Cybersafety Use Agreement: St Andrew's College Staff

St Andrew's College

Section A: Important Cybersafety Initiatives and Rules

Section B: Staff Obligations Regarding Student Cybersafety

Section C: Cybersafety Managers

Important terms used in this document:

A. The abbreviation '**ICT**' in this document refers to the term 'Information and Communication Technologies';

B. '**Cybersafety**' refers to the safe use of the Internet and ICT equipment/devices, including mobile phones;

C. '**College ICT**' refers to the College's computer network, internet access facilities, computers, and other College ICT equipment/devices as outlined in (d) below;

D. The term '**ICT equipment/devices**' used in this document, includes but is not limited to; computers (such as desktops and laptops), storage devices (such as USB and flash memory devices), cameras (such as video, digital, webcams), all types of mobile phones, gaming consoles, video and audio players/receivers, and any other, similar, technologies as they come into use;

E. '**Objectionable**' in this agreement means material that deals with matters such as sex, cruelty, or violence in such a manner that it is likely to be injurious to the good of students or incompatible with a school environment. This is intended to be inclusive of the definition used in the Films, Videos and Publications Classification Act 1993.

***Section A:** St Andrew's College ICT Initiatives and Rules*

The College's computer network, internet access facilities, computers and other school ICT equipment/devices bring great benefits to the teaching and learning programmes at St Andrew's College, and to the effective operation of the College.

Our College has rigorous cybersafety practices in place, which include cybersafety use agreements for all school staff and students.

The overall goal of the College in this matter is to create and maintain a cybersafety culture which is in keeping with the values of the College, and legislative and professional obligations. This use agreement includes information about your obligations, responsibilities, and the nature of possible consequences associated with cybersafety breaches which undermine the safety of the College environment.

1. Cybersafety Use Agreements

   i. All staff, students and volunteers, that make use of the College's computer network, internet access facilities, computers and other ICT equipment/devices in the College environment, will be issued with a use agreement.

   ii. Staff are required to read these pages carefully, and on an annual basis signify agreement to the terms herein.

   iii. This agreement should be considered alongside the following policies, accessible via **SchoolDocs**:
   Social Media
   Privacy

   iv. The College's computer network, internet access facilities, computers and other College ICT equipment/devices are for educational purposes appropriate to the College environment. Staff may also use College ICT for professional development and personal use, which is both reasonable and appropriate to the College environment. This applies whether the ICT equipment is owned or leased either partially or wholly by the College and used on or off the College Campus.

2. The use of any privately-owned/leased ICT equipment/devices on the College Campus, or at any school-related activity must be appropriate to the College environment. This includes any images or material present/stored on privately-owned/leased ICT equipment/devices brought onto the College Campus, or to any school-related activity. This also includes the use of mobile phones.

3. When using College ICT, or privately-owned ICT on the College Campus or at any school-related activity, users must not:
   - initiate access to inappropriate or illegal material;
   - save or distribute such material by copying, storing, printing or showing to other people.

4. Users must not use any electronic communication (e.g. email, text, social media, etc) in a way that could cause offence to others or harass or harm them, put anyone at potential risk, or in any other way be inappropriate to the College environment.
5. Teaching staff are reminded to be aware of professional and ethical obligations when communicating via ICT with students both inside and outside school hours. Page 12 of Our Code Our Standards – https://stac.nz/EducationCouncilCode provides examples of behaviour that may breach the boundaries of ethical professional relationships with learners.
6. Users must not attempt to download, install or connect any software or hardware onto College ICT equipment/devices, or utilise such software/hardware, unless authorised by the Chief Information Officer (or their delegate).
7. Online publication of staff or student resources/work
   i. Educational resources and other information needed to be communicated to staff, parents and students may be published online using the College website or via the intranet. All published work must have an acceptable standard of presentation in terms of the College's publication guidelines, be appropriate, authorised and respect copyright laws.
   ii. The online publication of any material accessible by the general public must adhere to the requirements set out in the College's Community and Staff Social Media Policies, accessible via **SchoolDocs**.
   iii. The Ministry of Education guidelines – https://stac.nz/GuidelinesForSchools should be followed regarding issues of privacy, safety and copyright associated with student material which staff may wish to publish or post on the College website.
8. Privacy
   i. Staff members shall only publish audio or visual recordings, including postings on the internet /social media, which depict or refer to students or staff of the College on-site or at school activities off-site, in accordance to the requirements set out in the College's Staff Social Media policy – accessible via **SchoolDocs**.
   ii. No staff member may access from College network or ICT equipment/devices any material that is inappropriate, illegal, pornographic, offensive or in any way brings the school into disrepute.
9. All College ICT equipment/devices should be cared for in a responsible manner. Any damage, loss or theft must be reported immediately to the Chief Information Officer (or their delegate).
10. All users are expected to practise sensible use to limit wastage of computer resources or bandwidth. This includes avoiding unnecessary printing, unnecessary internet access, uploads or downloads.
11. The users of College ICT equipment and devices must comply with the Copyright Act 1994 and any licensing agreements relating to original work. Users who infringe copyright may be personally liable under the provisions of the Copyright Act 1994.
12. Passwords must be strong, kept confidential and not shared with anyone else. A strong password is at least eight characters in length with a mix of lower case (abc . . .) and upper case (ABC . . .) letters, symbols (#*@ . . .) and numerals (123 . . .).
13. Users should not allow any other person access to any equipment/device logged in under their own user account.
14. Incidents involving the unintentional or deliberate accessing of inappropriate material by staff or students:
    i. In the event of access of such material, users should not show others.
    ii. If an incident involves inappropriate material or activities of a serious nature, or is suspected of being illegal, it is necessary for the incident to be reported to the Cybersafety Manager **immediately**. See Section C for the relevant manager.
15. Any electronic data or files created or modified on behalf of St Andrew's College on any ICT, regardless of who owns the ICT, are the property of St Andrew's College. Staff may not profit from such data or files and must leave copies in the event of leaving the employment of the College.
16. Monitoring by St Andrew's College:
    i. The College may monitor traffic and material sent and received using St Andrew's ICT infrastructure.
    ii. The College reserves the right to deploy filtering and/or monitoring software where appropriate to restrict access to certain sites and data, including email.
    iii. Users must not attempt to circumvent filtering or monitoring.

