Ringwood School

Policy Name	Staff Acceptable Use Policy
Date of Current Policy	June 2024
Author	Operations Manager
Created on	June 2024
Authorised By	Full Governing Body
Review Frequency	3Years
Review Date	June 2027
Rationale for Policy	Statutory

Minor amendments since issue:

8 Jan 25: updated wording on WhatsApp use in section 2 iii), following feedback from Dave Robinson on need to use it for coordination and recognizing that Governors also use it for that purpose

This Staff Acceptable Use Policy covers the use of ICT resources including the use of IT systems, telephones, email, remote access and use of the internet and the use of personal devices for School related business.

Staff are advised of this policy during their induction and of the School's requirement for them to adhere to the conditions therein and required to sign the Acceptance Use Agreement at the end of this document.

Ignorance of this policy and the responsibilities it places on members of staff is not an excuse in any situation where it is assessed that you have breached the policy and its requirements.

This policy consists of three sections:

1. Acceptable use of ICT equipment and data
2. Use of telephones, email and internet by staff (including personal devices)
3. Safe use of social networking

This policy is linked to: Staff Code of Conduct, IT Policy, Data Protection Policy

1. Acceptable Use of ICT Equipment and Data Security Principles

Ringwood School is committed to safeguarding its ICT resources to ensure they can be used in the most effective manner to support teaching and learning processes. Ensuring the safety and integrity of the School's ICT systems is the responsibility of all staff.

In using ICT equipment and service there are responsibilities for School staff which are outlined below. If you misuse School computing facilities in a way that constitutes a breach or disregard of this policy, consequences associated with that breach may follow and you may be in breach of other School regulations.

For the purposes of this policy the term "ICT resources" refers to any ICT resource made available to you, any of the services provided through the network, applications or software products that you are provided access to and the network infrastructure that you use to access any of the services (including access to the Internet). Staff who connect their own device to the School's network and the services available are particularly reminded that such use also requires compliance with this policy.

i) Objectives:

The main objective of the policy in this particular regard is to protect the School's:

- IT network and equipment
- Data from theft and/or wrongful disclosure of private, sensitive or confidential information
- reputation, and its employees from activities that might expose them to legal action from other parties

ii) **Password security**

Access to all systems and services is controlled by a central username and password. Staff are allocated their username and initial password as part of their induction with the School. **Usernames and passwords are never to be shared or revealed to any other party**. Those who use another person's user credentials and those who share such credentials with others will be in breach of this policy.

Passwords must conform to the specific complexity requirements as set out by the IT Team, and each member of staff is responsible for taking reasonable measures to safeguard their password and change it from time to time. If a user believes or suspects that their account has been compromised they should report this immediately to the IT Team.

If any School resource, including email, is accessed from a personal device then **this device must be protected by appropriate security to ensure that it cannot reasonably be used by another person**. Such measures should include PIN, password, thumbprint or facial recognition security. In most cases the School has also implemented Two Factor Authentication via the Microsoft Office 365 system to access systems from outside of the School premises or from equipment not owned by the School.

iii) **General Conditions of Acceptable and Non-Acceptable Use**

In general, use of School ICT resources should be for your teaching, research, study or the administrative purposes of the School. Modest use of the facilities and services for personal use is accepted so long as such activity does not contravene the conditions of this policy.

- **Your use of the School's ICT resources must**:
  - at all times comply with the law
  - must not interfere with any others' use of these facilities and services

- **You must not**:
  - use or copy any data or program belonging to other users without their express and specific permission
  - copy or share any documents or material from the ICT resources (such as from Sharepoint) for use by that person or any other party for business not relating to the School
  - use School computing services to harass, defame, libel, slander, intimidate, impersonate or otherwise abuse another person or for any hacking purpose
  - use School computing services for the creation, collection, storage, downloading or displaying of any offensive, obscene, indecent or menacing images, data or material capable of being resolved into such. (There may be certain legitimate exceptions for educational purposes which would require the fullest disclosure and specific authorisation from the Headteacher)
  - use the School's computing services to conduct any form of commercial activity without express permission from the Headteacher
  - use the School's computing services to disseminate mass (unsolicited) mailings
  - install or distribute any software which is not first authorised by the IT Team
  - use unlicensed software or use software in a manner that contravenes the license agreement
  - play computer games of any nature whether preinstalled with the operating

