Acceptable User Policy and Agreement (Students)

Dated: February 2019
Approved by Governing Body: February 2019
For Review: February 2020
ACCEPTABLE USE POLICY AND AGREEMENT

Introduction

This policy is designed to enable acceptable use for students, staff and governors.

The School provides a range of ICT resources which are available to students, staff members and governors. In order to ensure the safety of both staff, governors and pupils, it is important that students, all staff members and governors follow the guidelines detailed below.

This policy aims to:

- Promote the professional, ethical, lawful and productive use of the School’s ICT systems and infrastructure.
- Define and identify unacceptable use of the school’s ICT systems and external systems.
- Educate users about their data security responsibilities.
- Describe why monitoring of the ICT systems may take place.
- Define and identify unacceptable use of social networking sites and school devices.
- Specify the consequences of non-compliance.

This policy applies to all users of the School’s ICT systems, who are expected to read and understand this policy. To confirm acceptance of the policy, users will sign an Acceptable Use Agreement which is attached to this policy. Breach of this policy may result in disciplinary action.

The use by all users and the monitoring by the School of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the Data Protection Act 2018, together with the Employment Practices Data Protection Code issued by the Information Commissioner. Users are referred to the School's Data Protection Policy for further information.

If you are in doubt and require clarification on any part of this document, please speak to IT Services Manager.

Provision of ICT Systems

All equipment that constitutes the School’s ICT systems is the sole property of the School.

No personal equipment should be connected to or used with the School’s ICT systems. Users must not try to install any software on the ICT systems without permission from IT Services Manager. If software is installed without permission, it may cause extensive damage to the ICT systems and users could be held personally liable for any costs incurred in rectifying the damage.

Users are not permitted to make any physical alteration, either internally or externally, to the School’s computer and network hardware.

Network access and security

All users of the ICT systems at the School must first be registered. Following registration, a network user account will be created, consisting of a username, password and an e-mail address. All passwords should be complex to ensure data and network security. All user account details are for the exclusive use of the individual to whom they are allocated. All users are responsible for
ensuring their password remains confidential and their account is secure. Passwords must be regularly changed.

All users are personally responsible and accountable for all activities carried out under their user account(s). Users must take all reasonable precautions to protect their user account details and must not share them to any other person, except to designated members of the IT Support team for the purposes of system support. Users must report any security breach or suspected breach of their network, email or application account credentials to the IT Support team as soon as possible.

Users should only access areas of the schools computer systems to which they have authorised access.

When any computer is left unattended, it must either be logged off or locked. Activity that threatens the integrity of the school ICT systems, or activity which attacks or corrupts other systems, is forbidden. Users’ network activity must not compromise the security of the data on the school ICT systems or cause difficulties for any other users.

Under no circumstances should a pupil be allowed to use a staff computer account.

All users are strictly forbidden from introducing executable files (e.g. `.exe, .cmd, .bat, .bin’) to the network as these can is some cases contain harmful viruses. This includes but is not limited to copying such files onto shared network drives, saving them on your Home Area (M:\) and running them from your USB memory stick or OneDrive. Vandalism is defined as any malicious attempt to harm or destroy any equipment or data of another user or of any other networks that are connected to the system. This includes, but is not limited to, the uploading or creation of computer viruses, the wilful damage of computer hardware, whether connected to the network or not, the deletion of data from its place of storage.

All users are strictly forbidden from introducing music and video files (e.g. `.mp3, .mp4, .mpeg, .wav, .avi’). These files in many cases are copyrighted and the copying onto shared network drives or storing on your Home Drive (M:\), OneDrive or network shared areas may breach their copyright.

All users are strictly forbidden from downloading executable, music and video files when using the school’s Internet provision.

**School Email**

Where email is provided, it is for academic and professional use. The School’s email system can be accessed from both the school computers, and via the internet from any computer. All school related communication must be via the school email address.

The sending of emails is subject to the following rules:

- Language must not include swear words, or be offensive or abusive.
- Emails or attachments of a pornographic, illegal, violent, sexist or racist nature are not permitted.
- Sending of attachments which contain copyright material to which the School does not have distribution rights is not permitted.
- The use of personal email addresses by staff for any official school business is not permitted.
The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.

Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using secure and encrypted email or password protection.

Emails should never contain staff or children’s full names either in the subject line or preferably not in the main body of the text. Initials should be used wherever possible.

Access to school /setting email systems will always take place in accordance to data protection legislation and in line with other appropriate school/setting policies e.g. confidentiality.

Members of the community must immediately tell a Safeguarding Officer if they receive offensive communication and this will be recorded in the relevant files/records.

Staff will be encouraged to develop an appropriate work life balance when responding to email.

Emails sent to external organisations should be written carefully and checked before sending, in the same way as a letter written on school headed paper would be.

School email addresses and other official contact details will not be used for setting up personal social media accounts.

**Internet Access**

Internet access is provided for academic and professional use.

The School’s internet connection is filtered, meaning that a large amount of inappropriate material is not accessible. However, on occasions it may be possible to view a website which is inappropriate for use in a school. In this case the website must be reported immediately to a Safeguarding Officer and the IT Services Manager.

All users must not therefore access from the School's system any web page or any files downloaded from the web which could be regarded as illegal, offensive, in bad taste or immoral.

