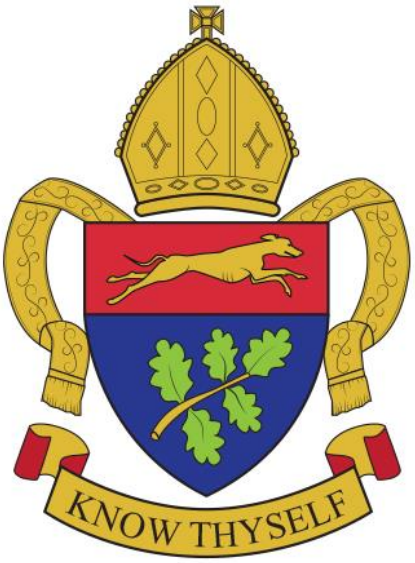

SLINDON
COLLEGE

E-SAFETY POLICY

Last review:	September 2023
Next review:	September 2024
Prepared by:	Chris Relf, ICT Teacher Emily Coffey, Assistant Head (DSL)
Approved by:	Governing Body

It is the duty of Slindon College to ensure that every pupil in its 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. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, abuse and radicalisation.

This policy, supported by the Acceptable Use Policy (for all staff, visitors and pupils), is implemented to protect the interests and safety of the whole College community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following College policies:

- Safeguarding and Child Protection
- Staff Code of Conduct and Expected Behaviours
- Health and Safety
- Behaviour Management
- Anti-Bullying
- Acceptable Use Policy
- Data Protection
- PSHE

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

At Slindon College we understand the responsibility to educate our pupils on E-safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving pupils in discussions about E-safety and listening to their fears and anxieties as well as their thoughts and ideas.

Scope of this Policy

This policy applies to all members of the College community, including staff, pupils, parents and visitors, who have access to and are users of the College IT systems. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers. 'Parents' includes pupils' carers and guardians. 'Visitors' includes anyone else who comes to the College, including occasional volunteers.

Both this policy and the Acceptable Use Policy (for all staff, visitors and pupils) cover both fixed and mobile internet devices provided by the College (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by pupils, staff, or visitors and brought onto College premises (personal laptops, tablets, smart phones, etc.).

Roles and responsibilities

1. The Governing Body

The governing body of the College is responsible for the approval of this policy and for reviewing its effectiveness regularly

2. Headteacher and the Senior Leadership Team

The Headteacher is responsible for the safety of the members of the College community and this includes responsibility for E-safety. The responsibility for E-safety is also the responsibility of the ICT Network Manager; DSL and ICT teacher. The role of the Headteacher and the Senior Leadership team is to ensure that:

- this policy is upheld by all members of the College community, and works with ICT Teacher to achieve this
- staff are adequately trained about e-safety
- staff are aware of the College procedures and policies that should be followed in the event of the abuse or suspected breach of E-safety in connection to the College.
- Serious breaches of the Acceptable Use Policy are addressed immediately and rectified according to the school's policy

3. ICT Network Manager

The College's ICT Network Manager is responsible for ensuring that the network is safe this includes:

- Ensuring that Firewall software is installed and up to date.
- Addressing an breeches and notifying the Head
- Setting the correct level of internet and data access for all staff and pupils
- Blocking any inappropriate sites that may have bypassed the firewall
- They are responsible for the security of the College's hardware system

4. DSL

- Monitor the daily Smoothwall reports detailing internet searches made by pupils which are of concern. The DSL will either ask the pupil's HOH to have an informal chat with the pupil; speak directly to the pupil and ask the Network manager to screen all of the pupil's searches that day/week. If necessary make a referral to MASH/Prevent/CAMHS
- Ensure that E-safety is in line with KCSIE
- Will identify areas of concern or weakness in the E-safety and work with the Network Manager and ICT teacher to find solutions
- will keep up to date on current e-safety issues and guidance issued by relevant organisations, including the ISI, the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International and the West Sussex Safeguarding Children's Service

5. ICT Teacher

- Embed E-Safety into the ICT curriculum
- Ensure that E-safety lessons are updated at annually in line with KCSIE and developing technologies/applications/internet usage and trends
- Create resources and presentation for staff training and parent conference
- will keep up to date on current e-safety issues and guidance issued by relevant organisations, including the ISI, the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International and the West Sussex Safeguarding Children's Service

6. Teaching and support staff

- All staff are required to sign the Acceptable Use Policy before accessing the College's systems.
- Monitoring pupil internet use during lessons

- As with all issues of safety at this College, staff are trained to respond to any e-safety issues which may arise in classrooms on a daily basis by reporting to the DSL

7. Pupils

- Pupils are responsible for using the College ICT systems in accordance with the Acceptable Use Policy, and for letting staff know if they see ICT systems being misused.