system or available online

- use social media sites, online gambling sites or sites pertaining to e-commerce through the internet using School equipment at any time other than for the performance of your School role

iv) **Data Security**

The School holds a variety of sensitive data including personal information about students and staff, most significantly in the School's MIS (Arbor), Sharepoint / One Drive or Safeguarding system. If you have been given access to this information, you are reminded of your responsibilities under Data Protection law, **including taking utmost care to maintain confidentiality and:**

- **Not to distribute disclose any information obtained from the systems to any other person (s) outside of the School**
- Best practice is not to access systems in any environment where the security of the information contained may be placed at risk

You must not make digital copies of, or share, data containing personal information outside the School's systems. This includes saving sensitive data onto personal laptops or home computers, memory sticks, cds/dvds, attaching to non-School emails or sharing files via 365 OneDrive / Teams that could be accessed outside of the School systems. If you do need to have data outside the School systems, this should only be with the authorisation of the Operations Manager and by using a method approved by the IT Team.

Personal data relating to students, staff, parents, suppliers, applicants, visitors or other real living persons must not be stored on any electronic device not owned and managed by the School. Names and any photo or video media involving students on a personal device is also not allowed.

For any systems not accessed through the network's single sign-on process, the principles noted above regarding strong password setting, regular changing and not sharing with others must be routinely applied.

There are a variety of methods of remote access to the School's ICT systems, such as Remote Desktop, which allow you to work on data in-situ rather than taking it outside the School. These should always be used in preference to taking and holding data off-site.

The IT Team offers a variety of information and support to help you keep data secure. If you are uncertain about any aspect of data security, you must contact the IT Team for advice.

v) **Cyber Security**

As part of the staff induction process and at least annually thereafter, the School will provide training on the threats to our data and other risks relating to cyber security. All staff must ensure to undertake such training whenever provided at the earliest opportunity and to follow the guidance that is provided within that, in particular to:

- checking email sender address and attachments before opening
- how to respond to a request for bank details, personal information or login details
- how to verify requests for payments or changes to information
- good password "hygiene" securely, as referenced above

Should staff not understand the training or recommendations thoroughly, or have any questions or concerns, they must seek clarification directly from the IT Team in first instance.

If staff have any suspicions about the integrity of any email received or other requests for information obtained through text or phone call, or that the School systems might have been compromised, they should immediately notify the IT Team.

vi) **Physical Security**

The users of ICT resources should always adhere to the following guidelines:

• Treat equipment safely, in the same manner as a reasonable person would

• Keep liquids away from ICT equipment

• Do not drop ICT equipment or objects onto it

• Any portable devices must be securely locked away when not in use.

• Personal devices (such as smartphones) should be secured when not in use as they remain your responsibility at all times.

• Do not leave any computer equipment belonging to the School, on view inside your car. It should be locked away in your car's boot out of sight.

• USB sticks are not permitted to be used on the School network for the withdrawal of confidential School data

• Staff supervising students using ICT equipment should ensure students take reasonable care of such equipment

vii) **Remote Access**

Remote access to the School network is possible where this has been granted by the IT Team.

Remote connections are considered direct connections to the School network. As such, generally accessing services remotely, subjects the user to the same conditions, requirements and responsibilities of this policy. All connection attempts are logged.

viii) **Breaches of This Policy**

If there is a breach of the policy, an investigation will be carried out, in confidence, by School Leadership under the direction of the Headteacher.

Incidents which are determined to be in contravention of this policy will be assessed for their severity. Investigating such incidents may require the collection and evaluation of user related activity and evidence.

It is not possible to provide an exhaustive list of potential ways in which a user may contravene this policy but in general such breaches will result in possible sanctions, consequences and/or penalties depending on the severity.

