Reviewed and Approved: Summer 2023
Next Review: Summer 2024
Responsibility: E-Safety Lead

E-Safety and Digital Awareness Policy

Part 1 – Introduction

Aims and Context

Digital technologies are now seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Therefore, the main objective of this policy – in conjunction with the relevant Acceptable Use Policies - is to support all members of the College community in the safe and responsible use of technology. By retaining a robust technical infrastructure, educating pupils, staff and parents of the risks associated with using digital technologies, and by providing expectations of behaviour both on and off site, it aims to protect the safety, well-being and reputation of all.

The scope of digital technologies is vast and at present includes the use of the internet and web-based services on computers and mobile devices such as phones, tablets and smart watches. However, the policy recognises the exponential rate at which technology is developing and therefore aims to provide a set of principles to inform digital safety practices – regardless of the specific technology that is being used.

As with most organisational practices, it is also important to understand what to do if something goes wrong. Therefore, the policy also aims to support those that need to report issues relating to safeguarding, misconduct, misuse or inappropriate content.

Scope of this Policy

This policy applies to all members of the College community (including governors, staff, pupils, volunteers, parents/carers, visitors) both within the College and remotely.

The Education and Inspections Act 2006 empowers the Head, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the College site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other digital incidents covered by this policy, which may take place out of College, but are linked to membership of the College. The College will deal with such incidents within this policy (and associated Behaviour, Anti-

bullying and Safeguarding policies) and will, whenever discovered, inform parents/carers of incidents of inappropriate digital behaviour that take place out of the College.

Safeguarding

It is recognised in the Keeping Children Safe in Education (KCSIE) statutory guidance (2022), that technology often provides the platform that causes harm through content – being exposed to illegal, inappropriate or harmful materials; contact – being subjected to harmful online interaction with other users; conduct – personal online behaviour that increases the likelihood of, or causes harm; and commerce – including risks such as online gambling, inappropriate advertising, phishing and or financial scams.

It is also recognised that young people are vulnerable to online grooming in the form of child sexual exploitation or radicalisation and extremism as outlined under the Prevent Duty (2015). Therefore, it is essential that internet filtering and monitoring take place in order to keep members of the College community safe from harm.

The College must also provide opportunities for the teaching of safeguarding with regard to E-Safety and media navigation in line with the Department of Education's Teaching online safety in schools guidance (2023). In addition, staff need to be regularly trained and updated to be able to recognise the indicators of abuse or exploitation as well as safeguarding policies and procedures.

Roles and Responsibilities

The following section outlines the roles and responsibilities for E-Safety of individuals and groups within the College.

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy on an annual basis.

The Safeguarding Governor is informed of any significant incidents by the Head. The Safeguarding Governor chairs the Education Committee and reports to them and to the Governing Council.

The Designated Safeguarding Leads (DSL's) maintain secure Records of Concern which contain all detailed notes regarding a given incident, including any details relating to the use of IT. The contents of these files are summarised and presented annually to the Governing Body in the form of an annual Safeguarding Report completed by the Senior DSL.

The Head and Senior Managers

In this policy the Head is the College Head who liaises with the Prep School Head and the Head of Pre-Prep, all of whom are responsible for the implementation of this policy.

The Head is responsible for ensuring the safety (including E-Safety) of members of the College community, though the day-to-day responsibility for E-Safety will be delegated to the Director of IT Services and the Designated Safeguarding Leads in consultation with the E-Safety Co-ordinators for each area of the college.

The Head is responsible for ensuring that the DSLs, E-Safety Lead and Co-ordinators and other relevant staff receive suitable CPD to enable them to carry out their E-Safety roles and to train other colleagues.

The Head will ensure that there is a system in place to allow for monitoring and support of those in the College who carry out the internal E-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

The College Head, the Prep School Head and the Head of Pre-Prep, will receive updates from the DSLs on an incident-by-incident basis. These will then be reported to the Head by the Head of the relevant section of the school.

In the event of a serious E-Safety allegation being made against a member of staff, the procedures detailed in the Safeguarding Policy (Child Protection) will be followed. The decision as to whether or not to notify the Local Authority Designated Officer (LADO) will depend on the details of the incident.

