SWALE ACADEMIES TRUST

E-Safety Policy

Our e–Safety Policy has been written by the trust safeguarding team building on the KCC e–Safety Policy and government guidance. The policy has links to the safeguarding policy and the use of cameras and images policy.

Each school/college within the Trust has appointed an appointed an e–Safety Coordinator:

The e-Safety Coordinator for Regis Manor Primary School

is……

The e-Safety Coordinator for Sittingbourne Community College

is ……

The e-Safety Coordinator for Westlands Primary School

is……

The e-Safety Coordinator for Westlands Secondary School

is……

The e-Safety Coordinator for Meopham Secondary School

Is ……

The e–Safety Policy and its implementation will be reviewed annually.

Why is Internet use important?

- The purpose of Internet use in school/college is to raise educational standards, to promote pupil/student achievement, to support the professional work of staff and to enhance the school's/college's management functions

- 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/college has a duty to provide pupils/students with quality Internet access as part of their learning experience

- Pupils/students 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 can Internet use enhance learning?

- The school/college Internet access will be designed to enhance and extend education

- The schools/college will ensure that the copying and subsequent use of Internet derived materials by staff and pupils/students complies with copyright law

- Pupils/students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use

- Access levels will be reviewed to reflect the curriculum requirements and age of pupils/students

- Staff should guide pupils/students to on-line activities that will support the learning outcomes planned for the pupils'/students' age and maturity

- Pupils/students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

- The schools/college will ensure that the copying and subsequent use of Internet derived materials by staff and pupils/students complies with copyright law

How will pupils/students learn how to evaluate Internet content?

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

- Pupils/students 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/college information systems and users will be reviewed regularly

- Personal data sent over the Internet or taken off site will be encrypted
- The ICT co-ordinator / network manager will review system capacity regularly
- The use of user logins and passwords to access the school/college network will be enforced
- All software must be approved by the ICT coordinator or network manager before use on any device

How will e-mail be managed?

- Staff will only use official school/college provided email accounts to communicate with pupils/students and parents/carers, as approved by the Senior Leadership Team
- Pupils/students will be taught to tell a designated member of staff if they receive offensive electronic communication
- Pupils/students will be taught not to reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult
- Pupils/students and staff may only use approved email accounts for school/college purposes and will be made aware that these are monitored and can be accessed by members of the school leadership team
- Access in school to external personal e-mail accounts will be blocked

How will published content be managed?

- The contact details on the website should be the school/college address, email and telephone number. Staff contact will be by official school email only. Staff or pupils' personal information must not be published
- The school/college website will comply with the school's/college's guidelines for publications including respect for intellectual property rights, privacy policies and copyright

Can pupils'/students' images or work be published?

- Pupils'/students full names will not be used anywhere on the website, particularly in association with photographs, unless parental permission has been obtained
- Written permission from parents or carers will be obtained before images/videos of pupils/students are electronically published
- Pupils'/students' work can only be published with their permission or their parents/carers

- Written consent will be kept by the school where pupils'/students' images are used for publicity purposes, until the image is no longer in use

- The school/college 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/college will control access to social media and social networking sites

- Pupils/students 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/students will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private

- Staff wishing to use Social Media tools with pupils/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

- All members of the school/college community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory

- If staff have concerns regarding pupils'/students' use of social networking, social media and personal publishing sites (in or out of school) the issue will be raised with their parents/carers by relevant staff

- Pupils/students 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, date of birth, address, mobile or landline phone numbers, school/college attended, IM and email addresses, full names of friends/family, specific interests and clubs

- 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/College Acceptable Use Agreement

How will filtering be managed?

- The school/college will work with KCC and the Schools Broadband team to ensure that filtering policy is continually reviewed

- The school/college will have a clear procedure for reporting breaches of filtering. All members of the school/college community (all staff and all pupils) will be aware of this procedure

- The school's broadband access will include filtering appropriate to the age and maturity of pupils/students.

- The school/college filtering system will block all sites on the Internet Watch Foundation (IWF) list

- If staff or pupils/students discover unsuitable sites, the URL will be reported to a designated member of staff who will then record the incident and escalate the concern as appropriate

How will video conferencing be managed?

