
# ACCEPTABLE USE POLICY

| **RECORD MANAGEMENT**<br>Document Name POL 1.0 – RBHS – Acceptable Use Policy V201911 | | | | | |
|---|---|---|---|---|---|
| **Revision Number** | **Date Published** | **Synopsis** | **Owner** | **Role** | **Retention** |
| V201911 | November 2019 | As adopted by the Governing Body | | | 5 years from adoption |

This policy will be next reviewed during: **November 2022**

# TABLE OF CONTENTS

# 1. INTRODUCTION

Rondebosch Boys' High School (RBHS) makes use of technology learning aids, computer software, information technologies, including the internet and e-mail, and technology services (IT facilities) to conduct its business. As appropriate, RBHS extends the use of these IT facilities to its employed staff, contracted service providers, scholars and the parents of these scholars, collectively termed users. The RBHS IT facilities, with the exception of the public website, are not open for access to the general public.

# 2. PURPOSE

The purpose of this document is to communicate the details regarding the acceptable use by users of the RBHS IT facilities. When making use of the RBHS IT facilities, users are accepting the terms and conditions stated in this policy.

## OBJECTIVES

The following core objectives are supported in this policy:

2.1. Information availability

Users with the authority to access information are able to access this information whenever and wherever they need it.

2.2. Education and research

Users are able to make use of the RBHS IT facilities for education and research purposes whenever and wherever they need to.

2.3. Collaboration

Access to the RBHS IT facilities enables users to communicate easily with peers, educators, groups and organizations around the world.

2.4. Security

Access to the RBHS IT facilities is done in a secure manner.

## 3. TERMS AND DEFINITIONS

| | |
|---|---|
| IT facilities | Computer systems, technologies, including the internet and e-mail, and technology services |
| IT Stakeholders | RBHS employed staff and contracted service providers, scholars and the parents of these scholars, excluding the general public |
| Users | Any person making use of the RBHS' IT facilities |
| Data | "Facts and statistics collected together for reference or analysis" - in Latin, data is the plural of datum meaning 'something given' (Oxford Living Dictionary) |
| Information | Data which is refined by processing<br>"What is conveyed or represented by a particular arrangement or sequence of things" - from the Latin term "informare" meaning 'shape, fashion, describe', from in- 'into' + forma 'a form' (Oxford Living Dictionary)<br>The term is used to refer to both derived information and data, whether this data is used for the purpose of creating information or not.<br>This term refers to both physical and digital information, whether of a structured nature, such as that in a database or filing cabinet, or not, such as presentations and charts. |
| Information treatment | Inclusive of information and data: Production; Creation; Modification; Deletion; Security; Access; Use; Analysis; Sharing; Communication; Integration; and Transmission. |
| Malware | Also known as malicious software is any program or file that is harmful to technology or to a user. Types of malware can include computer viruses, worms, Trojan horses and spyware. |

## 4. GENERAL DIRECTIVE

### 4.1. Ownership

Every part of the RBHS IT facilities is RBHS property and the use of this property is decided by the RBHS Headmaster and where applicable, the Board.

### 4.2. Ethics and compliance

Every user must use the RBHS IT facilities responsibly, ethically and lawfully.

### 4.3. Innovation

Suggestions of improvements to the RBHS IT facilities are welcomed and all suggestions will be considered.

### 4.4. Abuse

The RBHS IT facilities are important and valuable - mistreatment or abuse of these IT facilities will mean that appropriate action will be taken.

### 4.5. Access

Users must not access or try and access RBHS IT facilities which they have no reason to access, whether they able to do so or not.

### 4.6. Confidentiality

Users must take care to protect confidentiality:

4.6.1. Users must always ensure that information is treated with the utmost care and keep confidential information confidential;

4.6.2. Users must never respond to a notice to provide any private data or information, including e-mails, without first understanding the need for the request, knowing the identity of the person or system requesting the information and knowing why the information is needed. When in doubt, users should contact the RBHS IT Service Desk;

4.6.3. Users must never use the RBHS IT facilities to obtain, use, share or distribute any information in any unlawful manner or in any manner which inappropriately discloses confidential information.

### 4.7. Representation

When using the RBHS IT facilities:

4.7.1. Users may be viewed as representing RBHS and so must use the IT facilities in a manner which reflects the RBHS values and supports the RBHS ethos and culture.

