ST. ANDREW'S
COLLEGE
Cambridge

# COLLEGE POLICY DOCUMENT

# E-SAFETY POLICY

| | |
|---|---|
| **Issue No.: 01** | **Document Number: STAN0032012** |
| **Issue Date: September 5th 2011** | **Originator: Wayne Marshall** |
| **Version: 05** | **Responsibility: Principal** |
| **Reason for version change: Review & update RB** | **Dated: 5th September 2011** |
| **Authorised by: Wayne Marshall**<br>**Date: 24.07.2015** | **Signature:**<br>**Wayne Marshall** |

## Table of Contents Page

## 1. Introduction

St. Andrew's College Cambridge 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. 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 students 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. In furtherance of our duty to safeguard students we will do all that we can to make our students 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 e.g. Safeguarding, Acceptable Use of ICT and Disciplinary and Bullying. This policy is written in the expectation that all students and staff should be treated with respect, as individuals, and that respect extends to the way in which these technologies are used.

## 2. Creation, Monitoring and Review

This policy was written by the Principal / E-safety Officer after consultation with other key members of staff. It was approved by the College Senior Management Team and College in September 2011.

The impact of the policy will be monitored regularly with a full review being carried out at least once every year. The policy will also be reconsidered where concerns are raised by the E-safety Officer or where an E-safety incident has been recorded.

## 3. Policy Scope

The policy applies to all members of the College community who have access to the College IT systems, both on the premises and remotely. Any user of College ICT systems must adhere to and sign a hard copy of the Internet Acceptable Use Policy (16). This policy also covers all forms of electronic communication whilst on College business or affecting College's reputation. Finally the E-safety Policy applies to all use of the internet and electronic communication devices such as email, mobile phones, games consoles and tablets.

## 4. Roles and Responsibilities

There are clear lines of responsibility for E-safety within the College. The Safeguarding Officer is the designated person for all matters relating to E-safety. It is important however to note that **all staff are responsible for ensuring the safety of students** and should report any concerns immediately to the Principal. 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.

All students must know what to do if they have E-safety concerns and who to talk to. In most cases, this will be with their tutor. Where any report of an E-safety incident is made, all parties should know what procedure is triggered and how this will be followed up. Where appropriate, the Safeguarding Officer may intervene with appropriate additional support.

Safety Officer:

The E-safety Officer (who is also the Safeguarding Officer and Principal) is responsible for leading the E-safety policy and procedures, delivering staff development and training, recording incidents, reporting any developments and incidents to the Senior Management Team (SMT) and liaising with external agencies to promote E-safety within the College community. The E-safety Officer may also deliver workshops for students and staff where appropriate.

Students:

Students are responsible for using the College ICT systems and mobile devices in accordance with the College's Internet Acceptable Use Policy, which they must agree to and sign. 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. Students must act safely and responsibly at all times when using the internet and/or mobile technologies. If a student is a victim of cyber bullying this should also be reported to their tutor in the first instance.

Staff:

All staff are responsible for using the College ICT systems and mobile devices in accordance with the College Internet Acceptable Use Policy for staff and the E-safety Rules, which they must actively promote through embedded good practice. Staff are responsible for attending staff training on E-safety and displaying a model example to students at all times.

All digital communications with students must be carried out in line with the College communications policy and be professional in tone and content at all times. Online communication with students is restricted. Social networking sites should not be used by staff to make contact with students except in exceptional circumstances (e.g. gathering evidence for a cyber-bullying incident) and only then with prior written permission from the E-Safety Officer. Staff should not be 'friends' with current students of St. Andrew's College Cambridge on Facebook.

All staff should apply relevant College policies and understand the incident reporting procedures. Any incident that is reported to or discovered by a staff member must be reported to the E-safety Officer without delay. If a staff member is a victim of cyber bullying this should also be reported to the E-Safety Officer in the first instance.

**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 on social media, over the College network, will be monitored in line with the IT policy.

