. Staff or pupils' personal information must not be published. The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright. Written permission from parents or carers will be obtained before images/videos of pupils are electronically published. Images or videos that include pupils will be selected carefully and will not provide material that could be reused. Pupils' full names will not be used anywhere on the website, particularly in association with photographs.

Social networking and social media

There will be no access to any social media or social networking sites in school. However, we acknowledge that children will access such sites from home. Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupil will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private. Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc. Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc. All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory. Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites. Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Code of Conduct policy.

Filtering

Levels of Internet access and supervision will vary according to the pupil's age and experience. Access profiles must be appropriate for all members of the school community. Teachers might need to research areas including drugs, medical conditions, bullying, racism or harassment. In such cases, legitimate use should be recognised and restrictions removed temporarily. It is important that schools recognise that filtering is not 100% effective. There are ways to bypass filters (such as using proxy websites, using a device not connected to the network e.g. mobile phone). Occasionally mistakes may happen and inappropriate content may be accessed. It is therefore important that children should always be supervised when using internet access. In addition, Internet Safety rules should be displayed, and both children and adults should be educated about the risks online. The school's broadband access includes filtering appropriate to the age and maturity of pupils. The school works with LGfL to ensure that filtering is continually reviewed. The school has a clear procedure for reporting breaches of filtering to LGfL.

If staff or pupils discover unsuitable sites, the URL will be reported to the School e-Safety Coordinator who will then record the incident and escalate the concern as appropriate.

Emerging technologies

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school policy. We aim to keep up to date with new technologies, including those relating to mobile phones and handheld devices, and be ready to develop appropriate strategies.

Cyberbullying

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour for learning. All incidents of cyberbullying reported to the school will be recorded. The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary. Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.

Mobile phones

Mobile phones and other personal devices such as Games Consoles, Tablets, PDAs and MP3 Players etc. are considered to be an everyday item in today's society and even children in early years settings may own and use personal devices to get online regularly. Mobile phones and other internet enabled personal devices can be used to communicate in a variety of ways with texting, camera phones and internet accesses all common features. However, mobile phones can present a number of problems when not used appropriately:

- They are valuable items which may be stolen or damaged;
- Their use can render pupils or staff subject to cyberbullying;
- Internet access on phones and personal devices can allow pupils to bypass school security settings and filtering.
- They can undermine classroom discipline as they can be used on "silent" mode;
- Mobile phones with integrated cameras could lead to child protection, bullying and data protection issues with regard to inappropriate capture, use or distribution of images of pupils or staff.

Due to the widespread use of personal devices it is essential that we take steps to ensure mobile phones and devices are used responsibly at school and it is essential that pupil use of mobile phones does not impede teaching, learning and good order in classrooms. Staff are given clear boundaries on professional use. The use of mobile phones and other personal devices by students and staff in school will be decided by the school and covered in the school Mobile Phone Policy and the staff Code of Conduct.

Protecting personal data

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

Risk assessment

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use. Methods to identify, assess and minimise risks will be reviewed regularly.

Responding to incidents of concern

All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc). The designated Child Protection Coordinator will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately. The school will manage e-Safety incidents in accordance with the school discipline/ behaviour policy where appropriate. The school will inform parents/carers of any incidents of concerns as and when required. After any investigations are completed, the school will debrief, indentify lessons learnt and implement any changes required. Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguard Team or e-Safety officer and escalate the concern to the Police.

Handling e-Safety complaints

Complaints about Internet misuse will be dealt with under the School's complaints procedure. Any complaint about staff misuse will be referred to the head teacher. All e–Safety complaints and incidents will be recorded by the school, including any actions taken. All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns. Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures. All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

Policy communication

All users will be informed that network and Internet use will be monitored. e–Safety training is provided across the school to raise the awareness and importance of safe and responsible internet use amongst pupils. e-Safety rules are displayed in all rooms with Internet access. Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas. Particular attention to e-Safety education will be given where pupils are considered to be vulnerable.

The e–Safety Policy will be formally provided to and discussed with all members of staff. Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff. Staff who manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues. All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

Parents' attention will be drawn to the school e-Safety policy in newsletters, the school prospectus and on the school website. Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents.

e-Safety Contacts and References

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk
Childline: www.childline.org.uk
Childnet: www.childnet.com
Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk
Cybermentors: www.cybermentors.org.uk
Digizen: www.digizen.org.uk
Internet Watch Foundation (IWF): www.iwf.org.uk
Kidsmart: www.kidsmart.org.uk
Orange Education: www.orange.co.uk/education
Safe: www.safesocialnetworking.org
Teach Today: http://en.teachtoday.eu
Think U Know: www.thinkuknow.co.uk
Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com