17. The College reserves the right to monitor, and where appropriate, access and review all use of its computer network, internet access facilities, computers and other College ICT equipment/devices. This includes personal emails sent and received on the College's computers and/or network facilities at all times. The College may also commission an independent audit. If deemed necessary, this audit will include any stored content, and all aspects of its use, including email.

    Please note: conducting an audit does not give any representative of St Andrew's College the right to enter the home of College personnel, nor the right to seize or search any ICT equipment/devices belonging to that person, except to the extent permitted by law. St Andrew's may however request permission to audit privately owned ICT devices/equipment used on the College campus or at any school related activity.

18. Telephones and mobile phones
    i. All staff have access to the College phone system. In addition, some staff are issued with a College mobile phone. These phones are to be used primarily for College business, but provision is made to allow for reasonable personal use. All charges incurred as a consequence of usage deemed to be beyond a reasonable level must be paid for by the user.

19. College Databases
    i. Database passwords are personal and must not be disclosed to any other person, under any circumstances.
    ii. Database records must be kept confidential at all times, in accordance with the terms of the Confidentiality Agreement for users of College Databases – https://stac.nz/ConfidentialityAgreement.
    iii. Users must log out of the database on completion of tasks and ensure the database is not left open.

20. Cloud Services
    i. The use of any cloud hosted (online) services must be approved by the Chief Information Officer (or their delegate). This is to ensure that checks are carried out to verify that the online service provider can demonstrate adherence to New Zealand legislation regarding data handling, and that accurate records of online service usage can be maintained. Furthermore, this approach is critical to understanding where needs are not being met by existing services, so that a new service might be brought into the College's ICT application portfolio for the benefit of all staff.

21. Procurement
    i. All software and ICT equipment/devices must be procured in consultation with the ICT department, and with the approval of the Chief Information Officer (or their delegate).

22. The College requests your permission to take a photograph of you for staff directory and staff ID card purposes. You will be contacted by the Communications Department if it was proposed that your image was to be used in any promotional material. By signing this agreement, you give your consent for your photograph to be taken.

23. Breaches of the agreement
    i. A breach of the use agreement may constitute a breach of discipline and may result in a finding of serious misconduct. A serious breach of discipline would include involvement with objectionable material, antisocial activities such as harassment or misuse of the College ICT in a manner that could be harmful to the safety of the College or call into question the user's suitability to be in a school environment.
    ii. If there is a suspected breach of the use agreement involving privately-owned ICT on the College campus or at a school-related activity, the matter may be investigated by St Andrew's College. St Andrew's College may request permission to audit that equipment/device(s) as part of its investigation into the alleged incident.
    iii. Involvement with material which is deemed 'objectionable' under the Films, Videos and Publications Classification Act 1993 is serious, and in addition to any inquiry undertaken by the school, the applicable agency involved with investigating offences under the Act may be notified at the commencement, during or after the school's investigation.

24. Queries or concerns
    i. Staff should take any queries or concerns regarding technical matters to the Chief Information Officer (or their delegate).
    ii. Queries or concerns regarding other cybersafety issues should be taken to the Cybersafety Manager, Chief Information Officer (who may be the Cybersafety Manager), or to the Rector.
    iii. In the event of a serious incident which occurs when the Cybersafety Manager and the Rector are not available, another member of senior management should be informed immediately.

Section B: Staff Requirements regarding Student Cybersafety

1. Staff have the professional responsibility to ensure the safety and well-being of children using the College's computer network, internet access facilities, computers and other College ICT equipment/devices on the College campus or at any school-related activity.

2. Staff should guide students in effective strategies for searching and using the internet.

3. While students are accessing the internet in a classroom situation, the supervising staff member should be an active presence.

4. Staff should support students in following the student use agreement. This includes:
    i. Endeavouring to check that all students in their care understand the requirements of the student agreement.
    ii. Regularly reminding students of the contents of the use agreement they have signed and encouraging them to make positive use of ICT.

Section C: Cybersafety Managers

The current Cybersafety Managers for staff at St Andrew's College are:

Secondary	**Evert van Florenstein** (Head of Secondary School)
Primary	**Jonathan Bierwirth** (Preparatory School Principal)
Non-Teaching	**Dave Hart** (Chief Information Officer)