Misuse of the internet may, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material, or using any of the following facilities, will amount to gross misconduct (this list is not exhaustive):

- Accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials;
- transmitting a false and/or defamatory statement about any person or organisation;
- sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive, derogatory or may cause offence and embarrassment or harass others;
- transmitting confidential information about the School and any of its staff, students or associated third parties;
- transmitting any other statement which is likely to create any liability (whether criminal or civil, and whether for the employee or for the School);
- downloading or disseminating material in breach of copyright;
- cite references for any facts that is presented. All users must not copy other people’s work and imply that it is their own (i.e plagiarism). Plagiarism can lead to formal action, up to and including, withdrawal from examination and qualifications;
• engaging in online chat rooms, instant messaging, social networking sites and online gambling;
• forwarding electronic chain letters and other materials;
• accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child.

Students are not permitted to access non educational games, media (e.g. YouTube) or chat services available online.

It is strictly forbidden for students to use the Internet for ordering goods or services regardless of their nature. In addition it is also forbidden for students to subscribe to any newsletter, catalogue or other form of correspondence via the Internet, regardless of its nature.

Any such action will be treated very seriously and may result in disciplinary action.

If necessary such information may be handed to the police in connection with a criminal investigation.

**Digital cameras**

The school encourages the use of digital cameras and video equipment; however staff should be aware of the following guidelines:

• Photos should only be named with the pupil’s name if they are to be accessible in school only. Photos for the website or press must only include the child’s first name.
• The use of personal digital cameras in school is not permitted, including those which are integrated into mobile phones. Only school cameras should be used.
• All photos should be downloaded to the school network
• The use of mobile phones for taking photos or videos of staff or pupils is not permitted.

**File Storage**

All users have their own personal area on the network, as well as access to shared network drives. Any school related work should be stored on one of these network drives. Personal files are not permitted on the shared network areas. All users are responsible for ensuring they have rights for the storage of any file in their area, for example copyright music files. All users are advised to save all files to their Home Drive (M:\) or school OneDrive where it is routinely backed up and easily accessed. All users are advised to regularly save amendments to their files to minimise data loss if their service is interrupted. Any files stored on removable media must be stored in accordance with the information access and security policy, summarised as follows:

• If information/data has to be transferred it must be saved on an encrypted, password protected, storage device
• No school data is to be stored on a home computer, or un-encrypted storage device.
• No confidential, or school data which is subject to the Data Protection Act should be transferred off site unless it is sent by secure email.
Social networking

The School has a Social Media Policy which should be read in conjunction with this policy. 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 that they 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 Headteacher.
- **All users** will notify the IT Services 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/setting.
- **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 pupil 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 pupils 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.**
- **Students must not give staff access to their area on a social networking site, (for example adding a member of staff as a friend on Facebook).**

Monitoring of the ICT Systems

The school may exercise its right to monitor the use of its ICT systems. This includes websites accessed, the interception of e-mail and the viewing of data stored, where it believes unauthorised use of the school’s ICT system is, or may be taking place, or the system is, or may be being used for criminal purposes. Any inappropriate material found will be deleted. Monitoring software is installed to ensure that use of the network is regularly checked by the IT Services Manager to ensure there are no pastoral or behaviour concerns or issues of a safeguarding or prevent nature.

Other reasons for monitoring the ICT systems include the need to:

- ensure operational effectiveness of the services provided;
- maintain the systems;
- prevent a breach of the law, this policy, or any other school policy;
- investigate a suspected breach of the law, this policy, or any other school policy.

Failure to Comply with the Policy

Any failure to comply with the policy may result in disciplinary action.

Any unauthorised use of the school’s ICT systems, Cloud-based ICT systems, the internet, e-mail and/or social networking site accounts, which the Headteacher considers may amount to a criminal
offence or is unlawful shall, without notice to the user concerned, be reported to the police or other relevant authority.

The school reserves the right to audit and/or suspend a user’s network, e-mail and/or application account(s) pending an enquiry, without notice to the user concerned.

The John Roan makes no warranties of any kind whether expressed or implied, for the network service it is providing. The John Roan will not be responsible for any damages suffered whilst on this system. These damages include loss of data as a result of delays, non-deliveries, mis-deliveries or service interruptions caused by the system or elements of the system, errors or omissions. Use of any information obtained via the network or other information systems is at the students own risk. The John Roan School specifically denies any responsibility for the accuracy of information obtained via its Internet services.

The use of the ICT is a privilege and inappropriate use can result in that privilege being withdrawn. Students will participate in a discussion with a member of staff as to proper behaviour and use of the facilities. Staff will rule upon inappropriate use and may deny, revoke or suspend usage.
ACCEPTABLE USE AGREEMENT

To be completed by all users

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.

I agree to report any misuse of the network to the IT Services Manager. Moreover, I agree to report any websites that are available on the school internet that contain inappropriate material to the IT Services Manager.

Specifically when using school devices: -

- I must not use these devices for inappropriate purposes
- I must only access those services I have been given permission to use
- 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 users 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 by student .......................................................... Date ......................................

Tutor Group ................................................................. Year Group .................

Print name ........................................................................................................................................

Signed by parent/carer ............................................... Date ......................................

Print name ........................................................................................................................................

7