4.7.2. Users must never bind RBHS to legal obligations or liabilities, for example entering into agreements on behalf of RBHS, without first being provided with the necessary authority to do so.

### 4.8. Prohibited materials and activities

When using the RBHS IT facilities, users must take care to never store, access or interact with any prohibited materials, including the following:

4.8.1. Activities, messages, images, files, programs or statements which:

4.8.1.1. Are in breach of any South African laws, rules or regulations;

4.8.1.2. Are used to breach any South African laws, rules or regulations;

4.8.1.3. Adversely reflect upon RBHS and/or its reputation;

4.8.1.4. Adversely reflects upon any RBHS scholar, staff member, parent and/or their reputation;

4.8.1.5. Constitute pornography or sexual or racial incitement or harassment; or

4.8.1.6. Could be seen as offensive or insensitive to gender, religion or political inclination.

4.8.2. Unauthorised image or video websites or files, or live or video streaming.

4.8.3. Text or picture messages containing or with attachments containing:

4.8.3.1. Defamatory, offensive or harassing language, fraudulent material, sexually explicit images or language;

4.8.3.2. Material that infringes copyright or other intellectual property rights of third parties;

4.8.3.3. Offensive cartoons or jokes or otherwise involve lawful or wrongful conduct; or

4.8.3.4. Remarks that might be potentially embarrassing to RBHS.

4.8.4. Downloading, duplication or sharing of:

4.8.4.1. Software without prior formal authorisation;

4.8.4.2. Files using the BitTorrent protocol ("torrent");

4.8.4.3. Items presenting a breach of copyright; and

4.8.4.4. Items over the RBHS' network maximum size restrictions.

**4.9. Data Retention and destruction**

4.9.1. Users must take care to retain data records for as long as they are legally and contractually required to be retained.

4.9.2. Users must take care to only delete data records when required and authorized to do so.

**4.10. Personal use and rights**

4.10.1. The RBHS IT facilities are provided primarily to assist users in the performance of Rondebosch Boys' High School activities.

4.10.2. Certain limited personal use is permitted but no user must claim such personal use as a right.

4.10.3. Such limited personal use is permitted provided that at all times it:

4.10.3.1. Is incidental and occasional;

4.10.3.2. Is not excessive;

4.10.3.3. Does not interfere with the user's work or performance;

4.10.3.4. Does not interfere with any other user's work or performance; and

4.10.3.5. Does not interfere with RBHS operations or resources.

4.10.4. RBHS reserves the right, where necessary and by human or automated means, to access, monitor and review all materials that a user has created, stored, sent or received on the RBHS IT facilities, whether using the internet, e-mail or otherwise.

**4.11. Assurance**

4.11.1. RBHS performs audits on its IT facilities to ensure compliance with this policy and other applicable laws, rules and agreements.

4.11.2. Users are required to assist with this process and make RBHS equipment or technical infrastructure available for this purpose.

## 5. BRING YOUR OWN DEVICE

RBHS recognises the benefits that can be achieved by allowing staff, scholars and contracted service providers to use their own electronic devices when working on RBHS matters, whether that is at home, or while travelling. Such devices include laptops, smart phones and tablets, and the practice is commonly known as 'bring your own device' (BYOD). These devices are commonly known as personally owned devices (PODs).

### 5.1. Rights of use

When performing authorized RBHS activities, all scholars are under the supervision of RBHS staff and/or coaches. As such, RBHS staff members and/or coaches have the right to supervise the scholars' use of PODs. Any RBHS staff member and/or coach may intervene in a scholar's use of a POD and when doing so provide a rationale to the scholar for their action; they may:

5.1.1. Inspect a scholar's POD at any time, without interference;

5.1.2. Refuse a scholar the use of their (the scholar's) POD; and

5.1.3. Remove a scholar's POD for safe keeping in which case:

5.1.3.1. The RBHS staff member and/or coach becomes responsible for the safe keeping of the POD;

5.1.3.2. The scholar's guardian will be required to meet with the RBHS staff member and/or coach concerned to retrieve the POD and discuss the rationale for the removal; and

5.1.3.3. Repeated incidents may result in disciplinary action.

### 5.2. Access to school IT facilities and/or data

Any individual using their POD to access the RBHS IT facilities and/or data:

5.2.1. Shall ensure that all reasonable precautions are taken to secure their POD;

5.2.2. Shall appropriately manage their PODs such that no additional threats are brought to RBHS;

5.2.3. Shall not make use of "Jailbroken" PODs that is where the device's software restrictions are removed.

5.2.4. Shall not make use of rooted PODs that is where the individual has root access to the device.

### 5.3. User responsibilities

Any individual making use of BYOD must take responsibility for their PODs and how they use it. They must:

5.3.1. Familiarise themselves with their POD and make full use of its security features.

5.3.2. Maintain the POD, ensuring that the operating system and applications running on the POD are regularly patched and upgraded.