8. Parents and carers

- Parents and carers are responsible for endorsing the College's Acceptable Use Policy.
- Slindon College believes that it is essential for parents to be fully involved with promoting e-safety both in and outside of College. The College will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the College.
- We consult and discuss E-safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage.

Education and training

1. Staff: awareness and training

New staff receive information on Slindon College's E-Safety and Acceptable Use policies as part of their induction.

All staff receive regular information and training on E-safety issues in the form of INSET training and internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of E-safety.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following College E-Safety procedures. These behaviours are summarised in the Acceptable Use Policy which must be signed and returned before use of technologies in College. When children use College computers, staff should make sure children are fully aware of the agreement they are making to follow the College's ICT guidelines.

Teaching staff are encouraged to incorporate E-safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the College community.

A safeguarding concern must be completed by staff as soon as possible if any incident relating to E-safety occurs and be provided directly to the Designated Safeguarding Lead.

2. Pupils: E-Safety in the curriculum

ICT 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 regularly monitor and assess our pupils' understanding of it.

The College provides opportunities to teach about E-safety within a range of curriculum areas and ICT lessons. Educating pupils on the dangers of technologies that may be encountered outside College will also be carried out via PSHE, by presentations in assemblies, as well as informally when opportunities arise.

At age-appropriate levels, and usually via PSHE, pupils are taught about their E-safety responsibilities and to look after their own online safety. Year 7, pupils are formally / informally 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 any member of staff at the College who will pass it on to the DSL.

Year 9, pupils are also taught about relevant laws applicable to using the internet; such as data protection and intellectual property. Pupils are taught about respecting other people's information and images (etc.) through discussion and classroom activities.

Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also 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). Pupils should approach Safeguarding Lead or Head of House as well as parents, peers and other College staff for advice or help if they experience problems when using the internet and related technologies.

3. Parents

The College seeks to work closely with parents and guardians in promoting a culture of e-safety. The College will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the College.

The College recognises that not all parents and guardians may feel equipped to protect their son when they use electronic equipment at home. The College therefore hosts an annual parents' conference where the ICT teacher and DSL present on E-safety and the practical steps that parents can take to minimise the potential dangers to their sons without curbing their natural enthusiasm and curiosity. E-safety is also promoted via literature sent to parents via the school portal.

Policy Statements

1. Use of College and personal devices

Staff

College devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. Staff should only use the College device which is allocated to them for College work. When they are not using a device staff should ensure that it is locked to prevent unauthorised access. Devices issued to staff are encrypted, to protect data stored on them.

Staff at Slindon College are permitted to bring in personal devices for their own use. Staff, with the exception of the SLT and HoH, are not allowed to use their personal devices during the working day. They may use such devices in the main College staff room only during break-times and lunchtimes.

Personal telephone numbers, email addresses, or other contact details may not be shared with pupils or parents / carers and under no circumstances may staff contact a pupil or parent / carer using a personal telephone number, email address, social media, or other messaging system.

Day Pupils

If pupils bring in mobile devices (e.g. for use during the journey to and from College), they should be kept switched off and handed to their Head of House for safekeeping and collected at the end of the day. Pupils bringing in devices do so at their own risk and are responsible for any loss or damage. These requirements apply to phones and all devices that communicate over the internet, including smartwatches and other wearable technology.

College mobile technologies available for pupil use including laptops, tablets, cameras are available in classrooms during lesson time. Access is available via the subject teacher/designated LSA. Members of staff should check that all devices are handed after each use by a pupil.

The College recognises that mobile devices are sometimes used by pupils for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs. Where a pupil needs to use a mobile device for such purposes, the pupil's parents or carers should arrange a meeting with the appropriate person e.g. the SENCO or Head of House to agree how the College can appropriately support such use. The information will then be communicated to the pupil's teachers and other relevant members of staff about how the pupil will use the device at College.

Boarders

Boarders must leave all personal portable devices in their respective Houses during the College day.

ICT and internet provision is usually in 5a or the ICT room. The computers are available for general use by all boarders. We also have wireless internet access across the whole boarding house. All ICT activities are both monitored and filtered daily and checked by the DSL and HoHs. The WIFI facility is switched off at the appropriate bed times.

A Devices Register is kept and maintained for any boarders including flexi and taster boarders. The boarder will need to give their list of devices, the model and their WIFI Mac addresses. Any undeclared devices will not be able to access the network.

Parents are requested to set up appropriate parental controls on their pupils' devices. Please note that if this is not in place, the Head of Boarding may be in contact to do this in loco parentis. Please be advised, it is possible to contact your mobile phone provider to ensure the number is restricted from reaching sites with adult content.

Additionally, parents are requested to set up suitable parental controls on all streaming accounts (Netflix, Disney+ etc.) and ensure their son does not know the main account password.

