# CBJS E-Safety Policy

**Who writes and reviews the policy?**

The school will appoint an e-Safety Coordinator. This will be Sarah Hobden, headteacher, who is also the Designated Child Protection Coordinator as the roles overlap. The e-Safety Coordinator will work with the ICT subject leader and network manager and the local authority ICT Services. Our e-Safety Policy has been written by the school, building on the SMBC School's e-Safety Policy and government guidance and in consultation with staff, parents, governors and pupils. It has been agreed by the senior management and approved by governors. The e-Safety Policy and its implementation will be reviewed annually.

**Why internet use is important**

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.

Internet access is an entitlement for students who show a responsible and mature approach to its use. Internet use is part of the statutory curriculum and a necessary tool for learning.

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.

We are also aware that pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security both in and out of school.

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries and to experts in many fields for pupils and staff;
- inclusion in the National Education Network connecting all UK schools;
- educational and cultural exchanges between pupils world-wide;
- vocational, social and leisure use in libraries, clubs and at home;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across 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 SMBC and DCFS;
- access to learning wherever and whenever convenient.

**How the internet enhances learning**

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 will be given clear objectives for Internet use. Access levels will be reviewed to reflect the curriculum requirements and age of pupils. We believe in using a managed system that encourages young people to make responsible choices in school and out of school.

Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity and pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

**Pupils use of ICT and responsibilities**

Rules for Internet access will be posted in all networked rooms. An e-Safety training programme will be delivered to all pupils to raise the awareness and importance of safe and responsible use of the Internet and other electronic communications tools. This programme will focus on PSHE and ICT areas of learning. Instruction in responsible and safe use will precede Internet access and will be reinforced at regular intervals. We use the SMART rules (Kidsmart) as the basis of our e-safety teaching for pupils, as we believe they are a memorable way of reminding pupils of the rules in a simple, age-appropriate way. The SMART rules are displayed in all teaching rooms and elsewhere is school as appropriate.

Pupils will be aware that their ICT use in school will be monitored and that it s their responsibility to make responsible choices, to ask for help as needed and to report any worries or concerns to a safe adult.

**Staff ICT use and responsibilities in School**

All staff will read 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. Staff development in safe and responsible Internet use and on the school e-Safety Policy will be provided as required.

When using ICT with children, staff should take suitable [precautions to ensure pupils only access age-appropriate content, e.g. checking search engine results in advance for key topics, directing children to specific websites, using child friendly search engines etc.

**Parents' responsibilities and school's role in supporting parents**

Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school website. Internet issues will be handled sensitively to inform parents without alarm and parents will be informed of the procedure for reporting any issues as set out above. A partnership approach with parents will be encouraged. This will include parents' evenings with demonstrations and suggestions for safe home Internet use. Interested parents will be referred to organisations listed in the section on e-Safety Contacts and References. Such links will be available on the school website and on the school extranet site.

**Internet Access**

The school will maintain a current record of all staff and pupils who are granted Internet access. All users must read, sign and abide by the 'Acceptable ICT Use Policy' before using any school ICT resource. Parents will be informed that pupils will be provided with supervised Internet access and will sign a Responsible Internet Use agreement stating that their child will use the internet responsibly and within the school rules. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Methods to identify, assess and minimise risks will be reviewed regularly. The head teacher will ensure that the e-Safety Policy is implemented and compliance with the policy monitored. In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor SMBC can accept liability for the material accessed, or any consequences of Internet access.

**Passwords**

**Staff**

- Passwords will be alphanumeric
- Passwords will be changed at least annually (more frequently is recommended)
- Passwords will be private and not shared with other staff.

**Pupils**

- Passwords will be set prior to arrival at the school.
- Passwords will be kept safely by the class teacher
- Passwords will be private and not shared with other staff.
- Pupils will only use their own login.
- New passwords can be requested by staff (on a pupil's behalf) using the SSO log.

**Pupils evaluating internet content**

The schools will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law. If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to Solihull ICT Services through the e-safety officer or ICT manager. The evaluation of on-line materials is a part of every subject and the skills of evaluating the usefulness and accuracy of online materials, as well as crediting the owner where appropriate, will be taught and reinforced.