- Pupils/students will ask permission from a teacher before making or answering a video conference call

The equipment and network

- All video conferencing equipment in the classroom must be switched off when not in use and not set to auto answer

Users

- Parents and carers consent should be obtained prior to children taking part in video conferences

Content

- Video conferencing will be supervised appropriately for the pupils'/students' age and ability.

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/college 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?

- The school/college will maintain a current record of all staff and pupils/students who are granted access to the school's/college's electronic communications

- 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

- All staff will read and sign the School Acceptable Use Agreement before using any school/college ICT resources

- At Key Stage 1 pupils' access to the Internet will be by adult demonstration with supervised access to specific and approved online materials

- Secondary pupils/students will apply for Internet access individually by agreeing to comply with the school/college e–Safety Rules or Acceptable Use Agreement

- The school/college will maintain a current record of all staff and pupils/students who are granted access to the school's/college's electronic systems

How will risks be assessed?

- The school/college 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 school/college 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/college computer. Neither the school/college 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/college community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyber bullying, 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/college will manage e-Safety incidents in accordance with the school/college discipline/behaviour policy where appropriate

- The school/college will inform parents/carers of any incidents of concerns as and when required

- After any investigations are completed, the school/college will debrief, identify lessons learnt and implement any changes required

How will e-safety complaints be handled?

- Complaints of Internet misuse will be dealt with under the Trust's Complaints Procedure

- Any complaint about staff misuse will be referred to the Head of School

- All e–Safety complaints and incidents will be recorded by the school/college, including any actions taken

- All members of the school/college 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/college community

- All members of the school/college community will need to be aware of the importance of confidentiality and the need to follow the official school/college procedures for reporting concerns

How is the Internet used across the community?

- The school/college will be sensitive to Internet related issues experienced by pupils/students out of school, e.g. social networking sites, and offer appropriate advice

- The school/college will provide appropriate levels of supervision for pupils/students whilst using the internet and technology on the school/college site

- The school/college will provide an Acceptable Use Policy for any guest who needs to access the school/college computer system or internet on site

How will Cyber bullying be managed?

- Cyber bullying (along with all other forms of bullying) of any member of the school/college community will not be tolerated. Full details are set out in the school's/college's policy on anti-bullying and behaviour

- There are clear procedures in place to support anyone in the school/college community affected by cyber bullying

- All incidents of cyber bullying reported to the school/college will be recorded

- There will be clear procedures in place to investigate incidents or allegations of Cyber bullying

How will Learning Platforms and Learning Environments be managed?

- Only members of the current pupil/student, parent/carers and staff community will have access to any learning platforms

- When staff and pupils/students leave the school/college their account or rights to specific school/college areas will be disabled or transferred to their new establishment

How will mobile phones and personal devices be managed?

- The use of mobile phones and other personal devices by pupils/students and staff in school/college will be decided by the school/college and covered in the school/college Acceptable Use or Mobile Phone Policies

- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school/college community and any breaches will be dealt with as part of the school/college discipline/behaviour policy

- School/college staff may confiscate a phone or device if they believe it is being used to contravene the school's/college's behaviour or bullying policy. The phone or device might be searched by the Senior Leadership team with the consent of the pupil/student 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 relevant authority for further investigation.

- Electronic devices of all kinds that are brought in to school/college are the responsibility of the user. The school/college accepts no responsibility for the loss, theft or damage of such items. Nor will the school/college accept responsibility for any adverse health effects caused by any such devices either potential or actual.

How will the policy be introduced to pupils?

- An e–Safety training programme will be established across the school/college to raise the awareness and importance of safe and responsible internet use amongst pupils/students

- All users will be informed that network and Internet use will be monitored

How will the policy be discussed with staff?

- 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

- All members of staff will be made aware that their online conduct out of school/college could have an impact on their role and reputation within school/college. 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

- To protect all staff and pupils/students, the school/college will implement Acceptable Use Agreements

How will parents' support be enlisted?

- Parents' attention will be drawn to the school/college e–Safety Policy in newsletters and on the school/college website.

Approved by Directors July 2013/V02