Ringwood School

Policy Name	Staff Acceptable Use Policy
Date of Current Policy	December 2021
Author	Operations Manager
Created on	September 2018
Authorised By	Full Governing Body
Review Frequency	3 Years
Review Date	December 2024
Rationale for Policy	Statutory

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.

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 online resources

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

1. Acceptable use of ICT equipment and data 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.

The school encourages staff to fully use the ICT resources and to make use of portable ICT equipment offsite to support them in their work. The school encourages this use in a responsible and professional manner. Portable computers include for example laptops, tablets, smartphones and other portable ICT devices.

As a member of school staff, you have a right to use its computing services; that right places responsibilities on you as a user which are outlined below. If you misuse school computing facilities in a way that constitutes a breach or disregard of this policy, consequences associate with that breach may follow and you may be in breach of other school regulations.

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

Staff are advised of this policy during their induction and of the school's requirement for them to adhere to the conditions therein.

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 requires compliance to this policy.

Purposes

- To protect the school's networks and equipment
- To protect the school's data
- To protect the school and its employees from activities that might expose them to legal action from other parties

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 and each member of staff is responsible for taking reasonable measures to safeguard their password. If a user believes or suspects that their account has been compromised they should report this immediately to the Network Manager.

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 may include PIN, password, thumbprint or facial recognition security. In many cases the school has implemented Two Factor Authentication via the Microsoft Office 365 system.

General Conditions

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.
- Your use of the school's ICT resources 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.
- You must not use school computing services to harass, defame, libel, slander, intimidate, impersonate or otherwise abuse another person.
- You must not 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).
- You must not use the school's computing services to conduct any form of commercial activity without express permission from the Headteacher.
- You must not use the school's computing services to disseminate mass (unsolicited) mailings.
- You must not install or distribute any software which is not first authorised by the Network Manager.
- You must not use unlicensed software or use software in a manner that contravenes the license agreement.
- You must not play computer games of any nature whether preinstalled with the operating system or available online.
- You must not use social media sites, online gambling sites or sites pertaining to e-commerce through the internet using school equipment at any time.

Data Security

The school holds a variety of sensitive data including personal information about students and staff. If you have been given access to this information, you are reminded of your responsibilities under Data Protection law.

You must not make digital copies of data outside the school's systems. This includes putting sensitive data onto laptops, memory sticks, cds/dvds or into emails that could be accessed through a range of devices. If you do need to take data outside the school, this should only be with the authorisation of the Operations Manager and by using an encrypted USB or password protected file as approved by the Network Manager.

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 not allowed.

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 data off-site.

The ICT Department 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 Network Manager for advice.

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

Remote Access

Remote access to the school network is possible where this has been granted by the ICT Department.

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.

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 be categorised into one of three levels of severity and each level of breach will carry with it a possible range of sanctions, consequences and/or penalties.

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 you may be required to make a full or partial contribution towards any replacement costs, at the discretion of the school.

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, etc is removed from any devices. This specifically includes deleting all school email from devices.

All 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)

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 e-mail/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 e-mail, telephones and the Internet. In general, the use of personal devices to access school related systems, should be kept to a minimum.

Purposes

To provide guidance on inappropriate use of school telephones, email and internet facilities. To clarify when the school may monitor staff usage of these facilities.

Use of telephones

There will be occasions when employees need to make short, personal telephone calls on school telephones in order 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. 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 implemented, where possible, 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.

Use of email

The school provides an email account for staff to use and this should be for school related business only and not for personal use. E-mail 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 an e-mail communication.

Employees should be careful that before they open any attachment to a personal e-mail they receive, they are reasonably confident that the content is in no sense 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 e-mail to any other address, unless specifically requested to do so by an investigator appointed by the school. Any other use of e-mail 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 e-mail in either scale of use, content or nature of messages, it reserves the right to audit the destination, source and content of e-mail to and from a particular address.

The school also reserves the right to access an employee's e-mail account in her/his unexpected or prolonged absence (e.g. due to sickness) in order 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, in order to provide him/her with prior knowledge.

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 as long as 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 appropriate Code of Conduct. The school reserves the right to audit the use of the Internet from particular accounts where it suspects misuse of the facility.

Monitoring the use of telephone, e-mail 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 e-mail service or of the Internet via the school's networks. 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 e-mail or the Internet. Once approved, the monitoring process will be undertaken by designated staff acting, for operational purposes, under the direction of the Principal. These staff are required to observe the strictest confidentiality when undertaking these activities and they will monitor only to the extent necessary to establish the facts of the case. They will make their reports directly to the Headteacher/Governing Body or their delegated representative to enable Human Resources to advise the appropriate line manager the actions that may need to be taken in any particular case. 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 of online resources

Principles

This applies wherever access to Ringwood School Management Information Systems (MIS) is provided (SIMS). This applies to all online resources provided by Ringwood School, for example Capita SIMS and the Learning Zone. This policy applies whenever information is accessed through The Ringwood School MIS, whether the computer equipment used is owned by School or not. The policy applies to all those who make use of the SIMS MIS resources.

Purposes

Security

This Policy is intended to minimise security risks. These risks might affect the integrity of school's data, the Authorised MIS User and the individuals to which the MIS data pertains. In particular these risks arise from: The intentional or unintentional disclosure of login credentials

- The wrongful disclosure of private, sensitive, and confidential information

- Exposure of the school to vicarious liability for information wrongfully disclosed by authorised users.

Data Access

• This Policy aims to ensure all relevant aspects of the Data Protection Act (1998) and Fair Processing Policy are adhered to.

• This Policy aims to promote best use of the MIS system to further the communication and freedom of information between Ringwood School and Parents/Carers.

Guidelines

The School's online systems are provided for use only by persons who are legally responsible for students currently attending the school.

Access is granted only on condition that the individual formally agrees to the terms of this Policy.

Personal Use

Information made available through the MIS system is confidential and protected by law under the Data Protection Act 1998. To that aim:

• Users must not distribute or disclose any information obtained from the MIS to any person(s) with the exception of the student to which the information relates or to other adults with parental/carer responsibility.

• Best practice is not to access the system in any environment where the security of the information contained may be placed at risk.

Password Policy

Staff must assume personal responsibility for usernames and passwords. Never use anyone else's username or password.

You must always keep your individual user name and password confidential. These usernames and passwords should ***never*** be disclosed to anyone. Passwords and user names should never be shared.

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 regarding another member of staff, which could cause offence, are 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.

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 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 and observe all the restrictions explained in the School Acceptable Use Policy. If I am in any doubt, I will consult the [POSITION].

I agree to report any misuse of the network to the [POSITION]. Moreover, I agree to report any websites that are available on the School internet that contain inappropriate material to the [POSITION]. I finally agree to ensure that portable equipment such as cameras, iPads or laptops will be kept secured when not in use and to report any lapses in physical security to the [POSITION].

Specifically when using school devices: -

- 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.

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).

Signed ……. Date ……..

Print name ……