Designated Safeguarding Leads (DSLs)

Senior School:	Senior DSL	Jane Pawulska
	Deputy DSL	Richard Honey
	Deputy DSL	Sasha Gunes
	Deputy DSL	Alex Swart-Wilson
Prep School:	DSL	Imogen Cowan
	Deputy DSL	Joe Surrage
	Deputy DSL	Rupert Snow
	Deputy DSL	Kirsty Brooks
Pre-Prep:	DSL	Jo Wallace
Early Years:	DSL	Charlotte Cuthbert

The DSLs should be trained in E-Safety issues and be aware of the potential for serious child protection issues to arise from;

- sharing of personal data;
- access to illegal/inappropriate materials;
- underage gambling
- self-generated sexual imagery
- child-on-child abuse
- inappropriate online contact with adults/strangers;
- potential or actual incidents of grooming; or
- Cyberbullying, prejudice-based bullying and discriminatory bullying.

The DSLs:

- together with the Director of IT Services, takes day to day responsibility for E-Safety issues related to safeguarding and have a leading role in establishing and reviewing the College E-Safety Policy in conjunction with the E-Safety Lead on an annual basis;
- liaises with the Director of IT Services;
- receive reports of E-Safety incidents;
- ensure that staff including Governers are trained regularly in online safety;
- ensure children are taught about online safety
- engage with parents to share information about online-safety
- and report, as appropriate, to the Senior Management Teams.

E-Safety Lead

Meryem Brook

The E-Safety Lead:

- together with the Director of IT Services and the DSLs, have a leading role in establishing and reviewing the College E-Safety Policy on an annual basis;
- work with the Director of IT Services, the DSLs and the Policy Co-ordinator to ensure that all related policies are updated as appropriate;
- work with the Head and other Senior Staff members who are responsible for staff training and the Director of IT Services to identify training opportunities for staff;
- work with the DSLs to incorporate an appropriate level of E-Safety training for new staff as part of the Safeguarding Induction;
- should themselves be trained in E-Safety issues; and made aware of reports of E-Safety incidents to enable them to co-ordinate the provision of relevant E-Safety education to pupils across the College;
- work with the Director of IT Services and the DSLs to co-ordinate the provision of relevant E-Safety guidance to parents.

E-Safety Co-ordinators

Senior School:	Head of PSHE	Sasha Gunes
Prep School:	Head of ICT / Computing	Frances Sharpsmith
Pre-Prep:	Year 1 Teacher / ICT Co-ordinator	Rebecca Smith

The E-Safety Co-ordinators:

- together with the E-Safety Lead, co-ordinate the provision of relevant E-Safety education to pupils in their section of the College through ICT/Computing lessons, PSHE/Empower programmes and assemblies covering areas of risk related to content, contact, conduct and commerce
- should themselves be trained in E-Safety issues; and made aware of reports of E-Safety incidents to enable them to adapt and update the provision of E-Safety education to pupils as required;

Director of IT Services

Andrew Pawlowicz
The Director of IT Services is responsible for ensuring that;

- as far as is reasonably possible, the College's IT infrastructure is secure and is not open to misuse or malicious attack;
- only legitimate users are provided with a username to access the College's networks;
- the College's filtering policy, as specified by the Senior Management Team (SMT) informed by safeguarding audits, is applied and updated as appropriate;
- keeps up-to-date with E-Safety technical information in order to effectively carry out the E-Safety role and to inform and update others as relevant;
- the use of all IT systems under direct control are regularly monitored in order that any misuse/attempted misuse can be reported to the Senior DSL for investigation/action/sanction;
- monitoring software/systems are implemented and updated as required; and
- a log of incidents is maintained to inform future E-Safety developments.

Teaching and Support Staff

Staff are responsible for ensuring that;

- they have an up-to-date awareness of the current College E-Safety Policy and practices;
- they have read, understood and operate within the College Staff Acceptable Use Policy (AUP);
- they are aware of the contents of the Pupil Acceptable Use Policy (AUP) and ensure, through appropriate supervision and education that students adhere to it;
- **they report any suspected misuse or problem to the DSL in their area of the College for investigation/action/sanction.**

Pupils

Pupils are responsible for ensuring that;

- they have read, understood and operate within the College Pupil Acceptable Use Policy (AUP);
- they report any misuse or problem to a member of staff - ideally the DSL in their area of the College.

Parent/Carers

Parents and carers play a crucial role in ensuring that their children understand the need to use technology in an appropriate way. They are responsible for endorsing the Pupil Acceptable Use Policy where required by the College.

Parents and carers should also follow the guidance within this policy especially in relation to the use of personal devices when on the College site.

