POLICY: IT ACCEPTABLE USE POLICY

Introduction

1. The purpose of this document is to ensure that all users (employees, contractors, volunteers, students, visitors, etc.) of Waterford computing facilities are aware of Waterford's policies relating to their use. Effective and proper use of information technology is fundamental to the successful and efficient running of Waterford. However, misuse of information technology - in particular misuse of e-mail and access to the Internet - exposes Waterford to liability and is a drain on time and money. It is critical that all users read and understand this document and make themselves aware of the risks and exposure involved.
2. It is the responsibility of all users of Waterford computing facilities to be aware of and follow all Waterford IT policies and guidelines and to seek advice in case of doubt.
3. This policy may be updated or supplemented by specific standards or procedures to reflect further developments in technology or legislation or other relevant changes.
4. Waterford encourages the use of School computing facilities for the mutual benefit of Waterford and its employees and pupils. Similarly the regulations that constitute this policy seek to provide for the mutual protection of Waterford and the rights of its employees and students.
5. Waterford staff should not unnecessarily store sensitive pupil information on personal devices.

Computing facilities

6. Access to school computing facilities is managed by Technical Support. Use of any of Waterford computing facilities is at the discretion of Waterford.
7. Definition: The phrase 'Computing Facilities' as used in this policy shall be interpreted as including any computer hardware or software owned or operated by Waterford and any allocation of time, memory, disk space or other measure of space on any of Waterford hardware, software or networks.
8. Ownership: Computing facilities owned by Waterford and software and/or data developed or created (for whatever reason) on that equipment remains in all respects the property of Waterford.
9. Desktop PCs: are a critical asset to Waterford and must be managed carefully to maintain security, data integrity and efficiency. Users must consult Technical Support before installing non-standard software on computers managed by Technical Support as a Desktop PC. For clarification of a machine's status as a 'Desktop PC' or what software is permitted please consult Technical Support. All users have access to appropriate areas on Waterford file servers for the secure storage of valuable files. Valued documents and files should not be stored on Desktop PCs. Files stored on Desktop PCs are at risk of loss through hardware/software failure or automated administrative activity. Desktop PCs include the CPU/hard-drive unit and monitor both of which are recorded components and further, are subject to change control. Users must contact Technical Support in order to perform a 'swap' of these assets.
10. Portable PCs (laptops):
    - 10.1. Laptops are at high risk from loss or theft and require additional security protection. All reasonable precautions must be taken to ensure that hardware is stored securely. Also, to protect the integrity of Waterford systems and data procedures, passwords or authentication devices for gaining remote access to Waterford systems must not be stored with the computer. This includes the saving of passwords into remote access software.
    - 10.2. Highly confidential data can be encrypted to protect it in the event of Portable PC loss. Technical Support can help with this process. If a Portable PC is lost or stolen Technical Support must be notified as soon as possible and a report made to the police.
11. Mobile Technologies: Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for students. Many existing mobile technologies such as portable media players, PDAs, gaming devices,

mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Waterford chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

12. Personal Mobile Devices (including phones):
    12.1. The school allows staff to bring in personal mobile phones and devices for their own use.
    12.2. Students are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time.
    12.3. The school is not responsible for the loss, damage or theft of any personal mobile device
    12.4. The sending of inappropriate text messages between any member of the school community is not allowed.
    12.5. Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
13. School Provided Mobile Devices (PDA) (including phones):
    13.1. The sending of inappropriate text messages between any member of the school community is not allowed.
    13.2. Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used.
14. Software: Only software properly purchased and/or approved by Technical Support may be used on School hardware, except in certain circumstances. Non-standard or unauthorised software can cause problems with the stability of corporate computing hardware and it is necessary to contact Technical Support before the installation of such software. Software or shareware may be downloaded from the Internet or loaded from other sources (e.g. CDROM) when necessary, however it is the responsibility of the individual to ensure that any licensing issues are addressed promptly, either by on-line registration or the purchasing of a valid licence through Technical Support. The use or copying of software without the licensor's permission is illegal and equally the terms and conditions of software licences must always be adhered to. Whilst it is the user's responsibility to take reasonable care over the configuration of their computer hardware, it is possible for software to be installed on a machine without the full comprehension of the user. Users discovering software that has been installed in an unsolicited manner and which contravenes the licensing regulations above are encouraged to contact Technical Support who will be happy to assist in resolving any issues.
15. Data security: Users must only access information held on Waterford computer systems if properly authorised to do so and the information is needed to carry out your work. Under no circumstances should personal or other confidential information held on computer be disclosed to unauthorised persons. The unauthorised access to and/or unauthorised modification of data is a criminal offence. It is School policy to store data on a network drive where it is regularly backed up. Users must ensure that data that is not stored on the network file server is regularly backed up.
16. Anti-virus software: Anti-virus software is loaded on all computers as standard and is updated regularly via the network. Antivirus software must not be de-installed or deactivated. Files received by or sent by e-mail are checked for viruses automatically. Staff using their own equipment are responsible for maintaining up to date virus definitions on their computers and can contact Technical Support for help as required. Users must not intentionally access or transmit computer viruses or similar software. Non-Waterford software or data files intended to be run on School equipment by external people such as engineers or trainers must be checked for viruses before use. If it is suspected that a virus has infected a computer then stop using the computer and contact Technical Support immediately.
17. Network access and Security: Passwords protect Waterford systems from access by unauthorised people: they protect user's work and the School's information. Therefore a user's network password should never be disclosed to anyone else. Procedures are in place on systems to ensure users change passwords on a regular basis, passwords are of a minimum

