



ST. CATHERINE'S
COLLEGE
A CHURCH OF ENGLAND ACADEMY

E-Safety & Social Media Policy

Date approved: 22/01/18

Date to be reviewed: 21/01/2019

Version and Audit Control

Contents	Page
Introduction	3
Teaching and learning	3
Managing Internet access.....	3
Email	3
Published content and the College website	4
Publishing photographs, images and pupils work.....	4
Social networking and personal publishing on the College learning platform	4
Managing filtering	4
Managing the use of videoconferencing.....	5
Managing emerging technologies	5
Managing other devices	5
Protecting personal data	5
Policy.....	5
Assessing risk	5
Managing E-safety complaints	6
Community use of the internet	6
Communicating the policy to pupils.....	6
Communicating the policy to staff	6
Communicating the policy to parents	6

Introduction

The use of the internet, emails and social networking sites has grown considerably and has provided increased opportunities for teaching and learning. However, abuse of this technology, in terms of inappropriate use, is a concern and can give rise to disciplinary and/or safeguarding concerns.

The purpose of this policy is to ensure that-

- Pupils and employees are safeguarded
- The College is not exposed to legal risks
- College staff, including Governors, have clear guidelines on what they can and cannot do to keep themselves safe and protected against allegations
- Online conduct is exemplary in line with offline expectations
- The Headteacher can manage conduct effectively

Teaching and Learning- At St Catherine's College we are aware that the internet is an essential element in education and social communication in the 21st century.

- The College will provide pupils with quality internet access as part of their learning experience
- Internet use is part of the curriculum and a valued tool for staff and pupils
- The College's internet provider includes filtering systems appropriate to the needs and safety of the pupils
- Pupils will be taught what internet use is acceptable and will be educated in the effective use of the internet
- The College will ensure that internet derived materials comply with copyright law
- Pupils will be taught how to critically evaluate information before accepting its accuracy
- Staff will be mindful of the risks that the internet can pose to children in terms of a potential platform for grooming and radicalisation
- Pupils will be taught how to report inappropriate or offensive internet content using the CEOP Report Abuse icon



Managing Internet Access

- The College ICT security systems will be reviewed regularly
- Virus protection will be reviewed and updated

Email

- Pupils and staff will only be permitted to use approved email accounts on the College system
- Pupils must tell a member of staff if they receive an offensive email
- Staff must report if they receive an offensive email
- Pupils must not reveal personal details of themselves or others in email communication
- What is contained in an email may have to be released under the Data Protection Act or the Freedom of Information Act. Do not include information that may cause alarm, distress or embarrassment to yourself or the Colleg

- Always double check the correct email address has been entered
- If the email concerns an individual do not name them in the subject field
- The College email system will automatically add a confidentiality disclaimer to the footer of everyone's email.

Published content and the College web site

- The Headteacher will take overall responsibility and ensure that content is accurate and appropriate

Publishing photographs, images and work

- Photographs that clearly identify pupils will be carefully chosen and only used with the permission of the pupils and their parents
- Pupils names will not be published alongside their photographs if they are clearly identifiable
- Photographs will only be published if parents have signed their consent in the pupil diary
- Written permission will be obtained from staff prior to their photographs being used
- Parents should be clearly informed of the College policy on image taking and publishing

Social networking and personal publishing on the College learning platform

- The College will control access to social networking sites and ensure they educate pupils and parents in their safe use
- Staff and pupils will be advised not to share any personal details which may identify them or their location
- Staff should not link their social networking site to the College
- If professional networks are set up to provide pupils with information permission should be sought from the Headteacher and parents informed
- Staff must not communicate with pupils on social network sites and need to carefully consider befriending parents, carers and ex-pupils. If staff are also parents of pupils in College, it is advisable to inform the Personnel Manager so that appropriate safeguards can be put in place
- If staff use personal social networking sites, they should not post anything that could bring the College into disrepute
- If staff use personal social networking sites they should set the privacy settings to the highest level to ensure that personal and professional details are not in the public domain
- Pupils will be advised to use passwords, nicknames and avatars when using social networking sites

Managing filtering

- The College will work in partnership with East Sussex County Council to ensure systems used to protect children are reviewed and improved
- If staff or pupils come across inappropriate or offensive material, the site must be reported to the Head of Safeguarding

- The College will ensure that checks are made regularly, ensuring that filtering methods are effective and reasonable

Managing the use of videoconferencing

- Videoconferencing will be used via the College network to ensure security
- Pupils will only engage in videoconferencing with the permission of their teacher who will supervise the session

Managing emerging technologies

- With the constant changes in technology the College will ensure that new technologies will be risk-assessed before use in College is permitted

Managing other devices

- The sending of abusive, offensive or inappropriate material is not permitted
- Mobile phones and associated cameras will not be used during lessons except as part of an educational activity with the express permission of the teacher
- Staff should not share personal telephone numbers with pupils and parents, nor use personal email accounts for such communications

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1988

Policy

- All staff must read and sign the St Catherine's College 'Staff ICT Usage Policy' before being permitted to use any ICT College resource
- In addition, an online policy will also need to be read and accepted before log-ins are provided. This will be available to all staff including supply staff
- PGCE students will sign off the policy before being given a log in
- Parents will be asked to sign a consent form for pupils to access ICT
- All pupils, including school to school placements, must agree to comply with the responsible internet use before being granted internet access
- Any person not directly employed by the College, such as the school nurse, will sign an acceptable use of ICT form before being allowed access to the College site

Assessing Risk

- The College will ensure that all reasonable steps are taken to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that inappropriate material will never appear on a College computer. The College cannot accept liability for the material accessed, or the consequences of internet access.

- If inappropriate material is accessed, the College will review the E-safety policy to ensure that it is adequate

Managing E-safety complaints

- Complaints of internet misuse will initially be dealt with by the Head of Safeguarding
- All complaints about staff misuse will be referred to the Headteacher
- Staff must be aware that improper or unacceptable use of the internet or email system could result in legal proceedings and disciplinary procedures. Sanction depend on the gravity of the misuse and could result in dismissal
- Complaints of a child protection nature will be dealt with by the Head of Safeguarding in line with child protection procedures
- Pupils and parents will be informed of the potential consequences for pupils misusing the internet

Community use of the internet

- All use of the College's internet system by community or organisation users shall be in accordance with the College policy

Communicating the policy to pupils

- Elements of the E-safety policy will be shared with pupils
- E-safety rules and guidance will be posted in every networked classroom
- Pupils will be informed that internet and network use will be monitored
- The curriculum will provide opportunities for pupils to gain an understanding and awareness of e-safety issues and how to deal with them

Communicating the policy to staff

- All staff will be given a copy of the E-safety policy and will keep it in their safeguarding folder
- Staff will be aware that internet use will be monitored and traced to individual users.
- Staff who manage filtering systems or monitor ICT use will be supervised by a member of the senior team. Discretion and professional conduct is essential

Communicating the policy to parents

- The College's E-safety policy will be available on the College website.
- Parents and carers will be made aware of the policy through the College's newsletter 'Contact' and bulletins, such as twitter
- All new parents will be asked to sign the internet use agreement when their child registers at the College

This policy relies on staff acting responsibly. If staff have a concern that a colleague is acting in breach of this policy, they are encouraged to raise this with the Headteacher. If the concerns relate to the Headteacher, this should be shared with the Chair of Governors.

If the concern involves inappropriate interaction between a pupil and a member of staff a referral must be made to the Head of Safeguarding.