Part 2 - How the College will implement E-Safety

Technical Infrastructure, Filtering and Monitoring

The College will be responsible for ensuring that the College infrastructure/network is as safe and secure as is reasonably practicable and that appropriate policies and procedures to that end are implemented, including an annual review of such provision.The College will ensure that the people named in the above sections are effective at carrying out their E-Safety responsibilities:

- Servers, wireless systems and cabling will be securely located and physical access restricted.
- All users will have role-specific access rights to College IT systems.
- All users will be provided with a unique username and password (a group log-on may be used in the Pre-Prep and Shell under the careful supervision of staff).
- The "administrator" password for the MIS is currently held by the Director of IT Services and the Data Manager, who have access at the highest security level. In the case of an emergency occurring at a time when the Director of IT Services and Data Manager are unavailable, our supplier, WCBS, would reset the Bursar as the Administrator.
- All staff users are encouraged to change their passwords regularly and must change them if it is suspected that someone else may have seen their password.
- Users are responsible under the AUP for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Effective filtering processes are in place to protect staff and pupils from accessing content which could cause them harm. This includes, but is not limited to, online material which is;
    - violent or that which glorifies violence;
    - criminal, terrorist or glorified criminal activity (including drug abuse);
    - racist or designed to incite racial hatred;
    - of extreme views;
    - pornographic or with otherwise unsuitable sexual content;
    - crude, profane or otherwise unsuitable language;
    - blasphemous or mocking of religious and moral beliefs and values;
    - discriminative, particularly in relation to the protected characteristics of the Equality Act;
    - in breach of the law, including copyright, data protection and computer misuse.
- Requests from staff for websites or content to be removed from the filtered list will be considered by the Director of IT Services in consultation, whenever appropriate, with the DSL.
- College IT technical staff regularly distribute reports detailing the activity of users on the College IT systems and users are made aware that all online activity is monitored in the Acceptable Use Policy.
- Whilst content accessed through mobile data (3G/4G/5G connection) cannot be filtered by the College, both pupils and staff are provided with specific guidance on the use of personal devices within the respective AUPs.
- Users are asked to report any actual/potential E-Safety incident using the College's pastoral systems.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc. from accidental or malicious attempts to threaten the security of the College systems and data.
- Staff and Pupil AUPs forbid the downloading of executable files by users, forbid the installation of programmes on College workstations/mobile devices, describe the extent of personal use that users are

permitted, describe the appropriate use of removable media (e.g. memory sticks/CDs/DVDs) by users on College workstations/portable devices and describe restrictions regarding the protection of data.

- The College infrastructure, staff laptops and individual workstations are protected by up-to-date antivirus software and intrusion detection systems.
- Any third-party IT services which process either pupil or staff personal information complies with data protection regulations in accordance with the College's Data Protection Policy.

E-Safety Education – Pupils

Children and young people need the help and support of the College to recognise and avoid E-Safety risks and build their resilience. The overall aim for the College's E-Safety provision is to support pupils in making the right choices when using the internet and mobile technologies. In doing so, pupils should have the knowledge and skills to be able to protect their safety, well-being and reputation whilst still utilising all the benefits that technology has to offer.

E-Safety education will be provided in the following ways, as appropriate for each section of the school covering :

- Through discrete Computing/ICT lessons.
- As part of a planned series of sessions within the PSHE/Empower programme.
- Tutor time activities.
- Key E-Safety messages provided and reinforced during assembly times.

E-Safety education will endeavour to cover the following main areas of risk:

Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes) and/or pornography, sharing other explicit images and online bullying; and

Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If it is felt that pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/)

E-Safety should be promoted across all areas of the curriculum and staff should reinforce E-Safety messages and good working practices whenever the opportunity presents itself. For example:

- Pupils should be helped to understand the need for the Pupil Acceptable Use Policy (AUP) and encouraged to adopt safe, responsible and respectful use of IT, the internet and personal devices both within and outside College.

- Pupils should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Staff should also take the following considerations into account when delivering lessons where the use of the technology is pre-planned:

- It is best practice that pupils should be guided to websites checked as suitable for their use.
- Where pupils are allowed to search the internet freely e.g., using age-appropriate search engines, staff should be vigilant in monitoring the content of the website's pupils visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination etc.) that would normally result in internet searches being blocked. In such a situation, staff can request for the Director of IT Services to temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Any educational apps or online services to be used, must be on the College's approved Digital Learning Tools List and therefore assessed for compliancy with data regulations. If staff want to use an educational app or online service that is not on the list, they must request for it to be assessed in accordance with the College's Data Protection Policy.