length and old passwords cannot be reused immediately. Passwords must be eight or more characters long and include at least one numeric or non-alphabetic special character. The connection of non-Waterford computer equipment to the network without prior written request and technical approval is not allowed. This includes connection via dialup or Virtual Private Networking (VPN).

18. Further general guidance: Waterford users must ensure prior approval at a Head of Department level to:
    18.1. set-up world wide web sites on Waterford computing facilities
    18.2. publish pages on external world wide web sites containing information relating to Waterford
    18.3. enter into agreements on behalf of themselves or Waterford via a network or electronic system
    18.4. transmit unsolicited commercial or advertising material to other users of a network or to other organisations
    18.5. be used for external business interests or personal gain

Electronic mail

19. Use and responsibility: Waterford electronic mail (e-mail) system is provided for the School's business purposes. E-mail is now a critical business tool but inappropriate use can expose Waterford and the user to significant liability. Liability can arise in a number of ways including, among others, copyright or trademark infringement, misuse of confidential information, defamation and liability for inaccurate statements. The e-mail system costs the School time and money, it must be used judiciously in the same manner as other School resources such as telephones and photocopying. School-wide e-mail messages must be business related and of significant importance to all employees.
20. Content:
    20.1. E-mail messages must be treated like any other formal written communication.
    20.2. E-mail messages cannot be considered to be private, secure or temporary.
    20.3. Email can be copied and forwarded to numerous recipients quickly and easily and it should be assumed that they could be read by anyone.
    20.4. Improper statements in e-mail can give rise to personal liability and liability for Waterford and can constitute a serious disciplinary matter. E-mails that embarrass misrepresent or convey an unjust or unfavourable impression of Waterford or its business affairs, employees, suppliers, customers or competitors are not permitted.
    20.5. Do not create or send e-mail messages that are defamatory. Defamatory e-mails whether internal or external can constitute a published libel and are actionable.
    20.6. Never send confidential or sensitive information via e-mail. E-mail messages, however confidential or damaging, may have to be disclosed in court proceedings.
    20.7. Do not create or send e-mail messages that may be intimidating, hostile or offensive on the basis of sex, race, colour, religion, national origin, sexual orientation or disability.
    20.8. It is never permissible to subject another employee to public humiliation or ridicule; this is equally true via e-mail.
    20.9. Copyright law applies to e-mail. Do not use e-mail to transmit or circulate copyrighted materials.

21. Communication with students: When communicating with students by email school staff should preferably use their school email accounts. More importantly, all communications can be checked for appropriateness in the event of a complaint being lodged against a member of staff. The key to these recommendations is that all communications should be open.