Under no circumstances should any boarder be given or use the Guest network password. If it is suspected any pupil has this password it will be changed.

Pupils are advised that spot checking devices may occur. This is because inappropriate content could be downloaded at home or in 4G to view offline.

2. Use of internet and email

Staff

Staff must not access social networking sites, personal email, any website or personal email which is unconnected with College work or business from College devices or whilst teaching / in front of pupils. Such access may only be made from staff members' own devices whilst in the staff room staff-only areas of College.

When accessed from staff members' own devices / off College premises, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the College.

The College has taken all reasonable steps to ensure that the College network is safe and secure. Staff should be aware that email communications through the College network and staff email addresses are monitored.

Staff must immediately report to the DSL and/or Headteacher, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to the Network Manager

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm, or cause actual harm;
- bring Slindon College into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
    - using social media to bully another individual; or
    - posting links to or endorsing material which is discriminatory or offensive.

Under no circumstances should College pupils or parents be added as social network 'friends' or contacted through social media.

Any digital communication between staff and pupils or parents / carers must be professional in tone and content. Under no circumstances may staff contact a

pupil or parent / carer using any personal email address. The College ensures that staff have access to their work email address when offsite, for use as necessary on College business.

Pupils

Firewall and internet searches:

There is strong antivirus and firewall protection on our network. Websites containing unsafe/age inappropriate content are blocked. Pupil's internet searches are monitored via the Smoothwall and a daily report of any potentially dangerous searches is sent to the SLT and HoH. Inappropriate or harmful internet searches are discussed with the pupil and may be managed using the behaviour management policy or followed up by the DSL if deemed a safeguarding concern.

Pupils must report any accidental access to materials of a violent or sexual nature directly to a 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 Policy. Pupils should be aware that all internet usage via the College's systems and its Wi-Fi network is monitored.

Emails:

All pupils are issued with their own personal College email addresses for use on our network. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure, and must be used for all College work, assignments/research/projects. Pupils should be aware that email communications through the College network and College email addresses are monitored.

Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for College work/research purposes, pupils should contact the Network Manager for assistance.

Pupils should 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 a member of staff.

Social Media:

The College expects pupils 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.

3. Data storage and processing

The College takes its compliance with the Data Protection Act 1998 seriously. Please refer to the Data Protection Policy and the Acceptable Use Policy for further details.

Staff and pupils are expected to save all data relating to their work to their College laptop/ PC or to the College's central server/Google Drive Account as per the ICT Policy.

Staff devices should be encrypted if any data or passwords are stored on them. The College expects all removable media (USB memory sticks, CDs, portable drives) taken outside College or sent by post or courier to be encrypted before sending.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or pupils should be stored on personal memory sticks, but instead stored on an encrypted USB memory stick provided by College.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Network Manager and Headteacher.

4. Password security

Pupils and staff have individual College network logins, email addresses and storage folders on the server. Staff and pupils are regularly reminded of the need for password security.

All pupils and members of staff should:

- use a strong password (usually containing eight characters or more, and containing upper and lower case letters as well as numbers), which should be changed every [6] months;
- not write passwords down; and
- not share passwords with other pupils or staff.

5. 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 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 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).

Parents/carers are not permitted to take photographs or videos of pupils. The school will take photos when there is a school event. This is to respect everyone's privacy and in some cases protection.

Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow this policy and the Acceptable Use Policy ICT Policy concerning the sharing, distribution and publication of those images. Images should be taken on College equipment. However, on the rare occasion that personal equipment is used, for example on a school trip, the photos must be sent to the school Marketing Administrator as soon as possible and deleted from the member of staff’s device. Care should be taken when taking digital /

video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the College into disrepute.

Pupils must not take, use, share, publish or distribute images of others.

Written permission from parents or carers will be obtained before photographs of pupils are published on the College website (see Parent Contract/Acceptable Use Policy for more information).

Photographs published on the College website, or displayed elsewhere, that include pupils, will be selected carefully and will comply with good practice guidance on the use of such images. Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

6. Misuse

Slindon College 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 IFD. If the College discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the CEOP. If relevant, include the College's guidance on particular activities that would be illegal or classed as inappropriate and therefore restricted.

Incidents of misuse or suspected misuse must be dealt with by staff in accordance with the College's policies and procedures (in particular the Safeguarding Policy.

The College will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our Anti-Bullying Policy.

Complaints

As with all issues of safety at Slindon College, if a member of staff, a pupil or a parent/carer has a complaint or concern relating to E-safety, prompt action will be taken to deal with it. Parents/Carers should follow the Complaints Policy to address their concerns.

Incidents of or concerns around E-safety will be recorded using an incident report form or safeguarding form and reported to the College's Designated Safeguarding Lead, in accordance with the College's Child Protection Policy.