Paddock Wood Primary School

e-Safety Policy

April 2019

e-Safety Policy

Introduction

Our e–Safety Policy has been written by the school, building on the KCC e–Safety Policy and government guidance.

The school e-Safety co-ordinators are Carly Gavin and Charlotte Gunning.

Teaching and Learning

- 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.

How Does Internet Use Benefit Education?

Benefits of using the Internet in education include:

- Access to worldwide educational resources including museums and art galleries;
- Inclusion in the National Education Network which connects all UK schools;
- 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 KCC and DfE;
- 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.
- 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.

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.

How Will Information Systems Security be Maintained?

Local Area Network (LAN) Security:

- Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use. For KCC staff, flouting electronic use policy is regarded as a reason for dismissal.
- Workstations should be secured against user mistakes and deliberate actions.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date.
- Virus protection for the whole network must be installed and current.
- Access by wireless devices must be proactively managed and secured with a minimum of WPA2 encryption.

Wide Area Network (WAN) Security:

- Central KPSN Schools Broadband firewalls and local CPEs are configured to prevent unauthorised access between schools.
- Decisions on WAN security are made on a partnership between schools and KCC/EiS.
- The Schools Broadband network is protected by a cluster of high performance firewalls at the Internet connecting nodes in Maidstone and Canterbury. These industry leading appliances are monitored and maintained by a specialist security command centre.
- 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 ICT Network Manager 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.
- 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.
- Whole -class or group email addresses will be used for communication outside of the school.
- Staff will only use official school provided email accounts to communicate with parents/carers, as approved by the Senior Leadership Team.
- 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.
- The forwarding of chain messages is not permitted.

How Will Published Content be Managed?

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.
- 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.
- 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 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.
- The School will have a policy regarding the use of photographic images of children which outlines policies and procedures.

How Will Social Networking, Social Media and Personal Publishing be Managed?

- The school will control access to social media and social networking sites.
- 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.
- Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.
- Staff official blogs or wikis should be password protected and run from the school website with approval from the Senior Leadership Team. Members of staff are advised not to run social network spaces for pupil use on a personal basis.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- 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.
- 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.
- Newsgroups will be blocked unless a specific use is approved.

- 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 Acceptable Use Policy.
- All staff, pupils, volunteers and governors will be required to sign an Acceptable Use Consent Form.

How Will Filtering be Managed?

- School's broadband access will include filtering appropriate to the age and maturity of pupils.
- 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.
- The School Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Kent Police or CEOP.
- The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from the network manager.

How Are Emerging Technologies Managed?

- 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 Acceptable Use Policy.

How Should Personal Data be Protected?

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

How Will Internet Access be Authorised?

- All staff and pupils will read and sign the School Acceptable Use Policy before using any school ICT resources.
- Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child before signing.
- 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.
- Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.
- 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).
- At Key Stage 1 pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials.
- At Key Stage 2 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 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.
- 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.
- Methods to identify, assess and minimise risks will be reviewed regularly.

How Will The School Respond to Any 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 e-Safety Coordinator will record all reported incidents and actions taken.
- 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 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.
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Area Children's Officer or the County e-Safety Officer.
- If an incident of concern needs to be passed beyond the school then the concern will be escalated to the e-Safety officer to communicate to other school in Kent.

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 headteacher.
- All e–Safety complaints and incidents will be recorded by the school, including any actions taken.
- Pupils and parents will be informed of the complaints procedure.
- 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 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.

How Will Cyberbullying be Managed?

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated.
- All incidents of cyberbullying reported to the school will be recorded.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- 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.
- The Police will be contacted if a criminal offence is suspected.

How Will Learning Platforms be Managed?

- SLT and staff will regularly monitor the usage of the LP by pupils and staff in all areas, in particular message and communication tools and publishing facilities.
- Pupils/staff will be advised about acceptable conduct and use when using the LP.
- Only members of the current pupil, parent/carers and staff community will have access to the LP.
- All users will be mindful of copyright issues and will only upload appropriate content onto 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.
- Any concerns about content on the LP may be recorded.

How Will Mobile Phones and Personal Devices be Managed?

- Pupils' mobile phones and personal devices will not be used during lessons or formal school time. They should be switched off and handed to the school office for safe keeping at the beginning of the day.

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.
- Pupil instruction regarding responsible and safe use will precede Internet access.
- An e–Safety module will be included in the PSHE, Citizenship and/or ICT programmes covering both safe school and home use.
- 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.

How Will the Policy be Discussed with Staff?

- The e–Safety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff and pupils, the school will implement an Acceptable Use Policy.
- 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.

- The School will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils.
- 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.

How Will Parents' Support be Enlisted?

- Parents' attention will be drawn to the school e–Safety Policy in newsletters and on the school website.
- A partnership approach to e-Safety at home and at school with parents will be encouraged, including offering parent evenings with demonstrations and suggestions for safe home Internet use.
- Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss it's implications with their children.
- Information and guidance for parents on e–Safety will be made available to parents in a variety of formats.

Review of Policy

The Governing Body will ensure the policy is reviewed annually.

The policy may be revised at other times if necessary to take account of any statutory regulation or associated guidance or changes in policy by Kent County Council's policy.

Issue Date: April 2019 Review Date: April 2020