

E-Safety Policy

1. Introduction

- a) Kensington and Chelsea College recognises the benefits and opportunities which new technologies offer to teaching and learning. We encourage the use of technology in order to enhance skills and promote achievement.
- b) However, the accessible and global nature of the internet and variety of technologies available mean that we are also aware of potential risks and challenges associated with such use. Our approach is to implement safeguards within the College and to support staff and learners to identify and manage risks independently. We believe this can be achieved through a combination of security measures, training and guidance and implementation of our associated policies.
- c) In furtherance of our duty to safeguard learners and the Every Child Matters agenda, we will do all that we can to make our learners and staff stay e-safe and to satisfy our wider duty of care. This e-safety policy should be read in conjunction with other relevant college policies, in particular the Safeguarding Policy. Other relevant policies include Data Protection; Equality and Diversity and Dignity at Work (Staff) and Anti Harassment and Bullying (Students).

2. Creation, Monitoring and Review

- a) This Policy is based on the JISC e-safety Policy Template (August 2010 The impact of the policy will be monitored regularly by the Executive with a full review being carried out annually.
- b) Kensington and Chelsea College has a statutory and moral duty to ensure that the College functions with a view to safeguarding and promoting the welfare of children and vulnerable adults receiving education and training at the College. The College works in partnership with Her Majesty's Prison Service (HMPS) to ensure the safety of learners on secure sites and monitors policies and procedures in franchise partners.
- c) Throughout these policies and procedures, reference is made to "children and young people". This term is used to mean "those under the age of 18". The

policy and procedures also cover the Protection of Vulnerable Adults (see appendix I of the Safeguarding Policy for definitions).

Policy Scope

- a) This Policy applies to all users, including students, staff and the wider college community who have access to the college IT systems, both on College premises and remotely. Where applicable, this policy applies to staff working on secure sites. Any user of College IT systems must adhere to this Policy. In addition, staff must adhere to the IT Network and Acceptable Use Policy.
- b) This e-Safety Policy applies to all use of the internet and electronic communication devices such as email, mobile phones, games consoles, and social networking sites.
- c) Users should read this policy in conjunction with the Safeguarding Policy.

4. Roles and Responsibilities - general

- a) All staff are responsible for ensuring the safety of learners. Any e-safety incidents should be reported under the Safeguarding reporting procedures (section H of the Safeguarding Policy). Section K of the Safeguarding Policy contains contact details of relevant staff.
- b) Staff working on secure sites should refer to the internal procedures that apply to the location.
- c) The Senior Manager responsible for safeguarding at non-secure sites is the Vice Principal. Where a safeguarding incident may include e-safety, the Vice Principal may consult with the Director of ILT or Director of Resources.
- d) All members of the teaching staff are required to deliver e-safety lessons to classes as part of the tutorial programme and to read through and adhere to the incident reporting procedure as contained in the Safeguarding Policy. When informed about an e-safety incident, staff members must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved.
- e) All learners must know what to do if they have e-safety concerns and who to talk to. In most cases, this will be their Personal Tutor.
- f) Where management considers it appropriate, the child protection officer may be asked to intervene with appropriate additional support from external agencies.

5. Roles and Responsibilities

Designated manager for e-safety (non-secure sites)

- a) The designated senior member of staff with lead responsibility for e-safety is the Vice Principal. This person has a key duty to take lead responsibility for raising awareness within the staff of issues relating to the welfare of children and young people, as well as vulnerable adults and the promotion of a safe environment for these people learning within the College.
- b) Where appropriate, the Vice Principal may seek support from the Director of ILT or the Director of Resources if the incident relates to e-safety.

Students (non-secure sites)

- a) Students are responsible for using the college IT systems and mobile devices in accordance with the College Acceptable Use Agreement/Code of Conduct which they must sign up to as a condition of using the College network. By signing the Agreement, students are agreeing to abide by the terms of the Agreement/Code of Conduct, and other related policies.
- b) Students are responsible for attending e-safety lessons as part of the curriculum and ILT induction. They are expected to seek help and follow procedures where they are worried or concerned, or where they believe an e-safety incident has taken place involving them or another member of the college community.
- c) Students must act safely and responsibly at all times when using the internet and/or mobile technologies.

Staff (all sites)

All members of staff working on non-secure sites are responsible for using the College IT systems and mobile devices in accordance with the Email and IT Network Acceptable Use Policy for Staff working in non-secure sites. In addition, staff working on secure sites should familiarise themselves with the IT, safeguarding and e-safety policies adopted by the Prison Service in respect of the secure site at which they are located. Members of staff are responsible for undertaking staff training on safeguarding and e-safety and displaying a model example to learners at all times.

