

	COMMUNICATIONS & INFORMATION SECURITY
	POLICY
	VERSION 1.1

1. INTRODUCTION

St Andrew's is the owner and the custodian of information (some of which is personal to the learners and their parents) and information systems critical to its business as an educational institution. The Board of Governors requires that appropriate safeguards for the information are established and implemented.

The increasing use of information systems including, but not limited to, computers, cellular technologies, the Internet and email, in the education provided by St Andrew's and in St Andrew's administration, requires that members of the St Andrew's community understand their responsibilities and obligations in using information and information systems provided by St Andrew's

This policy applies to all users of information and information systems owned, or under the control of St Andrew's. It shall also apply to information communication devices (including cellular telephones) or storage media used to gain access to any St Andrew's information or information system's, as well as facilitate communication from St Andrew's campus.

The provisions of this policy shall apply to the following entities in the St Andrew's community:

- The Board of Governors, by virtue of their fiduciary relationship to St Andrew's;
- The educators and administrative staff employed by St Andrew's, as part of their contract of employment;
- The learners, by their acceptance of this and related policies, duly assisted by a parent;
- The parents, by their acceptance of this and related policies.

2. PURPOSE

The purpose of this policy is to establish the principles governing:

- the communication of information owned by, or under the control of St Andrew's; and
- to safeguard the information and information systems under the control of St Andrew's.

3. POLICY STATEMENTS

General

3.1 The basis of this policy is that information shall:

- be available to persons authorised by the owner to have access to the information;

- remain confidential to authorised persons and not be disclosed to persons not authorised by the owner to have access to the information; and
 - be protected from unauthorised or accidental amendment.
- 3.2 The Head has established an Information Security Forum, which is charged with the responsibility of implementing, monitoring and enforcing good information security practices at St Andrew's. These practices shall be incorporated in this policy and in related policies, procedures, standards and guidelines, published by St Andrew's from time to time.

Ownership and Classification of Information

- 3.3 All information owned or controlled by St Andrew's shall be assigned an owner, who shall determine who shall be entitled to gain access to the information.
- 3.4 All information shall be deemed to be "confidential", for use internally within St Andrew's, unless it has been assigned a more restricted classification or has been classified as "public information".
- 3.5 Any person who intentionally accesses or attempts to access information to which they are not authorised, may be subject to disciplinary action or any other legal remedies available to St Andrew's.
- 3.6 Unauthorised access to, interception of, or interference with information, constitutes a criminal offence. Where appropriate the Information Security Forum may recommend the institution of criminal proceedings, to protect the information under St Andrew's control and to safeguard the learners from potential danger or abuse.

Access

- 3.7 The Information Security Forum shall govern access to St Andrew's information and information systems. It shall, in its absolute discretion, grant and/or revoke access to St Andrew's information or information systems.
- 3.8 Access to St Andrew's information systems shall be protected by the allocation of user identities to authorised users and the selection of passwords by the users. The passwords shall conform to rules established by the Information Security Forum and communicated to users from time to time.
- 3.9 Passwords are confidential and users shall take all reasonable steps to safeguard their confidentiality.
- 3.10 Under no circumstances shall a user disclose his or her password to another person or record the password in a manner that would allow it to be accessed and used by another person.
- 3.11 No user shall request or use the password of another user. If a user is requested to disclose their password, regardless of the authority or the requestor, they shall immediately report this to the systems administrator or a member of the Information Security Forum. A request for another user's password shall be regarded as a serious breach of this policy and may be subject to disciplinary action.
- 3.12 Any access to an information system under St Andrew's control and all activity on the information system using the user identity assigned to, and the password selected by, a user shall be attributed to the user and the onus of proving the contrary shall be on the user.

- 3.13 Any user, who suspects that his or her password, or that of any other user, has become known to a person other than the authorised user, shall immediately report this suspicion to the system administrator.
- 3.14 Failure by a user to ensure confidentiality of his or her password may, if discovered, lead to immediate suspension of access by the user to St Andrew's information systems and such disciplinary action as may be appropriate.
- 3.15 All users shall:
- ensure, if information to which they are not authorised is accessed, that it will not be distributed to any other person;
 - report the fact they have gained access to information without authorisation to the system administrator;
 - report any unauthorised access by a third party of St Andrew's information or its information systems to the systems administrator.
- 3.16 Any user who has accessed an information system under the control of St Andrew's shall:
- not leave the computer or device used to access the information system unattended without activating a screen saver password; and
 - on completion of the task, immediately log off the information system.