E-Safety Training – Staff

All staff should be trained to a sufficient level of E-Safety awareness to effectively safeguard the pupils in their care. For most teaching and support staff, as well as Governers, this should be achieved through their Safeguarding induction and subsequent annual safeguarding training conducted by the Designated Safeguarding Leads and in conjunction with the E-Safety Lead.

For those staff who have specific pastoral and/or E-Safety responsibilities, further training is required to ensure that they have sufficient understanding of the risks relating to the personal use of technology and any necessary actions that need to be taken should a safeguarding incident occur;

- DSLs to ensure they have the knowledge to effectively act upon reported safeguarding issues related to E-Safety and to interpret the reports provided by IT technical staff to monitor user activity on College systems.
- The E-Safety Lead and E-Safety Co-ordinators to ensure that have the knowledge and skills to advise on the provision of E-Safety education to pupils, train other staff members and provide guidance to parents/carers.

E-Safety Guidance – Parents/Carers

As much as possible, the College will endeavour to make available up-to-date E-Safety information and guidance to parents and carers, so that they are able to support their children using technology safely and responsibly. This will be through official communication channels such as the College website, school newsletters and emails.

Part 3 - How the College community can support E-Safety

Definition

For the purpose of this document, a personal device is any piece of portable equipment including mobile phones, laptops, tablets, smart watches or wearable technology, cameras or any other device which is designed for, or capable of, taking digital imagery and/or connecting to the internet.

Staff

Whilst members of staff are working with pupils in any context within the College, the pupils' needs and welfare are the paramount concern. Therefore, all staff must use technology safely and responsibly in accordance with the College's Acceptable Use Policy and Data Protection Policy. Should a member of staff fail to follow the guidance in this policy or associated policies, the College would be unlikely to support them, should their actions be called into question.

Device use

The College allows staff to bring in personal devices for their own use during non-contact time, such as breaks and lunch time, when they are not supervising pupils.

Wherever possible, only College provided equipment should be used during contact time with pupils, which includes lessons and any direct contact or supervisory sessions. Staff are not allowed to use personal devices to capture, store or share photographic and/or video imagery of pupils, or pupil personal data. Staff from all sections of the school must not use personal devices at any time whilst in proximity to pupils from the Pre-Prep or Shell. For example; when pupils are travelling to and from the dining hall or swimming pool.

The College does **not** permit a member of staff to contact a pupil or parent/guardian via voice/video call or text/instant messaging using their personal device except in the case of an emergency. All contact must be through normal College communication channels, such as landlines, email and/or through a device provided by the College. Staff are permitted to use their personal device to contact a pupil or parent/guardian via College email systems, as long as the device is encrypted with a password.

Offsite visits and trips

On offsite visits and trips, members of staff must use the devices provided by the College to contact pupils or parents/guardians. (please see the Trips Policy for further details). If the need arises, this device could be used to store contact lists and numbers. Numbers must be deleted following the event.

If a pupil requires the use of a mobile device (in the event, for example of their own having run out of power), during offsite/school trips, the College device should be used. In the event that a College mobile device is not available, the member of staff may use their own device. However, the member of staff should supervise the call.

Use of digital photographic and video imagery

For any activities where imagery is to be taken, staff must only use College provided equipment. The imagery must only be transferred to College approved systems and if necessary, shared via official College communication channels or agreed processes.

Care should be taken by the member of staff taking the imagery that the pupils are aware that imagery is to be taken. Care should be taken when taking imagery that students are appropriately dressed and are not participating in activities that might bring the individuals or the College into disrepute.

Imagery published on the website, or elsewhere that include pupils, will be selected carefully and will comply with best practice guidance on the use of such images.

Where parents have not given permission for their children's image to be published, staff must respect this decision and ensure that imagery is not placed on the College website or in any other publication.

Pupils' full names or home addresses will not normally be used anywhere on a public website or blog, particularly in association with imagery.

In exceptional circumstances

Only with the **express permission of the Head**, staff are permitted to take photos on their own private devices of pupils participating in sports or activities, providing the following rules are observed:

- The event and imagery are entirely appropriate and in keeping within the KCSIE guidance.
- The images are used for formal College marketing or communications purposes.
- Pupils are fully aware the staff are taking the imagery and are happy for them to do so.
- Imagery is taken on a device which is protected by a security password to prevent others accessing them.
- The imagery is downloaded onto a College laptop or device as soon as is reasonably practicable.
- All images on the private device are then deleted.
- If the imagery is uploaded to the official College communication channels it is done within the agreed processes.