In the event a portable device is damaged or lost as a result of non-compliance with this policy or as a result of other negligent action, then staff may be required to make a full or partial contribution towards any replacement costs, at the discretion of the School.

ix) **Cessation of Employment**

At the cessation of employment, **you must ensure that all School owned hardware is returned, any School owned software is removed from personal devices and all data relating to students, staff, visitors, parents and other School specific matters is removed from any devices. This specifically includes deleting all School email from**

devices.

All printed documents relating to students, staff, visitors, parents, etc must also be returned to the School or securely destroyed.

These points apply equally to persons considered as staff members, such as trainee teachers, who may not be technically employed by the School, but have access to the School ICT resources as part of their role.

2. Use of Telephones, Email and Internet by Staff (including personal devices)

i) Principles

The provisions of this Policy apply to all members of staff, whether or not they have access to, or sole use of, a telephone or email/the Internet on a computer. Although access to such facilities does not form part of the benefits provided to staff, it is recognised that there are occasions when employees might legitimately make private use of these facilities. This Policy is intended to make clear what constitutes legitimate use. It is intended not to place employees under unjustifiable scrutiny, but to give them a high measure of security and confidence about their use of email, telephones and the Internet. In general, the use of personal devices to access School related systems, should be kept to a minimum.

ii) Objectives

The main objectives of this policy in this regard are to:
- provide guidance on inappropriate use of School telephones, email and internet facilities
- clarify when the School may monitor staff usage of these facilities.

iii) Use of telephones

There will be occasions when employees need to make short, personal telephone calls on School telephones to deal with occasional and urgent personal matters. Where possible, such calls should be made and received outside the employee's normal working hours or when they do not interfere with work requirements.

The use of School telephones for private purposes, which are unreasonably excessive or for School purposes which are defamatory, obscene or otherwise inappropriate, may be treated as gross misconduct under the appropriate disciplinary procedure.

Where the School has grounds to suspect possible misuse of its telephones, it reserves the right to audit the destination and length of out-going calls and the source and length of in-coming calls. This would not normally involve the surveillance of calls but in certain rare circumstances where there are reasonable grounds to suspect serious misconduct, the School reserves the right to record calls.

Personal mobile phones can be used to access some School systems hosted by cloud- based platforms. As noted earlier, where such access is required, staff should ensure that the device has security measures in place to restrict access (for example PIN code, biometric or facial recognition). The School has also in most cases implemented Two Factor Authentication to access such systems.

Staff should not, under any circumstances, use their personal device to create or save any video or photographic material of students or their personal data. In addition:

- WhatsApp should only be used on personal devices as a coordination / communication tool between staff and/or govenrors. School related information which includes personal or sensitive data must not be shared via WhatsApp.
- Technical support is not provided by the School on the user's own devices, but guidance may be provided if the IT Team have opportunity to do so
- The School does not accept responsibility for any loss or damage to the user's device when used on the School's premises or network services
- In the event of any loss or theft of your device, this should be immediately reported to the IT Team should it contain any School information or links to the School network or email system
- The School will not monitor the content of the user's own device but will routinely monitor any traffic over the School to identify and prevent inappropriate activity or potential security threats.

iv) **Use of email**

The School provides an email account for staff to use for School-related business only and not for personal use. Email should be treated like any other form of written communication and, as such, what is normally regarded as unacceptable in a letter or memorandum is equally unacceptable in email communication.

Employees should be careful that before they open any attachment to a personal email they receive, they are reasonably confident that the content is from a bona fide person relating to School business and does not pose a cyber security risk nor contain obscene or defamatory to avoid contravening the law. Equally, if an employee receives an obscene or defamatory e- mail, whether unwittingly or otherwise and from whatever source, s/he should not intentionally forward the email to any other address, unless specifically requested to do so by an investigator appointed by the School. Any other use of email for either personal or School purposes to send or forward messages or attachments which are in any way defamatory, obscene or otherwise inappropriate will be treated as gross misconduct under the appropriate disciplinary procedure.

Where the School has reasonable grounds to suspect misuse of email in either scale of use, content or nature of messages, it reserves the right to audit the destination, source and content of email to and from a particular address.