Internet usage

22. The laws of all nation states regulating such diverse subjects as intellectual property, fraud, defamation, pornography, insurance, banking, financial services and tax apply equally to on-line activities. However, the practical legal position regarding Internet usage is often uncertain.
23. Strictly, documents must not be published on the web which are defamatory or which may constitute intimidating, hostile or offensive material on the basis of sex, race, colour, religion, national origin, sexual orientation or disability under the sovereign law of the country in which the web server hosting the published material is sited.
24. Strictly, material must not be accessed from the web which would be objectionable on the above grounds under the sovereign law of the countries in which the networks transporting the material are sited or which would violate the Acceptable Use Policies of those networks.
25. Given the impracticality of assessing the exact legal position with regard to the previous two paragraphs, Waterford Acceptable Use Policy governing material that could be objectionable on the above grounds, is grounded in Swazi law and appropriate international laws, on which basis it is reasonable to expect Waterford employees to have good awareness and to be able to exercise good judgement. If in doubt over a case please escalate through your Head of Department.
26. Once information is published on the worldwide web anyone from anywhere in the world can access it. It is therefore critical that material of a proprietary or sensitive nature should not be published on unsecured public web sites.
27. All Internet usage from the Waterford network is monitored and logged. Reporting on aggregate usage is performed on a regular basis.
28. When specific circumstances of abuse warrant it, individual web sessions will be investigated and linked to the relevant user account. Such an investigation may result in action via Waterford School's Disciplinary Procedure and possibly criminal investigation.
29. Copyrights and licensing conditions must be observed when downloading software and fixes from the web sites of authorised software suppliers. Files so protected must never be transmitted or redistributed to third parties without the express permission of the copyright owner.
30. Newsgroups: Postings to newsgroups are in effect e-mails published to the world at large and are subject to the same regulations governing email as above. Always include a disclaimer with a posting if it could be interpreted as an official statement or policy of Waterford. For example: "The views expressed are my own and do not necessarily represent the views or policy of my employer."
31. Instant messaging: Instant messaging is free, fast, real-time and powerful. However instant messaging also carries inherent risks: lack of encryption (allowing the possibility of eavesdropping) logging of chat conversations without a user's knowledge and virus risks. Due to these risks, Waterford does not currently allow the use of instant messaging for the communication of sensitive or proprietary School information.
32. Managing Other Web 2 Technologies: Web 2, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, students are encouraged to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.
    32.1. At present, the school endeavours to deny access to social networking sites to students within school
    32.2. All students are advised to be cautious about the information given by others on sites, for example users not being who they say they are
    32.3. Students are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online

32.4. Students are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)
32.5. Our students are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals
32.6. Students are encouraged to be wary about publishing specific and detailed private thoughts online
32.7. Our students are asked to report any incidents of bullying to the school
32.8. Staff may only create blogs, wikis or other web 2 spaces in order to communicate with students using the Learning Platform or other systems approved by the principal.

Private use, legislation and disciplinary procedures

33. Private use: Computing facilities are provided for Waterford business purposes and responsible personal use is allowed provided there is no conflict with the interests or requirements of Waterford. Waterford does not accept liability for any personal loss or damage incurred through using the School computing facilities for private use.
34. Disciplinary and related action: Waterford wishes to promote the highest standards in relation to good practice and security in the use of information technology. Consequently it expects and supports the integrity of its employees. In exceptional circumstances, where there are reasonable grounds to suspect that an employee has committed a serious criminal offence, the police will be informed and a criminal prosecution may follow.
35. Privacy: E-mail messages to or from Waterford users cannot be considered to be private or confidential. Although it is not policy to routinely examine the content of individuals' e-mail, Waterford reserves the right to monitor messages, at any time, for specific instances in which there is good cause for such monitoring or some legal obligation to do so. Good cause shall include the need to fulfil School obligations, detect employee wrongdoing, protect the rights or property of the School, protect IT system security or to comply with legal process. Messages sent or received may be copied and disclosed by the School for lawful purposes without prior notice. It is not permissible to access or to send e-mail from another employee's personal account either directly or indirectly. Internet usage via any connected device is also governed by the previous statements in this paragraph, that is, it cannot be considered private when connected to the Waterford network and that usage may be monitored and logged.

Incident Reporting

36. Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's management. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to IT Director. Some incidents may need to be recorded in other places.

Approved by CMG: 2016-04-04

Appendix 1: Examples of behaviours which require the use of the Waterford disciplinary policy

1. This list is not exhaustive, but sets the framework of Waterford's approach to the misuse of the computing systems. Waterford has the right to monitor employees use of computer equipment.

2. Gross misconduct:
   2.1. Criminal Acts – for example in relation to child pornography.
   2.2. Visiting pornographic sites or any sexually explicit material, except where this forms an authorised part of the employees job, e.g. testing the filtering system.
   2.3. Harassment – inappropriate e-mails or printed e-mails sent to a colleague, even if sent as a joke. Harassment can take a number of forms and is defined as unwanted conduct that affects the dignity of people within the workplace.
   2.4. Obscene racist jokes or remarks which have been shared internally and externally – reflects on the image of employer and brings the organisation into disrepute.
   2.5. Downloading and installation of unlicensed products.
   2.6. Chat rooms – sexual discourse, arrangements for sexual activity.
   2.7. Attempting to bypass the school's filtering system or assisting someone to do so.
   2.8. Deliberate introduction of viruses to systems.

3. Misconduct:
   3.1. Frivolous use of School computing facilities that risk bringing Waterford into disrepute. The distribution of 'chain e-mails' beyond the internal e-mail system would represent examples of such misconduct.
   3.2. Entering into contracts via the Internet that misrepresent Waterford. Contracts are legally binding agreements and an employee must not enter into any agreements via the Internet to procure goods or services where Waterford is liable for this contract.