The
Rose
Learning Trust

IT ACCEPTABLE USE POLICY

Date	**September 2020**
Prepared by	**Information Security Consultant**
Review Date	**September 2020 Or when legislation for Cyber Essentials is implemented**
Version	**V2**

Date	**September 2019**
Prepared by	**Information Security Consultant**
Review Date	**September 2020 Or when legislation for Cyber Essentials is implemented**
Version	**V1**

1 Introduction

It is the responsibility of all users of The Rose Learning Trust to read and understand this Policy. This Policy may be updated from time to time, in order to comply with legal and policy requirements.

2 Purpose

This IT Acceptable Use Policy is intended to provide a framework for such use of The Rose Learning Trust IT resources, it should be interpreted such that it has the widest implication and so as to include new and developing technologies and uses, which may not be explicitly referred to.

For the purpose of this policy The Rose Learning Trust includes the Trust as well as each member academy.

3 Policy

The IT Acceptable Use Policy is to be taken to include the On-Line Safety Policy

4 Scope

Members of The Rose Learning Trust and all other users (staff, students, visitors, contractors and others) of The Rose Learning Trust's facilities are bound by the provision of its policies in addition to this Acceptable Use Policy. The Rose Learning Trust seeks to promote and facilitate the positive and extensive use of Information Technology in the interests of supporting the delivery of learning, teaching, innovation and research to the highest possible standards. This also requires appropriate and legal use of the technologies and facilities made available to students, staff and partners of the Trust.

5 Unacceptable Use

The computer network is owned by The Trust and is made available to students to further their education. It is the responsibility of all who have access to the computer system to abide by the IT Acceptable Use Policy. In practice this means that:

Users of The Trust network must:

- Not use equipment, Internet or the e-mail system which is prejudicial to The Trust's interests or is defamatory or abusive
- Take care when sending emails, remembering that emails have the same legal authority as signed letters on official headed paper and therefore should treat them as such. They should not make personal comments in emails that could be used against the college and that they are responsible for all e-mails sent and for contacts made that may result in e-mails being receive
- Take care when receiving emails and do not open any suspect emails or attachments particularly where the sender is unknown, instead delete them. Notify someone in the event of receiving any threatening, lewd or inappropriate email
- Understand if they use their email for personal reasons
- Let no one else use their log in ID
- Keep their passwords secret and get them changed if they are disclosed, paying particular attention to the 'Have I Been Pwned (HIBP)' service.
- Ensure that mandatory information security and data protection training is completed without undue delay
- Unsolicited "nuisance" emails

- Understand that The Trust has authorised the reporting on all aspects of information, computer systems, Internet and e-mail usage and the recording of usage of computer systems, e-mail and the Internet, without the consent of the Users
- Using the computer system for playing games
- Using email to distribute games or links to games
- Not download attachments from non-organisational email accounts
- Not use proxy sites to circumvent the firewall
- Understand that non-compliance may result in appropriate disciplinary, contractual and/or criminal action being taken within the context and spirit of the policy
- Not use the computers for personal: financial gain, gamble, political purposes or advertising
- Respect copyright i.e. don't copy from the internet or from someone else without their permission
- If using a home computer for Trust work that they be aware of other family usage and ensure that no-one other than the approved user gains access to the Trust network
- Lock computers if logged in when leaving the computer for any short period of time (a maximum of 10 minutes is advised)
- Log out when leaving the computer for an extended period of time (more than 30 minutes is advised or during break, lunch, or lesson changeovers)
- Ensure they understand and comply with the Policy
- Only use the network for activities which relate the professional activity of student's education or for acceptable personal usage outside teaching commitments
- Know that they have a responsibility for supervising pupils' usage of computer equipment

The Trust network may not be used directly or indirectly by a User for the download, creation manipulation transmission or storage of: -

- Any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
- Unlawful material, or material that is defamatory, threatening, discriminatory extremist or which has the potential to radicalise themselves or other
- Material which promotes discrimination based on race, gender, religion or belief, disability age of sexual orientation
- Material with the intent to defraud or which is likely to deceive a third party
- Material which advocates or promotes any unlawful act
- Material that infringes the intellectual property rights or privacy rights of a third party, or that is in break of a legal duty owed to another part; or
- Material that brings The Trust into disrepute

The Trust network must not be deliberately used by a User for activities, or likely to have, any of the following characteristics: -

- Intentionally wasting staff effort or other Trust resources
- Corrupting, altering or destroying another User's data without their consent
- Disrupting the work of other Users or the correct functioning of the Trust network

- Material which is subsequently used to facilitate harassment, bullying and/or victimisation of a member of The Trust or a third party

Any breach of industry good practice that is likely to damage the reputation of The Rose Learning Trust network will also be regarded prima facie as unacceptable us of The Rose Learning Trust network,

Users shall not: -

- Introduce data-interception, password-detecting or similar software or devices to the Trust network
- Take electronic devices belonging to The Rose Learning Trust to countries outside the European Union without prior permission from the Data Protection Officer.
- Seek to gain unauthorised access to restricted areas of the Trust network;
- Access or try to access data where the user knows or ought to know that they should have no access
- Carry out hacking, fraud, communicating personal data, distributing copyrighted works e.g. music
- Intentionally or recklessly introduce any form of spyware, computer virus or other potentially malicious software

6 Consequences of Breach

In the event of a breach of this Acceptable Use Policy by a User the Trust may in its sole discretion: -

- Restrict or terminate a User's right to use The Trust network
- Withdraw or remove any material uploaded by that User in contravention of this Policy; or
- Where appropriate, disclose information to law enforcement agencies and take any legal action against a User for breach of this Policy, including but not limited to claiming all costs, fees and disbursements (including but not limited to legal fees) connected therewith

In addition, The Trust may take such action, disciplinary or otherwise, as it deems appropriate.