The School also reserves the right to access an employee's email account in her/his unexpected or prolonged absence (e.g. due to sickness) to allow it to continue to undertake the employee's normal role. In normal circumstances the employee concerned will be contacted before this is done, to provide him/her with prior knowledge.

v) **Use of the Internet**

The primary reason for the provision of Internet access is for the easy retrieval of information for educational purposes, or to make use of learning resources, or to make legitimate authorised purchases to enhance the ability of its staff to undertake their School role.
However, it is legitimate for employees to make use of the Internet in its various forms in the same way as email above provided it is not used to view or distribute improper material such as text, messages or images which are derogatory, defamatory or obscene.

Unauthorised use of the Internet, which is unreasonably excessive for personal use or for purposes which are defamatory, obscene or otherwise inappropriate will be treated as gross misconduct under the staff Code of Conduct. The School reserves the right to audit the use of the Internet from particular accounts where it suspects misuse.

vi) **Monitoring the use of telephone, email and the Internet.**

It is not the School's policy, as a matter of routine, to monitor an employee's use of the School's telephone or email service or of the Internet via the School's networks (other than from school wide filtering and safeguarding alerts). However, as has been stated, where there are reasonable grounds to suspect an instance of misuse or abuse of any of these services, the Headteacher or Governing Body may grant permission for the auditing of an employee's telephone calls email or their internet usage.

Once approved, the monitoring process will be undertaken by designated staff acting, for operational purposes, under the direction of the Headteacher. Strictest confidentiality will be observed when undertaking these activities and monitoring will only be to the extent necessary to establish the facts of the case. Findings will be reported directly to the Headteacher/Governing Body or their delegated representative to support reaching a conclusion and determining any follow-up action. When monitoring is approved, the case for continued monitoring shall be reviewed on a regular basis with a view to terminating monitoring in as short a period of time as possible.

3. Safe Use Social Networking

The key requirements for staff are as follows:

- Staff members have a responsibility to protect the reputation of the School, staff and students at all times and must treat colleagues, students and associates of the School with professionalism and respect whilst using social networking sites.
- Social networking sites should be used responsibly, and users should ensure that neither their personal or professional reputation and/or the School's reputation, nor the reputation of individuals within the School are compromised by inappropriate postings.
- Use of social networking sites for School business is not permitted, unless via an officially recognised School site and with the permission of the Operations Manager.
- Members of staff will notify the Operations Manager if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the School.
- No School information, communication, documents, videos and / or images should be posted on any personal social networking sites.
- No details or opinions relating to any student are to be published on any website.
- Users must not knowingly cause annoyance, inconvenience or needless anxiety to others (cyber bullying) via social networking sites.
- No opinions about another member of staff, which could cause offence, to be posted.
- No photos or videos, which show students of the School who are not directly related to the person posting them, should be uploaded to any site other than the School's Website.
- No comment, images or other material may be posted anywhere, by any method that may bring the School or, the profession into disrepute.
- Users must not give students access to their area on a social networking site, (for example adding a student as a friend on Facebook). If, in exceptional circumstances, users wish to do so, please seek advice from the Designated Safeguarding Lead.

We recommend staff keep accounts / profiles private to avoid public access (including students).

ACCEPTABLE USE AGREEMENT

To be completed by all staff

As a School user of the network resources/equipment I hereby confirm that I have read and understood the Staff Acceptable Use Policy and that I agree to follow the School rules (set out within this policy) on its use. I will use the network/equipment in a responsible way, observe all the restrictions explained in it and follow all guidance provided by the School on cyber security. If I am in any doubt, I will consult the Operations Manager.

In addition, I agree to report to the Operations Manager:

- any misuse of the network
- any websites that are available on the School internet that contain inappropriate material
- any lapses in physical security

Furthermore, when using School devices I accept that:

- I must not use these devices for inappropriate purposes
- I must only access those services for which permission has been granted
- I will not download, use or upload any material which is unsuitable within a School setting or that may cause disruption to the School network
- I will ensure any portable equipment, such as laptops, cameras or iPads assigned to me will be kept securely

If I do not comply with the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that staff under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.

I understand that the School will monitor communications in order to uphold this policy and to maintain the School's network (as set out within this policy).

I agree to adhere to this staff acceptable use policy – please log your acknowledgement here: https://forms.office.com/e/HhL2JegycP