Highsted Grammar School

Online Safeguarding Policy

ONLINE SAFEGUARDING

Statement of intent

Highsted Grammar School believes that the use of information and communication technologies in schools brings great benefits. The school is proactive in recognising online safeguarding issues and make use of effective strategies to ensure appropriate, effective and safer use of electronic communications.

Who will write and review the policy?

The online safeguarding Policy and its implementation will be reviewed annually. The school has appointed a Designated Online Safeguarding Lead.

The Designated Online Safeguarding Lead for 2016-2017 is: Mr Daniel Quinn (DSL)

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 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. The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

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.

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 Group. Staff should not use personal email accounts during school hours or for professional purposes. 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. E-mail 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 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. Respect for intellectual property rights, privacy policies and copyright.

Can pupil's images or work be published?

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. Staff must seek guidance from the Designated Online Safeguarding Lead/IT Manager prior to allowing students to publish to external websites to ensure online safeguarding and that Terms and Conditions are fully read and understood

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

The school will filter / block access to 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. 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. 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.

How will filtering be managed?

The school will work with KCC and the Schools Broadband team to ensure that filtering policy is continually reviewed. 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 online safeguarding Lead who will then record the incident and escalate the concern as appropriate. The School Senior Leadership Group will ensure that regular checks are made to ensure that the filtering methods selected are effective. Any material that the school believes is illegal must be reported to appropriate agencies such as Kent Police 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. Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership group.

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. 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?

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' or School Acceptable Use Policy before using any school ICT resources. Secondary students will apply for Internet access individually by agreeing to comply with the School Online Safeguarding Rules or Acceptable Use Policy. All visitors 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.

How will risks be assessed?

The school will audit ICT use to establish if the online safeguarding policy is adequate and that the implementation of the online safeguarding 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. 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 online safeguarding concerns (such as breaches of filtering, cyberbullying, illegal content etc). The online safeguarding Lead will record all reported incidents and actions taken in the School online safeguarding incident log and other in any relevant areas e.g. Bullying or Child protection log.
The Designated Safeguarding lead will be informed of any online safeguarding incidents involving Child Protection concerns, which will then be escalated appropriately. The school will manage online safeguarding incidents in accordance with the school discipline/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, identify 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 online safeguarding 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 to KCC's e-safety officer (Rebecca Avery). If an incident of concern needs to be passed beyond the school then the concern will be escalated to the online safeguarding officer to communicate to other schools in Kent.

How will online safeguarding 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. Parents and pupils will need to work in partnership with the school to resolve issues. 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.

How is the Internet used across the community?

The school will liaise with local organisations to establish a common approach to online safeguarding.

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. There are clear procedures in place to support anyone in the school community affected by cyberbullying. 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. There will be clear procedures in place to investigate incidents or allegations of Cyberbullying. Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.

How will Learning Platforms and Learning Environments be managed?

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.

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. 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. Mobile phones and personal devices will not be used during lessons or formal school time. They should be switched off at all times. Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from a member of staff. 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. Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms, toilets and swimming pools. 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. 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. If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office. 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. 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?

An online safeguarding training programme, created by Childnet, 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 online safeguarding module, created by The South West Grid for Learning, will be included in all PSHCEE focus days, Citizenship activities and computing curriculum covering both safe school and home use. All users will be informed that network and internet use will be monitored.

How will the policy be discussed with staff?

The online safeguarding 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. Staff who manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Group and have clear procedures for reporting issues. 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. To protect all staff and pupils, the school will implement Acceptable Use Policies. 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 online safeguarding Policy in newsletters, the school prospectus and on the school website. Information and guidance for parents related to online safeguarding will be made available to parents in a variety of formats.

Policy Date

July 2015
Reviewed July 2016