Third Party Access

- 3.17 Save for persons employed by St Andrew's or enrolled as a learner at St Andrew's, no person shall be granted access to information or information systems under the control of St Andrew's, without the prior written authorisation of the Information Security Forum and such person having entered into a written agreement governing the conditions of such access.

Remote Access

- 3.18 No person shall be granted access to information systems under the control of St Andrew's using any computer or device not under the direct control of St Andrew's, without the prior written authorisation of the Information Security Forum and such person having entered into a written agreement governing the conditions of such access.

Use

- 3.19 The use of any information or information system under the control of St Andrew's shall be lawful, professional, ethical and conform to the provisions of this policy and any information security standards, procedures or guidelines that may be implemented by the Information Security Forum from time to time.
- 3.20 Use of the St Andrew's information systems and all information that may be accessed or communicated using the information systems, is provided to users primarily to assist in their education, or the execution of their tasks appropriate to their relationship with St Andrew's. While limited personal use may be permitted, this shall be at the absolute discretion of the Information Security Forum, which may delegate its authority to persons designated by it to determine what personal use is appropriate in any given circumstances.

- 3.21 Personal use shall be limited to use expressly authorised, incidental and occasional and shall not:
- interfere with the user's assigned work or performance of their duties;
 - interfere with any other user's work or the performance of their duties;
 - interfere with the operation of the St Andrew's information system; or
 - be contrary to the provisions of this policy, any other related policy, procedure, or standard published in terms of this or any other related policy.

Viruses

- 3.22 Viruses are the primary cause of disruption of information systems and, if not dealt with correctly and promptly, may cause both financial and indirect loss to St Andrew's. Care in use of email (dealt with later in this policy) and downloading of software are important protections in the avoidance of viruses.
- 3.23 No user shall download any software from any storage medium, the Internet or any other source, onto information systems under the control of St Andrew's. Only the systems administrator or persons designated by the systems administrator, in writing, shall be entitled to download any software onto St Andrew's information systems.
- 3.24 Any software that may reasonably required by a user shall be provided or referred to the systems administrator who shall supervise the checking and secure installation of the software onto the appropriate information system.

Internet use

- 3.25 St Andrew's encourages use of the Internet for the purpose of education and research. However, users shall exercise care to ensure that their use falls within the provisions of school policies generally, and, in particular, this policy.
- 3.26 No user shall, without the prior written consent of the Information Security Forum, use the information systems provided by St Andrew's to enter into any commercial transaction. If the required consent is granted, St Andrew's shall not be liable for any loss of whatever nature that may be suffered by the user in using it's information systems.
- 3.27 No user may attempt to unblock websites which the school has denied users access to via the firewall. Any attempt to unblock such websites will result in disciplinary action. Users who require access to a website which may be blocked can request access from the computer department, if the website is deemed safe and is required for educational purposes.
- 3.28 Users shall not use the St Andrew's Information System to:
- display, download or communicate any material, which is sexually explicit, obscene, discriminatory, racially or religiously prejudicial, defamatory, or may constitute an infringement of a third parties intellectual property rights;
 - communicate their own, or any third parties, photograph or personal information including but not limited to, telephone or mobile numbers, physical addresses or email addresses;

- subscribe to or participate in Chat Groups, Bulletin Boards, Newsgroups or Discussion Groups without the prior written authorisation of the systems administrator;
- surf the World Wide Web without purpose. Any St Andrew's teacher or the system administrator shall be entitled at any time to request that the history of any connection to websites be disclosed.
- communicate any information relating to St Andrew's, its learners or their parents, without the prior written consent of the Information Security Forum or the owner of the information.

E-mail and voice communication

3.29 Users shall not use St Andrew's information system for excessive personal voice or email communication.

3.30 Users shall not use St Andrew's information systems to:

- subscribe to or access any email system which is not the standard email system provided by St Andrew's.
- initiate or forward chain messages;
- initiate or forward unsolicited email;
- send numerous emails with the intention of disrupting or inconveniencing the recipient;
- access the email accounts of other users;
- communicate any information that is confidential to St Andrew's;
- communicate any material, which is sexually explicit, obscene, discriminatory, racially or religiously prejudicial, defamatory, or may constitute an infringement of a third parties intellectual property rights;
- communicate any files in excess of the size designated by the system administrator from time to time;
- open emails received from an unknown source.

3.31 Users shall immediately report to the system administrator emails received from an unknown source, chain messages, unsolicited mail, any suspicion of unauthorised access to email accounts, or the receipt of any material, which is sexually explicit, obscene, discriminatory, racially or religiously prejudicial, defamatory, or may constitute an infringement of a third parties intellectual property rights.