Commissioning staff must ensure that: Commissioned photographers (external suppliers) must only take the images they have been briefed to take. They must ensure that all pupils are aware an image is to be taken, are dressed appropriately and are not participating in activities that might bring the College or the individuals into disrepute. They must ensure all images are stored safely and securely and held separately from other images. They must undertake that under no circumstances, may they share these images with anyone outside the College Community. All photos must be given to the College, unless copyright is retained by the supplier.

Pupils

Pupils are expected to adopt safe, responsible and respectful use of IT, the internet and personal devices both within and outside the College.

The College allows pupils to bring in personal devices to school from Fourth Form upwards. Pupils should only use personal devices during lessons, assemblies and other contact times, if instructed to do so by a member of staff.

Whether using College equipment or their personal device, they should do so in accordance with the College's Pupil Acceptable Use Policies (AUP).

Pupils must not take, use, share, publish or distribute images of others at any time, without their prior permission.

Visitors including volunteers and current/prospective parents

It is recognised that visitors to the College will most likely have a personal device on their person. However, they should not use any personal device whilst in proximity to pupils unless otherwise directed by the member of staff supervising them.

All visitors to the Pre-Prep will be asked to hand in all personal devices into the respective Administration Office.

Visitors are not permitted to take imagery of any pupils unless specifically commissioned to do so.
Visitors that require access to the College's WiFi network must only do so using the temporary security key provided by the IT Department and only on agreement of the College's Acceptable Use Policy.

Online communications

For the purpose of this document, online communications relate to any platform that enables users to communicate with others through written means or multimedia, create, post and share content or to participate in social networking including but not limited to; social media channels, gaming websites, blogs, forums, email and messaging apps.

The College encourages the appropriate use of online communications by all members of the College community. It especially acknowledges the place of online communications in increasing opportunities to learn and in promoting positive, respectful and thought-provoking discussions. Such platforms provide a recognised forum through which ideas can be shared in an open, supportive and collaborative environment, allowing pupils, staff, alumni, parents and the wider community to keep abreast of events using real-time communication. Narratives posted onto these platforms have the potential for considerable breadth of dissemination and individuals choosing to post content on these channels should be mindful of this.

The College expects all members of the College community to consider fully and prior to posting on such platforms, any potential impacts on safety, reputation and liability for themselves, other members of the College and the College itself.

Any member of staff or any pupil who wishes to set-up an online communications channel in relation to the College i.e. a house or sports team social media page, must only do so with express consent from the College and in consultation with the Marketing Department. The administrators of any such channel must also adhere to the College's Social Media Acceptable Use Policy.

The College asks parents/carers to also follow effective safeguarding practices when posting content online, especially in regards to the posting of imagery of their children. When sharing content of College events, parents/carers should be mindful of seeking permission from the parents/carers of any other children that maybe included in the imagery, before posting online.

Part 4 - How to Respond to Safeguarding Concerns, Incidents of Misuse and Report Inappropriate Content

It is intended that all members of the College community will be responsible users of technology, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through carelessness or irresponsibility or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse.

Safeguarding concerns

If any apparent or actual misuse appears to involve illegal activity i.e.:

- child sexual abuse images.
- adult material which potentially breaches the Obscene Publications Act.
- criminally racist or hate material.
- other criminal conduct, activity or materials.

Incidents must be reported to the appropriate DSL. If necessary however, it can be reported by anyone directly to the National Crime Agency's CEOP Command via https://www.ceop.police.uk/safety-centre/. This agency works with child protection partners across the UK and overseas to identify the main threats to children and coordinates activity against these threats to bring offenders to account. They protect children from harm online and offline, directly through NCA led operations and in partnership with local and international agencies.

Misuse

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal, it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. Such incidents should be reported immediately to the Director of IT Services.

It is more likely that the College will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible, in a proportionate manner, and that members of the College community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as per the agreed Pupil Behaviour Policy and Staff Disciplinary Policy. This may also include loss of access to College systems and the internet and/or confiscation of equipment.

Inappropriate content

Whilst the College endeavours to ensure that filtering processes are robust enough to protect staff and pupils from accessing content which could cause them harm; it recognises that some online material could, by omission or commission, bypass these preventative measures. In the event of inappropriate content being accessible on the College network, it should be reported immediately to the Director of IT Support Services and the DSLs.