REED'S
School

Staff Information Technology (IT) Acceptable Use Policy

1. Introduction

1.1 The purpose of this document is to ensure that all staff users of Reed's School computing facilities are aware of the policies relating to their use. Effective and proper use of information technology is fundamental to the successful and efficient running of Reed's. However, misuse of information technology - in particular misuse of e-mail and access to the Internet - exposes Reed's to liability and is a drain on time and money.

1.2 It is the responsibility of all users of Reed's School computing facilities to be aware of and follow Reed's School's Acceptable Use Policy.

1.3 Access to educational computing facilities is managed by the IT Department. Use of any of Reed's School computing facilities is at the discretion of the IT Department.

2. Definition

2.1 The phrase 'Computing Facilities' as used in this policy shall be interpreted as including any computer hardware or software owned or operated by Reed's School and any allocation of time, memory, disk space or other measure of space on any of Reed's School hardware, software or networks.

3. Desktop PCs

3.1 Desktop PCs are a critical asset to Reed's School and must be managed carefully to maintain security, data integrity and efficiency. Users must consult the IT Department before installing non-standard software on computers managed by the IT Department as a Desktop PC. For clarification of a machine's status as a 'Desktop PC' please consult The IT Department. Non-standard software shall be interpreted as any software that does not comply with the regulation of the 'Software' sub-section below.

3.2 All users have access to appropriate areas on Reed's School file servers for the secure storage of valuable files. Valued documents and files should not be stored on Desktop PCs.

3.3 Files stored on Desktop PCs are at risk of loss through hardware/software failure or automated administrative activity.

3.4 Wherever possible material should be saved to Office 365 cloud based storage.

4. Laptop PCs/iPads/Mobile Electronic Devices

4.1 Laptop PCs/iPads/mobile electronic devices that belong to the school are at high risk from loss or theft and require additional security protection. All reasonable precautions must be taken to ensure that such hardware is stored securely. Also, to protect the integrity of Reed's School systems and data procedures, passwords or authentication devices for gaining remote access to Reed's School systems must not be stored with the computer. This includes the saving of passwords into remote access software. If your Laptop PCs/IPads/Mobile electronic device is lost or stolen, the IT Department must be notified as soon as possible and a report made to the police and the Estates and Facilities Director.

5. Loan Equipment

5.1 The policy regarding loan equipment is similar to that for Laptop PCs/iPads/Mobile electronic devices. Most loan equipment is highly portable and attractive to thieves. Users who borrow loan equipment bear the responsibility for its care. Loan equipment should be concealed and stored securely when not in use.

5.2 If loan equipment is stolen or lost, the IT Department must be notified as soon as possible and a report made to the police and the Facilities Manager.

6. Software

6.1 Only software properly purchased and/or approved by the IT Department may be used on Reed's School hardware. Non-standard or unauthorised software can cause problems with the stability of computing hardware. Software or shareware may be downloaded from the Internet or loaded from other sources (e.g. CD-ROM) 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 the IT Department. 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.

6.2 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 must contact the IT Department who will assist in resolving any issues.

7. Data Security

7.1 You must only access information held on Reed's School computer systems if you have been properly authorised to do so and you need the information to carry out your work. Under no circumstances should you disclose personal or other confidential information held electronically to unauthorised persons. The unauthorised access to and/or unauthorised modification of data is a criminal offence under the Computers' Misuse Act 1990.

7.2 It is school policy to store data on a network drive where it is regularly backed up. You must ensure that data that is not stored on the network file server is regularly backed up on Cloud storage.

8. Virus Protection

8.1 Anti-virus software is loaded on all computers as standard and is updated regularly via the network. Anti-virus software must not be de-installed or deactivated. Files received by or sent by e-mail are checked for viruses automatically. Remote users are responsible for maintaining up to date virus definitions on their computers and can contact IT for help as required.

8.2 Users must not intentionally access or transmit computer viruses or similar software.

8.3 Non-Reed's School 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 you suspect that a virus has infected a computer you will need to stop using the computer and contact the IT Department immediately.

9. Network Access

9.1 Passwords protect Reed's School systems from access by unauthorised people: they protect your work. Therefore you must never give your network password to anyone else.