**Managing Published Content**

The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information, beyond name and job title, will not be published. The ICT manager will take overall editorial responsibility and ensure that content is accurate and appropriate. The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

**Publishing images of staff and pupils**

Photographs on websites that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. Pupils' full names will not be used anywhere on the website, particularly in association with photographs. Images of staff should not be published without consent.

**Managing social networking- in school**

*This section is based on advice from Solihull metropolitan Borough Council*

- 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 would include real name, address, mobile or landline phone numbers,

school, IM address, email address, names of friends, specific interests and clubs etc. Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name, school or shopping centre.

- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.
- Students should be encouraged to invite known friends only and deny access to others. They should be advised not to publish specific and detailed private thoughts.
- Schools should be aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments. Incidents of bullying through social networking will be dealt with in line with the school policy on bullying.

**Managing Social networking- staff**

*This section is based on advice from Solihull metropolitan Borough Council*

- Staff members' official blogs or wikis should be password protected and run from the school website. Teachers should not run social network spaces for students on a personal basis.
- Staff should not have any contact with pupils on social network sites on educational or any other matters. Exceptions could be for immediate family and even then care should be taken on comments made to avoid being unprofessional or open to criticism. Staff also need to make careful judgements when making contact with other members of the school community to ensure this does not compromise their professional role.
- Staff using social networking sites need to ensure that any content posted online could not be perceived as negative or unprofessional. Comments relating to school are to be avoided.

**Cyber-Bullying**

At CBJS, bullying is not tolerated. Cyber bullying will be dealt with in accordance with the school bullying policy. As a school, we accept our responsibility to deal appropriately with cyber-bullying incidents that occur outside of school, involving our pupils when we are made or become aware of them. This will involve communication with parents, the pupils involved as appropriate and will fall in line with the existing bullying policy.

**Managing filtering**

The school will work in partnership with Solihull MBC and BECTA 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 coordinator. Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP.

**Managing email**

- Pupils may only use approved email accounts on the school system. Pupils must immediately tell a teacher 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.
- Staff and pupils should only communicate through the school system (Solgrid email).
- Use of words included in the filtering/checking 'banned' list will be detected and logged. 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. The forwarding of chain letters is not permitted. Email addresses should be published carefully, to avoid spam harvesting.

**Video Conferencing**

All video conferencing equipment in the classroom must be switched off when not in use and not set to auto answer. IP video conferencing should use the educational broadband network to ensure quality of service and security rather than the Internet. Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name. External IP addresses should not be made available to other sites. Video conferencing contact information should not be put on the school website. Pupils should ask permission from the supervising teacher before making or answering a videoconference call. Video conferencing should be supervised appropriately for the pupils' age. When recording a lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material shall be stored securely. If third-party materials are to be included, check that recording is acceptable to avoid infringing the owners' Intellectual Property Rights (IPR).

**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 will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

**Managing information services**

The security of the school information systems will be reviewed regularly. Virus protection will be updated regularly. The network manager will review system capacity regularly.

**Protecting personal data**

Personal data will be recorded, processed, transferred and made available in compliance with to the Data Protection Act 1998.

**Transferring data outside of school**

School data sometimes needs to be used outside of school by staff, e.g. tracking documents. School data should only be copied to a memory stick or laptop encrypted in accordance with school policy and even then it is the staff member's responsibility to ensure that this information is kept safe and that any loss or potential loss of information is reported promptly to a member of senior management..

**E-safety concerns, complaints and logging**

An e-safety log will be kept in the w: drive (W:\ICT\ICT Incident Log) and any ICT issues involving inappropriate content and inappropriate use of ICT by pupils will be recorded here. Formal 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 who should use the agreed SMBC procedures. Pupils and parents will be informed of the complaints procedure. Sanctions for pupils within the school discipline policy include:

- interview/counselling by senior member of staff;
- informing parents or carers;
- removal of Internet or computer access for a period.

**Community use of ICT and the internet**

The school will liaise with local organisations to establish a common approach to e-safety. The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

**September 2013**