



Joy Lane Primary School  
Joy Lane, Whitstable, Kent. CT5 4LT Tel: 01227 261430  
[www.joylane.kent.sch.uk](http://www.joylane.kent.sch.uk)

## School e - Safety Policy

Our School Policy has been agreed by the Senior Leadership Team and approved by governors.

The School e-Safety Coordinator is [Ms D Hines \(Headteacher\)](#)

Policy approved by Head Teacher: [Debra Hines](#)

Date: [February 2015](#)

Policy approved by Governing Body: ..... (Chair of Governors)

Date: .....

The date for the next policy review is: [February 2016](#)

### Teaching and Learning

#### Why is Internet use important?

- 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.

#### How does Internet use benefit education?

Benefits of using the Internet in education include:

- access to worldwide educational resources;
- 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 KCC and DCSF;
- access to learning wherever and whenever convenient.

#### How can Internet use enhance learning?

- 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.
- 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.

#### How will pupils learn how to evaluate Internet content?

- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- 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.

### Managing Information Systems

#### How will information systems security be maintained?

- 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 be 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 ICT Technician will review system capacity regularly.
- The use of user logins and passwords to access the school network will be enforced.

#### **How will email be managed?**

- Pupils may only use approved email accounts for school purposes.
- Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team.
- Access in school to external personal email accounts is not allowed.
- The forwarding of chain messages is not permitted.
- Staff should not use personal email accounts or for professional purposes.

#### **How will published content be managed?**

- The head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

#### **Can pupils' images or work be published?**

- Images or videos that include pupils will be selected carefully and will not provide material that could be reused.
- Written permission from parents or carers will be obtained before images/videos of pupils are electronically published.
- Written consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.

#### **How will social networking, social media and personal publishing be managed?**

- 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 on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- 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.

#### **How will filtering be managed?**

- The school will work with KCC and the Schools Broadband team to ensure that filtering policy is continually reviewed.
- If staff or pupils discover unsuitable sites, the URL will be reported to the ICT Technician or School e-Safety Coordinator who will then record the incident and escalate the concern as appropriate.
- Changes to the school filtering policy will be risk assessed by the headteacher.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Kent Police or CEOP.

#### **How will videoconferencing be managed?**

- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Videoconferencing contact information will not be put on the school Website.
- The equipment must be secure and if necessary locked away when not in use.

#### **Users**

- Videoconferencing will be supervised appropriately for the pupils' age and ability.
- Parents and carers consent should be obtained prior to children taking part in videoconferences.
- Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.

## **Content**

- When recording a videoconference 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.
- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non school site it is important to check that they are delivering material that is appropriate for your class.

## **How are emerging technologies managed?**

- Emerging technologies will be examined for educational benefit and an 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 Mobile Phone Policy.

## **How should personal data be protected?**

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

## **Policy Decisions**

### **How will Internet access be authorised?**

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff will read and sign the 'Staff Information Systems Code of Conduct' before using any school ICT resources.
- All visitor to the school site who require access to the schools network or internet access will be asked to read and sign an Acceptable Use Policy.
- When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

### **According to Setting Type**

- At Key Stage 1, Years 3, 4 and 5 pupils' access to the Internet will be by adult demonstration with directly supervised access to specific and approved online materials.
- Year 6 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.

### **How will risks be assessed?**

- 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. Neither the school nor KCC can accept liability for the material accessed, or any consequences resulting from Internet use.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Kent Police.

### **How will the school respond to any incidents of concern?**

- The e-Safety Coordinator will record all reported incidents and actions taken in the School e-Safety incident log and other in any relevant areas e.g. Bullying or Child protection log.
- The Designated Child Protection Coordinator will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.

### **How will e-Safety complaints be handled?**

- 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.
- Parents and pupils will need to work in partnership with the school to resolve issues.
- 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.

### **How is the Internet used across the community?**

- The school will be sensitive to Internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
- The school will provide appropriate levels of supervision for students who use the internet and technology whilst on the school site.

### **How will Cyberbullying be managed?**

- 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.
- 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.

Sanctions for those involved in cyberbullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or
- A service provider may be contacted to remove content if the bully refuses or is unable to delete content.
- Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
- Parent/carers of pupils will be informed.
- The Police will be contacted if a criminal offence is suspected.

### **How will Learning Platforms be managed?**

- Only members of the current pupil and staff community will have access to the LP.
- When staff, pupils etc. leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.
- A visitor may be invited onto the LP by a member of the SLT. In this instance there may be an agreed focus or a limited time slot.

### **How will mobile phones and personal devices be managed?**

- 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.
- Mobile phones and personal devices will not be used during lessons or formal school time. They should be switched off at all times.
- Electronic devices of all kinds are discouraged in school. The school accepts no responsibility for the loss, theft or damage of such items.

### **Pupils Use of Personal Devices**

- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.
- If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone.

### **Staff Use of Personal Devices**

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school phone where contact with pupils or parents/carers is required.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.

## **Communication Policy**

### **How will the policy be introduced to pupils?**

- All users will be informed that network and Internet use will be monitored.
- An e-Safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.
- e-Safety rules or copies of the student Acceptable Use Policy will be posted in all rooms with Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.

### **How will parents' support be enlisted?**

- Parents' attention will be drawn to the school e-Safety Policy in newsletters, the school prospectus and on the school website.
- Information and guidance for parents on e-Safety will be made available to parents in a variety of formats.

## **e-Safety Contacts and References**

**CEOP (Child Exploitation and Online Protection Centre):** [www.ceop.police.uk](http://www.ceop.police.uk)

**Childline:** [www.childline.org.uk](http://www.childline.org.uk)

**Childnet:** [www.childnet.com](http://www.childnet.com)

**Digizen:** [www.digizen.org.uk](http://www.digizen.org.uk)

**Internet Watch Foundation (IWF):** [www.iwf.org.uk](http://www.iwf.org.uk)

**Kent Police:** In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Kent Police via 01622 690690 or contact your Safer Schools Partnership Officer. Also visit [www.kent.police.uk](http://www.kent.police.uk) or [www.kent.police.uk/internetsafety](http://www.kent.police.uk/internetsafety)

**Kent Safeguarding Children Board (KSCB):** [www.kscb.org.uk](http://www.kscb.org.uk)

**Kidsmart:** [www.kidsmart.org.uk](http://www.kidsmart.org.uk)

**Think U Know website:** [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)

**Action Fraud:** <http://www.actionfraud.police.uk>

**ParentPort** (report inappropriate content): <http://www.parentport.org.uk>

**Kent County Council** (guidance and advice for Parents/carers) [www.kent.gov.uk/esafety](http://www.kent.gov.uk/esafety)