9.2 Passwords must be eight or more characters long and include at least one numeric or non-alphabetic special character to make them complex.

9.3 Reed's School does not allow the connection of non-school computer equipment to the network without authorisation from the Network Manager.

10. Electronic Mail

10.1 Reed's School electronic mail (e-mail) system is provided for educational purposes. E-mail is now a critical working tool but inappropriate use can expose Reed's School and the user to significant liability. Liability can arise in a number of ways including, among others, misuse of confidential information, defamation and liability for inaccurate statements.

10.2 The e-mail system costs the organisation time and money and it must be used judiciously in the same manner as other organisational resources such as telephones and photocopying.

10.3 Group e-mail messages should be school related and relevant to all recipients.

10.4 Reed's School Staff are encouraged to activate their own 'Out Of Office' message before going on trips or activities. This message can also be activated remotely from Outlook Web Access if you are ill.

10.5 Staff should observe email protocol published to minimise email traffic and timing of correspondence.

11. Content

11.1 E-mail messages should be treated like any other formal written communication. E-mail messages cannot be considered to be private, secure or temporary. E-mail can be copied and forwarded to numerous recipients quickly and easily and you should assume that they could be read by anyone.

11.2 Improper statements in e-mail can give rise to personal liability and liability for Reed's School and can constitute a serious disciplinary matter. E-mails that embarrass misrepresent or convey an unjust or unfavourable impression of Reed's School or its affairs, employees, suppliers, customers or competitors are not permitted. Do not create or send e-mail messages that are defamatory or bring the School into disrepute.

11.3 Defamatory e-mails whether internal or external can constitute a published libel and are actionable.

11.4 Think twice before sending confidential or sensitive information via e-mail. E-mail messages, however confidential or damaging, may have to be disclosed in court proceedings.

11.5 Do not create or send e-mail messages that could be intimidating, hostile or offensive on the basis of sex, race, colour, religion, national origin, sexual orientation or disability.

11.6 It is never permissible to subject another employee to public humiliation or ridicule; this is equally true via e-mail.

11.7 Copyright law applies to e-mail. Do not use e-mail to transmit or circulate copyrighted materials.

12. Archiving

12.1 The process of Archiving e-mail is the responsibility of the IT Department. Once the archive is created the user is responsible for the hard copy of the archive and the local copy of the archive. PC's need to be rebuilt from time to time and it is the user's responsibility to inform the IT Department of the presence of an archive on the hard drive. The IT Department will also keep a record of stored data on workstations as a precaution.

13. Privacy

13.1 E-mail messages to or from you cannot be considered to be private or confidential. Although it is not policy to routinely examine the content of individual's e-mail, Reed's School 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 legislative obligations, detect employee wrongdoing, protect IT system security or to comply with legal process.

13.2 Messages sent or received may be copied and disclosed by Reed's School for lawful purposes without prior notice.

13.3 It is not permissible to access or to send e-mail from another employee’s personal account either directly or indirectly.

13.4 The School reserves the right to access the e-mail and or documents from a staff account in their absence in the interest of the School e.g. to find a work related document. In such an event the authorisation of the Headmaster, Deputy Head or Bursar will be required.

14. Internet Usage

14.1 International laws regulating such diverse subjects as intellectual property, fraud, defamation, pornography, insurance, banking, financial services and tax apply equally to on-line activities.

14.2 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.

14.3 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.

14.4 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.

14.5 All Internet usage from the Reed’s School network is monitored and logged. Reporting on aggregate usage is performed on a regular basis. When specific circumstances of abuse warrant it, individual web sessions will be investigated and linked to the relevant employee’s user account. Such an investigation may result in action via the Reed’s School Disciplinary Procedure and possibly criminal investigation.

14.6 In line with Prevent guidance, the School will ensure that children are safe from terrorist and extremist material when accessing the internet in school by having secure filters which will block inappropriate content. In addition to this, any internet searches which may be of concern will be investigated further by the Designated Safeguarding Lead (DSL) using the Securus system.

14.7 Pupils and staff are aware of the procedures in school for reporting any concerns relating to inappropriate content found on the internet.

14.8 Pupils and staff are asked to sign the Acceptable Use Policy (AUP) annually to confirm that they understand what is acceptable.

14.9 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.