5.3.3. Take all reasonable steps to:

5.3.3.1. Prevent theft and loss of data;

5.3.3.2. Keep information confidential as appropriate;

5.3.3.3. Keep RBHS data and personal data separate; and

5.3.3.4. Maintain data integrity.

5.3.4. Take responsibility for all POD downloads.

5.3.5. Protect their PODs with screen lock passwords of sufficient length and complexity for the particular type of device.

5.3.6. Ensure that remote wipe facilities are enabled and implement a remote wipe if their POD is lost.

5.3.7. Ensure that encryption facilities are used as necessary.

5.3.8. Immediately report any security breach to the Head of IT and Innovation.

5.3.9. Report the loss of any POD containing company data, including email, to the Head of IT and Innovation as soon as possible.

5.3.10. Ensure that no RBHS data is left on their POD indefinitely.

5.3.11. Ensure that they dispose of their POD appropriately, whether selling, transferring or giving their PODs away, ensuring that RBHS data is appropriately deleted.

### 5.4. RBHS responsibilities

RBHS is committed to supporting staff, scholars and contracted service providers in this practice. RBHS will therefore:

5.4.1. Support the common types of PODs and POD manufacturers and provide separate security protocols for each but shall not allow devices outside of this support matrix.

5.4.2. Provide access by PODs to the IT facilities using a secure Virtual Private Network (VPN) service to ensure that such communications are secure.

5.4.3. Periodically re-authenticate PODs to ensure verify POD owners and users.

5.4.4. Endeavour to assist individuals wherever possible in the support of the use of their POD to access the RBHS IT facilities and data, but cannot take responsibility for technically supporting PODs.

## 6. AUDIO DEVICES

Another type of POD is an audio device. RBHS recognises that audio devices are important tools. Such devices include hearing aids for the hearing impaired, speakers for projecting audio and headsets, earbuds and earphones for personal use. Individuals remain responsible for all audio devices at all times.

### 6.1. Rights of use

RBHS staff members and/or coaches have the right to supervise the scholars' use of audio devices. Any RBHS staff member and/or coach may intervene in a scholar's use of an audio device and when doing so provide a rationale to the scholar for their action; they may:

6.1.1. Intervene, without interference, in the volume of the device;

6.1.2. Refuse a scholar the use of their (the scholar's) audio device; and

6.1.3. Remove a scholar's audio device for safe keeping in which case:

6.1.3.1. The RBHS staff member and/or coach becomes responsible for the safe keeping of the audio device;

6.1.3.2. The scholar's guardian will be required to meet with the RBHS staff member and/or coach concerned to retrieve the audio device and discuss the rationale for the removal; and

6.1.3.3. Repeated incidents may result in disciplinary action.

### 6.2. Appropriate use

With the exception of hearing aids for the hearing impaired, for safety and security reasons, the following applies to all individuals:

6.2.1. No personal audio device may be used outside of classrooms unless prior authorization has been given to do so; and

6.2.2. The use of personal audio devices is strongly discouraged when not performing RBHS activities, but still in RBHS uniform or representing RBHS in any form.

## 7. PRIVACY AND SECURITY

### 7.1. Right of privacy

7.1.1. Use of the RBHS IT facilities, including the ability to choose usernames and passwords to gain access to the RBHS IT facilities, does not imply that users must have an expectation of privacy or confidentiality when using the RBHS IT facilities.

7.1.2. Users expressly waive any right of privacy in anything they create, store, send or receive on the RBHS IT facilities.

7.1.3. Users further consent to allowing duly authorised RBHS representatives, to access and review all materials that the user has created, stored, sent or received on the RBHS IT facilities.

### 7.2. Maintaining privacy

7.2.1. No users may pry into the personal affairs of other users without being formally authorised by the RBHS Headmaster to do so.

7.2.2. Users who are able to unduly access the private information of other users are to inform the RBHS Head of IT and Innovation as soon as possible who will ensure that a formal record of such an alert is available.