Online communication with learners must only be done through the College network and Moodle/Virtual Campus and relate to learning. Staff must not disclose their private email to students or invite students to become 'friends' on their private social networking sites. Similarly, staff should decline any request to become a 'friend' of a student on a social networking site.

5. Security

The College will do all that it can to make sure the College network is safe and secure. Every effort will be made to keep security software up to date. Appropriate security measures will include the use of enhanced filtering and protection of firewalls, servers, routers, work stations etc. to prevent accidental or malicious access of College systems and information. Digital communications, including email and internet postings, over the College network, will be monitored in line with the e-security policy.

7. Behaviour

- a) Kensington and Chelsea College will ensure that all users of technologies adhere to the standards of behaviour as set out in the Email and IT Network Acceptable Use Policy for Staff and the Student Acceptable Use Agreement/Code of Conduct.
- b) The College will not tolerate any abuse of IT systems. Whether offline or online, communications by staff and learners should be courteous and respectful at all times. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the relevant College policies.
- c) Where conduct is found to be unacceptable, the College will deal with the matter internally. Where conduct is considered illegal, the College will report the matter to the police.

8. Communications

As the use of ICT in learning and teaching increases, policies on communication using technology will be reviewed.

On secure sites, prison regulations and procedures will always take precedence over College procedures and policies in the event of rapid changes and to eliminate doubt. Forums within Moodle and Virtual Campus is permitted amongst teaching staff and students on secure sites. Most mobile devices are prohibited within secure sites – if in doubt, staff should consult with their Centre Manager.

Students may use social networking sites and chat rooms on non-secure sites in drop-in IT access areas in the library and canteen and other social areas, but not in classrooms. In all areas students must stop using College IT equipment for these purposes if requested to do so by a member of staff – generally, where another student requires the resource for learning. Students should be aware that the use of social networking sites is also subject to the College's strict rules to protect students from bullying and

harassment, and should report any incidents to their Personal Tutor. Further details are in the Safeguarding Policy.

9. Use of Images and Video

The use of images, or photographs, is popular in teaching and learning and should be encouraged where there is no breach of copyright or other rights of another person. This will include images downloaded from the internet and images belonging to staff or learners.

Cameras are not permitted on secure sites – staff must not take photos of students or anywhere on secure sites without the express permission of the prison authority.

All learners and staff should be aware of the risks of downloading images as well as posting them online and sharing them with others. There are particular risks where personal images are posted onto social networking sites, for example. An online learning module is available on Moodle to highlight these risks.

College staff will provide information to learners on the appropriate use of images as detailed in the Communications policy. Our aim is to reinforce good practice as well as offer further information for all users on how to keep their personal information safe.

No image/photograph can be copied, downloaded, shared or distributed online without permission from the Marketing Department. Photographs of activities on the College premises should be considered carefully and have the consent of the Marketing Department before being published. Approved photographs should not include names of individuals.

10. Personal Information

Any processing of personal information needs to be done in compliance with the Data Protection Act 1998.

Personal information is information about a particular living person. The College collects and stores the personal information of learners and staff regularly e.g. names, dates of birth, email addresses, assessment materials and so on. The College will keep that information safe and secure and will not pass it onto anyone else without the express permission of the learner or parent carer.

No personal information can be posted to the College website without the permission of the Director of Resources. Staff must keep learners' personal information safe and secure at all times. When using an online platform, all personal information must be password protected. No personal information of individuals is permitted offsite unless the member of staff has the permission of the Director of Resources. Every user of IT facilities is required to log off on completion of any activity, or where they are physically absent from a device.

Any mobile device (laptop, USB) requires to be encrypted, password protected and signed out by the IT staff. Where the personal data is no longer required, it must be securely deleted in line with the Data Protection policy.

11. Education and Training

Students should familiarise themselves with the e-safety modules on Moodle, and the safeguarding systems detailed within the Safeguarding Policy and summarised in the Student Planner. Tutorial sessions will include safeguarding and e-safety.

Staff will take part in safeguarding and e-safety training using online learning materials. Further resources of useful guidance and information will be available to all staff on the Staff Intranet.

12. Incidents and Response

Where an e-safety incident is reported to the College this matter will be dealt with very seriously. The College will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring. If a learner wishes to report an incident, they can do so to their Personal Tutor or a member of the safeguarding team. Where a member of staff wishes to report an incident, they must contact their line manager. Following any incident, the College will review what has happened and decide on the most appropriate and proportionate course of action. Sanctions may be put in place, external agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident.

The reporting procedure detailed in the Safeguarding Policy should be adopted for any e-safety incidents.

13. Feedback and Further Information

Kensington and Chelsea College welcomes all constructive feedback on this and any other College policy. If you would like further information on e-safety, or wish to send us your comments on our e-Safety Policy, then please contact: Darren Tysoe, Director of ILT on d.tysoe@kcc.ac.uk or telephone number: 020 7573 1416.