15. Newsgroups

15.1 Postings to newsgroups are in effect e-mails published to the world at large and are subject to the same regulations governing e-mail as above.

15.2 Always include a disclaimer with a posting if it could be interpreted as an official statement or policy of Reed's. For example:

15.3 "The views expressed are my own and do not necessarily represent the views or policy of my employer, Reed's School."

16. Instant Messaging

16.1 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. Reed's School advises against using IM within the workplace.

17. Social Networking

17.1 Staff are strongly advised not to use Social Networking sites such as Facebook, to communicate or engage with current Reed's School pupils unless there is a good pastoral reason to do so e.g. monitoring bullying type behaviour. Pupils should be contacted through the school e-mail system for school related matters only. Please refer to the Social Media policy for further information.

18. Security

18.1 All staff should be security conscious and take all practical precautions. These should include:

- Do not leave yourself 'logged on' when leaving any computer unattended
- Do not divulge your password to another colleague or to a pupil
- Change your password on an annual basis at the very least

19. Private Use

19.1 Computing facilities are provided for Reed's School for educational purposes and responsible personal use is allowed provided there is no conflict with the interests or requirements of Reed's School. Reed's School does not accept liability for any personal loss or damage incurred through using the school's computing facilities for private use. The Reed's School Staff AUP also applies to staff who use school computers and software at home.

20. Updates to this Policy

20.1 In the light of changes in the business, technology, legislation or relevant standards it may be necessary to update this policy from time to time. An up to date copy of the Staff AUP will be available on the staff drive of the intranet for staff to read. Notification to all staff will be made when updates are made.

21. Disciplinary and Related Action

21.1 Reed's School 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.

21.2 In exceptional circumstances, where there are reasonable grounds to suspect that an employee has committed a serious criminal offence, the police may be informed and a criminal prosecution may follow.

21.3 Examples of Gross Misconduct include;

- Criminal Acts – for example in relation to child pornography
- Visiting pornographic sites (adult top shelf materials) and viewing sexually explicit materials except where this forms an authorised part of the employee's job (for example 'Testing').
- 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.
- Obscene racist jokes or remarks which have been shared internally and externally – this reflects on the image of employer and brings the organisation into disrepute
- Downloading and installation of unlicensed products
- Deliberate Introduction of viruses to systems
- Chat rooms – sexual discourse, arrangements for sexual activity
- Software media counterfeiting or illegitimate distribution of copied software

21.4 Examples of Misconduct include;

- Frivolous use of the School's computing facilities that risk bringing Reed's School into disrepute.
- Entering into contracts via the Internet that misrepresents Reed's. Contracts are legally binding agreements and an employee must not enter into any agreements via the Internet to procure goods or services where Reed's School is liable for this contract, without first consulting the Bursar or the appropriate person in school.

21.5 Please note that these are not exhaustive lists. Reed's School has the right to monitor employee's use of computer equipment where there is evidence to suggest misuse (Regulation of Investigatory Powers Act 2000).

22. Reed’s School Data Storage Policy

22.1 Reed’s School has a number of servers and network shares for data. Data relevant to Reed’s School and the education of its pupils should be stored in network shares allowing the data to be backed up.

22.2 This occurs at 12.00pm every night and the backups are overwritten on a weekly basis from Monday to Thursday. On Friday’s the backups are rotated so that we have a 4 week ability to retrieve data.

23. Personal Data

23.1 Only reasonable storage of personal data up to 100MB on the network is allowed. All Reed’s School teaching staff will be monitored on a regular basis with regards to the amount of data stored on the school network. The IT Department has the authority to archive any data deemed oversize and it will be archived to a hard copy media like DVD.

24. Subject Relevant Data

24.1 Data that is required for teaching should be stored on the network in the following locations

- N:\My Documents – If the data has been created in Word, Excel or PDF and is specific to your teaching only.
- P:\Staff\Staff Subject Resources – For all shared data relevant to your department
- P:\Staff\Marketing Photographs – Please store activities and sports based images in this location under the relevant year/activity.
- Using the Firefly virtual learning environment (VLE).

Compiled By: Deputy Head (Academic)	Revision Number: 6 (Summer Term 2020)
	Next Revision Date: Summer Term 2021