7.2.3. In addition to the consequences outlined in this policy, users found accessing the private information of other users may face claims for damages for wrongful infringement of privacy rights and/or criminal prosecution.

### 7.3. Right of security

7.3.1. Users have the legitimate right to safety and security when using the RBHS IT facilities.

7.3.2. RBHS endeavours to provide suitable and appropriate safety and security measures for users making use of the RBHS IT facilities.

7.3.3. It is also the responsibility of the user of the RBHS IT facilities to ensure that they take suitable and appropriate measures to support RBHS in this endeavour.

### 7.4. Physical security

7.4.1. It is the responsibility of every user to ensure that the devices and associated peripheral equipment (equipment) assigned by RBHS to them for their use are adequately protected against unauthorised use, theft or damage.

7.4.2. Users must ensure that when travelling with this equipment that it is securely transported, such as in a locked car boot and not in the passenger compartment of a vehicle or as hand luggage on an aeroplane and not in checked baggage.

7.4.3. Users must ensure that the equipment is adequately secured when the equipment is not in an RBHS classroom or office, such as kept in a safe at a hotel or similar location or suitably secured at the user's residence.

7.4.4. Users must ensure that the equipment is adequately secured at RBHS before going home and when unattended for any lengthy period of time.

### 7.5. Information security

7.5.1. Users are responsible for ensuring the continued security, integrity and confidentiality of all information to which they have access.

7.5.2. Users must take reasonable steps, in addition to the rules relating to passwords, to ensure that no confidential information resident in their personal computer is visible during their absence or accessible by unauthorised persons, where such reasonable steps include:

7.5.2.1. Logging out of and switching off devices when not in use;

7.5.2.2. Ensuring that the RBHS authorised security measures are always enabled, updated and current (as example, encryption software);

7.5.2.3. Securely saving files and data using for example password protection; and

7.5.2.4. To the extent possible, not storing confidential information on removable or mobile equipment and rather storing information, as example on the RBHS shared IT facilities (e.g. file server).

7.5.3. Users must not store, save, move or copy information, of any type or classification, on or to any form of cloud-based or internet-based storage medium or service, including e-mail services, without formal authorisation to do so.

7.5.4. In the event that a user is authorised to store, save, move or copy information on or to a form of cloud-based or internet-based storage medium or service, including e-mail services, the information must be encrypted both in transit and at rest.

7.5.5. Users must not remove any information stored on a removable storage device (as example, memory stick) from RBHS premises without formal authorisation to do so.

7.5.6. In the event that a user is authorised to remove information stored on a removable storage device from the RBHS premises, the user must ensure that:

7.5.6.1. All information is stored in an RBHS approved encrypted format;

7.5.6.2. The storage media remains in the user's personal possession at all times;

7.5.6.3. The same care is exercised over this media as that required for all such equipment in terms of this policy;

7.5.6.4. Transfer of possession, or provision of access, to the media is never be provided to an unauthorised party; and

7.5.6.5. In the event that possession of the storage media is transferred or access provided to another authorised party, the user obtains written acknowledgment of having released the information to this party.

**7.6. Encryption**

7.6.1. The use of any form of cryptography, other than that which has been approved by RBHS, is prohibited.

7.6.2. When RBHS-approved cryptography is applied, users must place all private keys or other decryption keys in escrow with the RBHS Head of IT and Innovation.

**7.7. Anti-malware**

Malware (as example worms, Trojans, spyware and viruses) can cause substantial harm to the RBHS IT facilities. Where users are assigned responsibility for particular components of the RBHS IT facilities (as example laptops, mobile devices or servers):

7.7.1. They are to ensure that the most recently available, RBHS approved anti-malware protection software has been installed and that this software is operational at all times.

7.7.2. They must never install anti-malware software on the RBHS facilities which is not authorised.

7.7.3. They are to ensure that scheduled anti-malware scans start and complete at least once a week and are to report any actual or suspected deviation from this schedule to the Head of IT and Innovation.

7.7.4. They must not disable anti-malware software on their equipment without prior authorisation to do so.

7.7.5. Prior to connecting any storage media to equipment or opening information files, they are to ensure that a comprehensive scan of the storage media and files is performed.

7.7.6. In the event malware is detected, they are to immediately notify the Head of IT and Innovation.

## 8. INTERNET, EMAIL AND TELEPHONY

### 8.1. Internet access

The following applies to all access to the public internet:

8.1.1. RBHS reserves the right to restrict access to certain websites, or areas of the internet, whether or not such websites or internet areas contain prohibited material.

