

E-SAFETY POLICY

I. Background / Rationale

New technologies have become integral to the lives of children and young people in today's society, both within Colleges and in their lives outside College. The use of these exciting and innovative tools in College and at home has been shown to raise educational standards and promote student achievement. However, the use of these new technologies can put young people at risk within and outside the College. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to , loss or sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing or distribution of personal images without an individual's consent or knowledge
- Inappropriate communication or contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video or internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world, thus this policy is used in conjunction with other college policies (Behaviour Management, Child Protection and Acceptable Internet Use policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

2. Scope of the Policy

This policy applies to all members of the College community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of College ICT systems, both in and out of College.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students 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 e-safety incidents covered by this policy, which may take place out of College, but is linked to membership of the College. The College will deal with such incidents within this policy and the behaviour management policy and will inform parents / carers of incidents of inappropriate e-safety behaviour.

3. Roles and Responsibilities

3.1 **Governors:** Governors are responsible for the approval of the E-Safety Policy and for reviewing its effectiveness. This will be carried out by the Governors' Learning and Community Committee. A member of the Governing Body has taken on the role of E-Safety Governor.

3.2 **Principal and Senior Leaders:** The Principal and other members of the Senior Leadership Team are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

3.3 **E-Safety Coordinator / Officer:** Matthew Lennon will be College E-Safety Coordinator and will work closely with Wendy Ohlson, designated person for child protection. The E-safety Coordinator will:

- take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the College e-safety policies / documents
- ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- provides training and advice for staff
- liaises with College ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- reports regularly to Senior Leadership Team

3.4 **Network Manager / Technical staff** are responsible for ensuring:

- that the College's ICT infrastructure is secure and is not open to misuse or malicious attack
- that users may only access the College's networks through a properly enforced password protection policy, in which passwords are regularly changed
- that the use of the network is regularly monitored in order that any misuse can be reported to the E-Safety Co-ordinator for investigation and action where necessary
- that monitoring software systems are implemented and updated as agreed in College policies

3.5 **College Staff** are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current College e-safety policy and practices
- they have read, understood and signed the College Guidance for 'Safer-working Practice for Adults who work with Children and Young People'.
- they report any suspected misuse or problem to the E-Safety Co-ordinator for investigation and action.
- digital communications with students should be on a professional level and only carried out using official College systems
- students understand and follow the College e-safety and acceptable use policy
- they monitor ICT activity in lessons, extra curricular and extended College activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current College policies with regard to these devices
- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

- 3.6 Designated person for Child protection is 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
 - inappropriate on-line contact with adults / strangers
 - potential or actual incidents of grooming
 - cyber-bullying
- 3.7 Students are responsible for using the College ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to College systems
- 3.8 Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The College will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about e-safety campaigns and literature. Parents and carers will be responsible for endorsing (by signature) the Student Acceptable Use Policy

4. Policy Statements

4.1 Education – students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the College's e-safety provision. Children and young people need the help and support of the College to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- A planned e-safety programme will be provided as part of the ICT and PSHE curriculum - this will cover both the use of ICT and new technologies in College and outside College
- Key e-safety messages in assemblies and tutorial activities
- Students are taught in all lessons to be critically aware of the content they access on-line and are guided to validate the accuracy of information

4.2 Staff learning

- A planned programme of e-safety training will be made available to staff. It is expected that some staff will identify e-safety as a training need within the performance management process
- All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand the College e-safety policy and Acceptable Use Policies
- The E-Safety Coordinator will provide advice, guidance and training as required to individuals

4.3 Governors Training – Governors

Training and awareness sessions are made available to any Governor who wishes to take part.

4.4 Technical – infrastructure / equipment, filtering and monitoring

The college ICT systems are managed in ways that ensure that the College meets the e-safety technical requirements. There are regular reviews and audits of the safety and security of College ICT systems Servers, wireless systems and cabling are securely located and physical access restricted

- All users have clearly defined access rights to College ICT systems
- All users are provided with a username and password by the Network Manager who will keep an up to date record of users and their usernames
- The “master / administrator” passwords for the College ICT system, used by the Network Manager are available to the Principal and kept in a secure place. Users will be made responsible 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
- The College maintains and supports the managed filtering service provided by Smoothwall
- College ICT technical staff regularly monitor and record the activity of users on the College ICT systems and users are made aware of this in the Acceptable Use Policy
- The College infrastructure and individual workstations are protected by up to date virus software
- Personal data can not be sent over the internet or taken off the College site unless safely encrypted or otherwise secured. Staff who need to do this in their particular role have their laptops encrypted

4.5 Curriculum

- E-safety is a focus in all areas of the curriculum and staff reinforce e-safety messages in the use of ICT across the curriculum
- in lessons where internet use is pre-planned, students are guided to sites checked as suitable for their use
- Where students are allowed to freely search the internet, staff are vigilant in monitoring the content of websites visited
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager can temporarily remove those sites from the filtered list for the period of study. Any request to do so, is audited with clear reasons for the need
- Students are taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information

4.6 Use of digital and video images – Photographic and Video

- When using digital images, staff should inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they recognise the risks attached to publishing their own images on the internet eg on social networking sites
- Staff are allowed to take digital / video images to support educational aims, but must follow College policies concerning the sharing, distribution and publication of those images. Those images should only be taken on College equipment, the personal equipment of staff should not be used for such purposes

- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the College into disrepute
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs
- Parents or carers are given the opportunity to withdraw photographs of students that are published on the College website

4.7 Data Protection See Data Protection Policy

4.8 Communications

When using communication technologies the College considers the following as good practice:

- The official College email service may be regarded as safe and secure and is monitored. Users need to be aware that email communications may be monitored (see KCC staff communications guidelines)
- Users must immediately report, to the nominated person – in accordance with the College policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email
- Any digital communication between staff and students or parents / carers (email, VLE etc) must be professional in tone and content

4.9 Unsuitable / inappropriate activities

Users shall not visit Internet sites, post, download, upload, communicate or pass on, material and comments that contain or relate to:

- Offensive materials: child sexual abuse images, promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation, adult material that potentially breaches the Obscene Publications Act in the UK, racist material, pornography, promotion of any kind of discrimination, promotion of religious hatred, threatening behaviour
- Using College systems to run a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Smoothwall and / or the College
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
- This also applies to students' personal handheld technologies to and from College and whilst on College premises

4.10 Responding to incidents of misuse

Any apparent or actual misuse which appears to involve illegal activity ie.

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

will be reported initially to the E-Safety Coordinator.

Actions will be followed in line with the College procedures including reporting the incident to the police and the preservation of such evidence.

It is more likely that the College will need to deal with incidents that involve inappropriate rather than illegal misuse. Such incidents of misuse will be dealt with through the normal behaviour management policy.

5. **Review of Policy**

This policy is reviewed by the Learning & Community Committee of Governors on an annual basis.

**Ratified by the Learning & Community Committee
31st January 2012**