E-SAFETY POLICY

Written by:	DQ October 2017
Revised by:	JM June 2018
Reviewed by:	BM, SS, MW, JP, EC, MS
Applicable to:	All Staff and members of resident boarding staff households.
For review:	June 2019

This policy applies to Slindon College day school and Boarding House and forms part of the safeguarding regime and should therefore be read in conjunction with the Safeguarding policy, a copy of which is available on the Slindon College website. A hard copy is also available on request.

It is our duty to ensure that every boy in our care is safe and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people. New technologies are continually enhancing communication, the sharing of information and learning, social interaction and leisure activities. Current and emerging technologies include:

- instant messaging and snapchat;
- blogs;
- social networking sites;
- websites;
- email;
- chat rooms;
- music/video downloads;
- gaming sites;
- text messaging and picture messaging;
- video calls;
- podcasting;
- online communities via games consoles; and
- mobile internet devices such as tablets, smart phones and watches.

Whilst exciting and beneficial, both in and out of the context of education, these platforms are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

This policy outlines how we ensure our pupils stay safe in the online environment and how they can mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, abuse and radicalisation.

MONITORING

We have appropriate filters and monitoring systems in place to keep children safe online, these are managed and monitored by the IT Manager – Mr Steve Smart. The systems we use are Open DNS and Smoothwall. Such systems aim to reduce the risk of children being exposed to illegal, inappropriate and harmful materials online, including terrorist and extremist material. They also aim to reduce the risk of children being subjected to harmful online interaction with others and help manage online behaviour that can increase a child's likelihood of, or cause harm.

E-S AFETY IN THE CURRICULUM

IT and online resources are used increasingly across the curriculum. We believe it is essential for e-safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety and monitor and assess our pupils' understanding of it.

We provide opportunities to teach about e-safety within a range of curriculum areas and IT lessons. Educating pupils on the dangers of technologies that may be encountered outside College will also be carried out via IT lessons, PSHE, the tutor programme, in assemblies, as well as informally when opportunities arise.

At age-appropriate levels, pupils are taught about their e-safety responsibilities and to look after their own online safety. From Key stage 2, pupils are taught about recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. Pupils can report concerns to the DSL, the Deputy DSLs or any member of staff at the College.

From Keys stage 3, students are also taught about relevant laws applicable to using the internet, such as data protection and intellectual property. Students are taught about respecting other people's information and images through discussion and classroom activities.

Boys should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues. Please see the College's Anti-bullying Policy, which describes the preventative measures and the procedures that will be followed when the College discovers cases of bullying. A copy of this policy is available on the Slindon College website and a hard copy is available on request. Pupils should approach the DSL, Deputy DSLs, the Network Manager as well as parents, peers and other College staff for advice or help if they experience problems when using the internet and related technologies.

RULES FOR BOYS

- All children are issued with their own logins and personal email addresses. They are reminded of the need for password security, including using a strong password (usually containing eight characters or more and containing upper and lower case letters as well as numbers). They must not write passwords down and they must not share passwords with others.

- There is strong anti-virus and firewall protection on our network. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for College purposes, boys should contact the Network Manager for assistance.

- Pupils and students must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication to the DSL, Deputy DSLs or any other member of staff.

- The College expects boys to think carefully before they post any information online, or repost or endorse content created by other people. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others.

- Boys must report any accidental access to materials of a violent or sexual nature directly to the Network Manager or another member of staff.

- Deliberate access to any inappropriate materials by a pupil will lead to the incident being recorded on their file and will be dealt with under the College's Behaviour Management and Exclusion Policy.

- Boys must let the Network Manager or another member of staff know if they see any IT systems being misused.

SUPERVISION OF PUPILS

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms. When children use College computers, staff should make sure children are fully aware of the agreement they are making to follow the College's IT guidelines.

Staff should ensure that pupils are supervised as much as is practicable during IT lessons/sessions. Monitoring software is available in the IT suites and training is available; in any event staff should be vigilant. Pupils should not be sent to use a computer where there is no staff supervision.

If a pupil or student is caught misusing the computers, the normal disciplinary procedures should be followed as detailed in the Behaviour Management and Exclusion policy, a copy of which is on the Slindon College website. The Network Manager and DSL must be contacted as soon as possible if any incident relating to e-safety occurs.

SAFE USE OF DIGITAL AND VIDEO IMAGES

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or have downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with

publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate pupils and students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet (e.g. on social networking sites).

Boys must not take, use, share, publish or distribute images of others without consent.

MISUSE

We will not tolerate illegal activities or activities that are inappropriate in a College context, and will report illegal activity to the police and/or the Local Children's Safeguarding Board.

Incidents of misuse or suspected misuse will be dealt with by staff in accordance with the College's Behaviour Management and Exclusion policy, a copy of which is available on the Slindon College website.

DISPLAY SCREEN POLICY

Although students do not spend most of their College day working with computers, they spend increasing amounts of their private study and leisure time with screens. They are provided with guidance on posture, simple exercises to help circulation and to combat fatigue and on the need to take regular, short breaks from the screen as part of IT.

TRAINING FOR STAFF

All staff are required to familiarise themselves with this policy and ensure they are implemented and followed by all pupils.

All staff are required to take online e-safety training through Educare, to ensure they are equipped with the knowledge to safeguard children online.

PARENTS/CARERS

We seek to work closely with parents and guardians in promoting a culture of e-safety. We will always contact parents if we have any concerns about pupils' behaviour in this area and likewise we hope that parents will feel able to share any concerns with the College.

COMPLAINTS

As with all issues of safety at Slindon College, if a member of staff, child or a parent has a complaint or concern relating to e-safety, prompt action will be taken to deal with it. Please see the Complaints

Procedure which can be found on the Slindon College website.

Monitoring by:	Head Teacher Deputy Head Teacher Bursar IT Manager
Evidenced by:	Speaking to Pupils and students Speaking to staff
Policies are subject to continuous monitoring, refinement and audit by SLT. The Chairman of Governors undertakes an annual review of policies and of the efficiency with which the related duties have been discharged by the date stated or earlier if changes in legislation, regulatory requirements or best practice guidelines so require.	