### 6. Risk Assessment

Any potential College wide issue arising from E-safety will be added to the College's Risk Register.

### 7. Behaviour

St. Andrew's College Cambridge will ensure that all users of technologies adhere to the standard of Behaviour as set out in the E-safety and Internet Acceptable Use Policy.
The College will not tolerate any abuse of ICT systems. Whether offline or online, communications by staff and students should be appropriate, 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 student and staff disciplinary codes.
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 and/or relevant external agencies.

### 8. 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 students.

All students and staff should be aware of the risks in downloading these 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, and these should be discussed within tutorial/lessons. The 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 relevant staff or student. Photographs of activities on the College premises should be considered carefully and have the consent of the Marketing Manager(s) before being published. If the person is identified by name, written consent should be sought.

### 9. Personal Information

Personal information is information about a particular living person. St. Andrew's College Cambridge collects and stores the personal information of students 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.

Employment references (for staff only) will only be completed where an employee confirms they wish the College to provide a reference to a specific external organisation. The College is legally obliged to disclose information regarding disciplinary action taken against an employee, also where there are concerns in relation to Safeguarding. The College will not disclose information in relation to sick absence or attendance asked on an employment reference.

No personal information can be posted to the College website without the permission of the Marketing Manager(s). Only names and work email addresses of some relevant staff will appear on the College website.

Staff must keep students' personal information safe and secure at all times. When using an online platform, all personal information must be password protected. Staff are not permitted to store personal information on removable storage devices e.g. USB memory sticks unless the devices are password protected. No personal information of individuals is permitted offsite unless the member of staff has the permission of the E-safety Officer. Every user of IT facilities is required to lock or log off on completion of any activity, or where they are physically absent from a device (e.g. desktop PC). Any College's mobile device (such as laptop) requires to be password protected. Where the personal data is no longer required, it must be securely deleted in line with the Data Protection Policy.

## 10. Education and Training.

With the current unlimited nature of internet access, it is impossible for the College to eliminate all risks for staff and students. It is our view therefore, that the College should support staff and students through training and education. This will provide them with the skills to be able to identify risks independently and manage them effectively.

For students:

Students will participate in an E-safety session in tutorials. This will take place at the beginning of a new College year. Issues associated with E-safety apply across the curriculum and students should receive guidance on what precautions and safeguards are appropriate when making use of the internet and technologies. Students should also know what to do and who to talk to where they have concerns about inappropriate content, either where material is directed to them, or where it is discovered as part of a random search. All the College's policies relating to ICT and E-safety will be available on the website.

Within classes, students will be encouraged to question the validity and reliability of materials researched, viewed or downloaded. They will also be encouraged to respect the copyright of other parties and to cite references properly.

For staff:

Staff will take part in E-safety training, usually as part of their induction training at the beginning of the new College year which will be led by the E-safety Officer. Further resources of useful guidance and information will be issued to all staff following the session.

Any new or temporary users will be asked to sign the College Staff Acceptable Use Policy and E-safety Rules.

Staff are also asked when they send emails to students to use the BCC so that the recipients cannot see the other emails, which will prevent usage of those emails for incorrect purposes.

## 11. 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 student wishes to report an incident, they can do so to their tutor or to the College E-safety Officer. Where a member of staff wishes to report an incident, they must contact the Principal. 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.

## 12. Feedback and Further Information

St. Andrew’s College Cambridge 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: Wayne Marshall Principal at wayne.marshall@standrewscambridge.co.uk.

Useful Links for Further Information:

Child Exploitation & Online Protection Centre http://www.ceop.police.uk

Internet Watch Foundation http://mobile.iwf.org.uk

DirectGov ‘Staying Safe Online’

http://www.direct.gov.uk/en/YoungPeople/CrimeAndJustice/KeepingSafe/DG_10027670

Get Safe Online http://www.getsafeonline.org

**Review:**

**September 2012, August 2013, August 2014, December 2014 and July 2015.**

**Next review: 1st August 2016.**