8.1.2. Users must not use internet anonymizers to hide their identities under any circumstance.

8.1.3. Users must not harass or disrupt any other person whilst connected to the internet.

8.1.4. Users must not transact using the internet or submit credit card numbers online, unless provided with the necessary prior formal authorisation to do so.

8.1.5. Users must not share, post, publish or transmit information without the necessary prior formal authorisation to do so, in which case suitable security measures will be applied.

8.1.6. Users must not share, post, publish or transmit information which could assist unauthorised access to the RBHS IT facilities (as example, usernames, server names, access ports and passwords).

8.1.7. Users must not download information via file transfer protocol (FTP) unless authorised to do so, in which case suitable security measures will be applied.

8.1.8. Users must not host or display personal web pages using the RBHS IT facilities or internet access.

8.1.9. Users must not user the RBHS IT facilities or internet access to subscribe to, or participate in, chat groups, bulletin boards, newsgroups, or discussion groups that are not related to RBHS activities.

8.1.10. Users must not browse, download or post files, of any type, or stream data which are excluded in terms of this policy.

**8.2. E-mail access**

8.2.1. Every RBHS staff member and scholar receives a **Rondebosch.com** e-mail address.

8.2.2. Users do not have the right to withhold RBHS related e-mail messages that should legitimately be made available to Rondebosch.com e-mail address holders.

8.2.3. Users should confirm that all recipients required notification of the message and content prior to using the “Reply all” function.

8.2.4. RBHS reserves the right to archive e-mails stored on the RBHS e-mail facilities after a set period of time, which must be no less than 90 days, following which users will need to formally request retrieval of such e-mails which will be done at RBHS’ discretion.

8.2.5. RBHS reserves the right, at its discretion and where required, to access and disclose all messages sent using RBHS e-mail facilities, with or without informing the user.

8.2.6. Requests made to RBHS for access to the contents of e-mail without the consent or knowledge of the sender or recipients may be approved only by the Head of IT and Innovation.

8.2.7. RBHS reserves the right to not transmit e-mail messages where such messages may threaten the security of RBHS, its staff or scholars, or include prohibited material.

**8.3. E-mail transmissions**

8.3.1. Confidential material must not be sent, transmitted or distributed by Rondebosch.com e-mail address holders to non Rondebosch.com email addresses.

8.3.2. In the event that it is necessary to communicate confidential material, prior approval from the Head of IT and Innovation is required.

8.3.3. All communications, including e-mail communications, between RBHS and its legal representatives must be privileged and as such they:

8.3.3.1. Must be suitably and prominently identified as such communication;

8.3.3.2. Must not be disclosed without the prior authorisation of the RBHS Headmaster; and

8.3.3.3. Must not be divulged to those who are not party to the e-mail communication in question.

8.3.4. Correspondence, and associated attachments, sent using the RBHS e-mail facilities are considered company records and as such:

8.3.4.1. Correspondence of a formal nature is to be sent using an RBHS letterhead;

8.3.4.2. Users are responsible for determining whether the intended recipient received their e-mail together with the required attachments; and

8.3.4.3. Users are alerted to the fact that the transmission of documents can bind RBHS to an agreement.

8.3.5. Users must not disguise their identity while using the RBHS e-mail facilities.

8.3.6. Users must not alter the “From” line (i.e. the Sender) or any other indication of the origin of any Rondebosch.com e-mail.

8.3.7. When forwarding or replying to e-mails, users must not alter any portion of the original e-mails, even though they may have the ability to do so.

8.3.8. Users must not present personal views as that of RBHS.

**8.4. E-mail disclaimer**

Users must ensure that Rondebosch.com e-mails contain the most recent RBHS e-mail disclaimer.

