Rushden Academy

Aspire • Explore • Succeed

Acceptable use of ICT Policy

Date Published: September 2023

Review Date: September 2024

TOVE LEARNING TRUST

Staff must read, accept and sign the Acceptable use of ICT Policy before being able to access the academy's computer and software resources. In order to carry out effective practice, staff associated to the academy must agree to the following:

- Any personal data created or accessed by staff through email, the internet or through any computer programme may be viewed or accessed by the academy without their permission.
- Not open any emails or attachments from persons they do not know or trust and to confirm the validity of attachments from any source before opening.
- Any inappropriate material inadvertently received by email which may cause offence to others must be reported to the user's line manager. The definition of 'inappropriate material' for the purposes of this policy is anything which could potentially be illegal or personally abusive.
- Do not view, upload, download or send by email any content which is likely to be unsuitable for children or schools. This applies to any material of a violent, dangerous, racist, inappropriate sexual content, or material that could undermine network security. If a staff member is ever unsure about this point, or the suitability of any content, they should consult their line manager.
- Under no circumstances should material received from an internal or external source, which is not for business purposes, be passed on to any other system user or to any other email address. It must not be stored on any of the school's systems.
- Do not download or install applications on the academy computers.
- Academy ICT systems must not be used for conveying messages that may be considered defamatory, derogatory, obscene, discriminatory or otherwise abusive or inappropriate.
- Ensure all work/activity on the internet and email is directly related to their school work.
- If the data network is used for the transmission or storage of CCTV images, then care should also be taken to ensure that legal requirements are met.
- Do not share passwords or login names to anyone.
- Do not publish anything on personal social media sites that is linked to Rushden Academy unless authorised by the Principal.
- Under no circumstances should personal or other confidential information held on a computer be disclosed to unauthorised persons.
- Any mobile storage devices, such as laptops, should be appropriately encrypted.
- Data should not be stored or transported via portable media devices such as USB sticks or portable hard disks.
- Users must ensure that copyright laws are not infringed by the downloading, streaming, displaying or circulation of material from the internet.
- The academy does not accept liability for any personal loss or damage incurred through using the academy's IT resources for private use.
- Do not send emails to multiple external addresses without addresses being blind copied in line with the General Data Protection Regulation (GDPR). Where required to do so, emails to external addresses should follow the communication procedure.

Monitoring and Sanctions

The academy, for various legitimate business practices, may need to monitor the use of staff email and internet access from time to time to:

- establish the existence of facts (e.g. the details of an agreement made).
- monitor for quality control and staff training purposes.
- prevent or detect a crime.
- investigate or detect unauthorised use of the academy's ICT systems (including email and internet).
- intercept for operational purposes, such as protecting against viruses and making routine interruptions, such as forwarding email to correct distributions.
- gain access to routine business communications (e.g. checking email) when staff are on holiday or sick leave.

In addition:

- The academy may monitor, without notice and with justification, external and internal email and internet usage, including length of use and sites visited. It has the right, if it wishes, to access any content sent or received by the user.
- The academy may monitor and assess online content to ensure staff comply with this policy - in particular to prevent the use of computer resources for discriminatory purposes or harassment, and/or committing a criminal offence.
- Should an employee have their access to the internet and email withdrawn, with or without notice, they can appeal against this decision through the academy grievance procedure.

Penalties for misuse of computer systems will depend on the nature and seriousness of the offence. Disciplinary action may be taken against staff who contravene this policy. Viewing of illegal material by staff must be reported to the principal who will then inform the police.

Where a concern is identified that involves the Principal's use of the academy's IT, this must be raised directly to the Chair of Governors to investigate. This follows the same procedure as any safeguarding concerns.

Scope of staff email and internet acceptable use policy

The Acceptable use of ICT Policy will:

- apply to all employees, employment agency staff and contractors, and other users who have access to internal/external email and/or the internet.
- may also apply to visitors, including Governors, and cover staff as appropriate.
- be modified as necessary to enable ICT technical/support staff to perform their duties as directed.
- apply to all access to the network, internet and use of email using computers owned or operated by the school or brought onto its premises, whether accessed during normal working hours or not.

Internet and email access is provided for school business purposes. However, limited and responsible personal use may be permitted at the Principal's discretion.

Responsibilities

- Human Resources are responsible for ensuring all staff and agency staff have a signed copy of the Acceptable use of ICT Policy agreement sheet stored with their staff records **(Appendix 1)**.
- Line managers are responsible for ensuring their staff, agency and contract staff are made fully aware of the Acceptable use of ICT Policy.
- IT Support are responsible for providing line managers with appropriate information on policy compliance and monitoring of the ICT systems.

Legislation

The Academy promotes the highest standards of good practice and security in the use of information technology, and expects the highest levels of integrity in its staff. In exceptional circumstances, where there are reasonable grounds to suspect that an employee has committed a serious criminal offence, the police will be informed.

Amongst others, the following legislation applies to the use of school ICT resources:

- Regulation of Investigatory Powers Act 2000

- Computer Misuse Act 1990
- Protection from Harassment Act 1997
- Sex Discrimination Act 1975
- Race Relations Act 1976
- Disability Discrimination Act 1995
- Obscene Publications Act 1959
- Telecommunications Act 1984
- Protection of Children Act 1978
- Criminal Justice Act 1988
- General Data Protection Regulation (GDPR) 2018
- The Patents Act 1977
- Copyright, Designs and Patents Act 1988
- Defamation Act 1996
- Freedom of Information Act 2000
- Human Rights Act 1998

The policy was approved by the board: September 2023

Signature of LGB chair: 

Name of LGB chair: Mr Tim Foster

Date of renewal: September 2024

APPENDIX 1

Rushden Academy
Aspire • Explore • Succeed

Safeguarding Acceptance Document

I have read and understand my responsibilities in relation to the **Acceptable use of ICT Policy** and I agree to publish only items that promote Rushden Academy events on social media.

Name (Please print): .....

Position: .....

Signed: .....

Date: .....

Please sign and return to HR Office