3.32 Users shall not retain email for a period longer than is required for it's immediate use. Should it be necessary to store emails arrangements should be made with the system administrator to provide appropriate storage for emails.

Cellular phones or other information storage and computer devices

- 3.33 No information confidential to St Andrew's or its learners shall be downloaded, displayed or communicated or removed from St Andrew's using cellular phones, other computer devices or storage media without the prior consent of the owner of the information or the systems administrator.
- 3.34 Teachers or the system administrator shall have the right to check that information under the control of St Andrew's or accessed from its information system has not been downloaded onto any cellular phone, computer device or storage media.
- 3.35 Cellular phones are to be used only in compliance with St Andrew's "Acceptable Use of Electronic Communication Devices Policy".

4. PRIVACY OF PERSONAL INFORMATION

- 4.1 St Andrew's shall adhere to legislation protecting the privacy of personal information.
- 4.2 St Andrew's shall collect, process, store and communicate personal information of the learners or their parents for the purposes of providing education to learners, administering the activities that learners may participate in and administering the business of St Andrew's. Disclosure of personal information to third parties, unless required in terms of law, shall not be made without the prior consent of one of the learners' parents.
- 4.3 St Andrew's shall use its best endeavours to protect personal information from unauthorised disclosure to third parties but shall not be liable any damages suffered by a learner or parent resulting from any inadvertent disclosure of personal information.
- 4.4 A parent shall be entitled to have sight of any personal information of the learner or their own personal information, collected or stored by St Andrew's and shall be entitled to require St Andrew's to correct any incorrect information.
- 4.5 St Andrew's shall destroy personal information no longer required and/or that it is not obliged to retain by law.
- 4.6 St Andrew's shall be entitled to use personal information for the purpose of processing statistical data or profiling groups of learners provided that the aggregated information cannot be linked to the identity of a particular learner or the learners parent.
- 4.7 St Andrew's shall use personal information to facilitate communication with learners, individual parents and the parent body. St Andrew's cannot guarantee the secure communication of this information and while it shall use commercially reasonable efforts to provide secure communication it shall not be liable for inadvertent disclosure of information as a result of the interception of communications containing personal information.
- 4.8 The learner and learner's parent/s in accepting this policy consent to St Andrew's use of their personal information for the purposes stated and in the manner described in the policy.

5. CONSENT TO INTERCEPTION AND MONITORING OF COMMUNICATIONS

- 5.1 Users acknowledge that the provisions of this policy are intended to safeguard information generated, stored and communicated using the St Andrew's information systems. Further, to safeguard the safety and well-being of St Andrew's learners.
- 5.2 Users acknowledge that to provide the intended safeguards that it may be necessary that information generated, stored and communicated using the St Andrew's information systems be intercepted and monitored by the systems administrator on the authority of the Information Security Forum.
- 5.3 By signing or accepting this policy users (where necessary assisted by their parents) consent to the interception and monitoring of information generated, stored or communicated using St Andrew's information systems.
- 5.4 No information that may be intercepted or monitored shall be disclosed by the systems administrator to any persons other than the Head and those persons appointed by the Head to the Information Security Forum.
- 5.5 The information intercepted and monitored shall not be used for any purposes other than disclosure to parents, disciplinary action, or, if required by law, disclosure to third parties.

6. ENFORCEMENT OF POLICY

- 6.1 The terms of this policy shall have the force of a contractual agreement between St Andrew's, its employees and its learners (duly assisted by their parents), as the case may be.
- 6.2 This policy shall be enforced by those parties appointed by the Head to do so.
- 6.3 If disciplinary proceedings are appropriate they will:
 - 6.3.1 in the case of St Andrew's learners, be conducted in accordance with the procedures established in the Acceptable Conduct Policy agreed to by the learners (duly assisted by their parents);
 - 6.3.2 in the case of persons employees of St Andrew's, be conducted in terms of the disciplinary procedures established by St Andrew's Board of Governors and employment agreements entered into with employees.

7. RELATED POLICIES, STANDARDS, PROCEDURES AND GUIDELINES

- 7.1 Acceptable Conduct Policy
- 7.2 Information Security Procedures, Standards and Guidelines;
- 7.3 Acceptable Use of Electronic Communication Devices Policy

8. GLOSSARY OF TERMS

Unless inconsistent with the context, the expressions set out in this policy will have the meanings assigned to them in the glossary of terms applicable to all policies, procedures, standards and guidelines adopted and published by St Andrew's. The Glossary of terms shall be available on the St Andrew's website, www.standrews.co.za , or from the personal assistant to the Head, in either physical or electronic form.