**8.5. E-mail restrictions**

The RBHS e-mail facilities must not be used:

8.5.1. To send or receive any e-mail message the size of which in total, including any files or attachments thereto, exceeds 10 megabytes without prior formal approval, in which case a suitable alternative mechanism will be applied;

8.5.2. For the personal dissemination or storage of personal advertisements, solicitations, promotions, destructive programs, political material, or any prohibited material;

8.5.3. To send any e-mail which requests the recipient to forward such message to multiple other recipients (as example, chain-messages) unless required by RBHS;

8.5.4. To send unsolicited messages of a commercial nature to persons with whom the sender does not have a prior relationship;

8.5.5. To send frequent and / or numerous e-mail messages with the intention of disrupting or inconveniencing the receiver; nor

8.5.6. To send or receive any attachment prohibited in terms of this policy.

The RBHS e-mail facilities must not be used to forward e-mails:

8.5.7. Which requests the recipient to forward the message to multiple other recipients (as example, chain-messages) unless required by RBHS;

8.5.8. Of an unsolicited, commercial nature to persons with whom the sender does not have a prior relationship;

8.5.9. Which are likely to lead to the embarrassment of the original sender, without a prior RBHS approval; nor

8.5.10. Where there exists in the message a clearly expressed restriction to do so.

**8.6. Telephony usage**

RBHS staff members or contracted service providers may be provided access to telephony services such as a handset or mobile device. In such instances:

8.6.1. Users are expected to act responsibly and keep costs to a minimum.

8.6.2. Wherever possible premium directory enquiry services should be avoided.

8.6.3. Users must not make use of premium rate phone numbers (as example, competition lines).

8.6.4. When making or receiving calls, users should aim to be pleasant, informative, helpful and brief.

8.6.5. Users are to ensure that calls to mobile phones are clear, succinct and as brief as possible.

8.6.6. Users must not provide an RBHS telephone number as a contact point for personal business purposes.

8.6.7. Users are responsible for any fine or other penalty incurred for breach of legislation if using an RBHS mobile telephone whilst driving.

8.6.8. International Roaming is not permitted on RBHS mobile telephones without prior authorisation by the RBHS Headmaster.

8.6.9. Mobile phones must be kept secure at all times, and out-of-sight whenever possible.

8.6.10. All RBHS and personal smartphones setup with Rondebosch.com e-mail accounts and/or internet based access to RBHS data must be protected with the authorised security measures.

8.6.11. Users must never provide information using telephonic facilities unless it is absolutely clear who it is being given to and that they are entitled to the information and are ready and able to accept it.

8.6.12. Users must take care to ensure that conversations involving confidential and/ or personal information cannot be overheard.

8.6.13. Users should only leave voicemail messages containing personal information after due consideration has been given to any security and confidentiality risks involved.

## 9. SOFTWARE, HARDWARE AND NETWORK

### 9.1. Software

RBHS has licensed, or developed, certain software. These proprietary interests are to be protected and the terms of applicable licences are to be complied with. Without prior authorization, users may not:

9.1.1. Copy software from or to the RBHS IT facilities;

9.1.2. Distribute software to any third party;

9.1.3. Install or implement any software without prior approval;

9.1.4. Make use of software on the RBHS IT facilities (as example, without having been provided with an assigned username for the software concerned);

9.1.5. Make use of cloud-based or internet-based software using the RBHS IT facilities (as example, access to internet-based personal banking facilities being authorised by the RBHS firewall);

9.1.6. Modify, revise or adapt software;

9.1.7. Translate, reverse engineer or disassemble any software residing on the RBHS IT facilities;

9.1.8. Create software on the RBHS IT facilities.

**9.2. Hardware**

RBHS appoints and authorises staff and service providers to conduct maintenance and support of the IT facilities and associated equipment.

9.2.1. Unless appointed and authorised to do so, users must not attempt to maintain, repair or upgrade any equipment or any part or component of equipment assigned to them.

9.2.2. Unless appointed and authorised to do so, users must not attempt to maintain, repair or upgrade any RBHS IT facility or any part or component thereof.

9.2.3. Users must not allow any person or persons other than those appointed and authorised to maintain, repair or upgrade any equipment or any part or component of equipment assigned to them.

**9.3. Network**

RBHS strives to provide optimal fixed line and wireless coverage within resource constraints and priorities.

9.3.1. In a wireless environment, network reliability is a function both of the level of user congestion (traffic loads) and service availability (interference and coverage). RBHS strives towards a cost-effective balance between expected use, peak times and technical issues. Adjustments in coverage and capacity may occur from time to time.

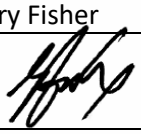
9.3.2. RBHS cannot be held legally responsible for network connection failures or denials of service.

9.3.3. Unauthorised wireless devices are prohibited from connecting to the wireless network.

## 10. ADOPTION

**The Board hereby adopts this policy.** For and on behalf of the RBHS Board of Governors:

Name: Mr Gary Fisher Role: Chairman

Signature:  Date: 19 November 2020