The Orchard School

E-Safety Policy

Draft: June 2017

Ratified:

Review:

Chair of Governors:

Headteacher :

DRAFT
06/17

The Orchard School
E-Safety Acceptable Use Policy

Who will write and review the policy?

- Our e–Safety Policy has been written by the school, building on the KCC e–Safety Policy and government guidance.
- The e-Safety Policy and its implementation will be reviewed annually.
- Our School Policy has been agreed by the Senior Leadership Team and approved by governors.

Why is Internet use important?

- Internet use is part of the statutory curriculum and 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.

How does Internet use benefit education?

- Vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for pupils and staff;
- Improved access to technical support including remote management of networks and automatic system updates;
- Access to learning wherever and whenever convenient.
- Access to world-wide educational resources including museums and art galleries;

How can Internet use enhance learning?

- The school Internet access will be designed to enhance and extend education.
- 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 be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Staff should guide pupils to on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

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.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.
- Pupils will use age-appropriate tools to research Internet content.

How will information systems security be maintained?

- Virus protection will be updated regularly.
- The security of the school information systems and users will be reviewed regularly.
- Unapproved software will not be allowed in pupils' work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The ICT Manager will review system capacity regularly.
- The use of user logins and passwords to access the school network will be enforced.

How will e-mail be managed?

- Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team.
- 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.
- 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 school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

Can pupil's 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.
- Pupils work can only be published with their permission or their parents/carers.

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.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- 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 have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.
- If staff or pupils discover unsuitable sites, the URL will be reported to the School ICT Manager who will then record the incident and escalate the concern as appropriate.
- Any material that the school believes is illegal must be reported to appropriate agencies such as Kent Police, the IWF or CEOP.
- The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.

How can emerging technologies be managed?

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

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 will read and sign the School Acceptable Use Policy before using any school ICT resources.
- 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.
- Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.

- 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).

How will risks be assessed?

- 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.
- 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.

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 ICT Manager 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 Safeguarding Lead 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 Social & Emotional Behaviour Support 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, identify lessons learnt and implement any changes required.
- 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.

How will e-safety complaints be handled?

- Complaints of Internet misuse will be dealt with under the School's Complaints Procedure.
- Any complaint about staff misuse will be referred to the Headteacher.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.
- 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.

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 whilst using the internet and technology on the school site.
- The school will provide an Acceptable Use Policy for any guest who needs to access the school computer system or internet on 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 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: a) The bully will be asked to remove any material deemed to be inappropriate; b) A service provider may be contacted to remove content if the bully refuses or is unable to delete content; c) 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; d) Parent/carers of pupils will be informed; e) The Police will be contacted if a criminal offence is suspected.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.

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 Acceptable Use Policy.
- Parents / carers are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.
- School staff may confiscate a phone or device if they believe it is being used to contravene the schools behaviour or bullying policy. The phone or device might be searched by the Senior Leadership team with the consent of the pupil or parent/carer. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.
- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- Phones and devices must not be taken into examinations. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.

- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.
- 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.
- Members of staff are advised that personal mobile phones and devices must be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Senior Leadership Team.
- 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.

How will the policy be introduced to pupils?

- e-Safety rules or copies of the student Acceptable Use Policy will be posted in all rooms with Internet access.
- All users will be informed that network and Internet use may be monitored.
- 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 Acceptable Use Policies.
- 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?

- A partnership approach to e-Safety at home and at school with parents will be encouraged. This may include offering suggestions for safe home Internet use, or highlighting e–Safety at attended events e.g. parent evenings.
- Parents' attention will be drawn to the school e–Safety Policy in newsletters, the school prospectus and on the school website.
- Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.