

## Human Resources

# ICT User Policy

Academy level contribution:	All Academies	
CEO approval:	Sean Kelly	Date: March 2021
Education Group consultation (where applicable):	All members	Date: September 2021
LGB Cluster consultation (where applicable):	n/a	Date:
Joint Negotiating Council (JNC) consultation (where applicable):		Date: March 2021
Board ratification:	Full Board	Date: March 2021
Last reviewed on:	March 2021	
Next review due by:	April 2023	

## Contents

1. Introduction .....	3
2. Scope and purpose .....	3
3. Monitoring .....	3
4. Policy rules .....	4
5. Review of policy .....	9

## 1. Introduction

- 1.1 ICT is provided to support and improve the teaching and learning in our Trust as well as ensuring the smooth operation of our administrative and financial systems.
- 1.2 This policy sets out our expectations in relation to the use of any computer or other electronic device on our network, including how ICT should be used and accessed within the Trust.
- 1.3 The policy also provides advice and guidance to our employees on the safe use of social media. The acceptable use of ICT will be covered during induction and ongoing training will be provided, as appropriate.
- 1.4 This policy does not form part of any employee's contract of employment has been implemented following consultation with recognised trade unions.
- 1.5 A breach of this policy may result in disciplinary action being taken.

## 2. Scope and purpose

- 2.1 This policy applies to all employees, trustees / members, volunteers, visitors, and any contractors using our ICT facilities. Ensuring ICT is used correctly and properly, and that inappropriate use is avoided is the responsibility of every employee. If you are unsure about any matter or issue relating to this policy you should speak to your line manager, Schools' IT (our service provider), or a senior member of staff.
- 2.2 The purpose of this policy is to ensure that all employees are clear on the rules and their obligations when using ICT to protect the Trust and its employees from risk.
- 2.3 Employees may be required to remove internet postings which are deemed to constitute a breach of this policy. Failure to comply with such a request may, result in disciplinary action.
- 2.4 Any failure to comply with this policy may be managed through the disciplinary procedure. A serious breach of this policy may be considered as gross misconduct which could lead to dismissal. If we are required to investigate a breach of this policy, you will be required to share relevant password and login details.
- 2.5 If you reasonably believe that a colleague has breached this policy, you should report it without delay to your line manager or a senior member of staff.

## 3. Monitoring

- 3.1 The contents of our ICT resources and communications systems held in whatever media, including information and data held on computer systems, hand-held devices, tablets or other portable or electronic devices and telephones, relating both to the Employer's own education provision or any pupils, clients, suppliers and other third parties with whom the Employer engages or provides educational provision for, remains our property. Therefore, employees should have no expectation of privacy in any message, files, data, document, facsimile, social media post, blog, conversation or message, or any other kind of information or communication transmitted to, received or printed from, or stored or recorded on our electronic information and communications systems. Do not use our ICT resources and communications systems for any matter that you wish to be kept private or confidential.
- 3.2 We may monitor, intercept and review, without notice, employee activities using our ICT resources and communications systems, including but not limited to social media postings and activities, to ensure that our rules are being complied with and are for legitimate business purposes. This might include, without

limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies.

- 3.3 We will comply with the requirements of **Data Protection Legislation** (being (i) unless and until the GDPR is no longer directly applicable in the UK, the General Data Protection Regulation ((EU) 2016/679) and any national implementing laws, regulations and secondary legislation, as amended or updated from time to time, in the UK and then (ii) any successor legislation to the GDPR or the Data Protection Act 2018) in the monitoring of our IT resources and communication systems and monitoring undertaken is in line with our Workforce Privacy Notice which sets out how we will gather, process and hold personal data of individuals during their employment. Our Data Protection Policy sets out how we will comply with Data Protection Legislation.
- 3.4 In line with the requirements of Data Protection Legislation, we may store copies of data or communications accessed as part of monitoring for a period of time after they are created, and may delete such copies from time to time without notice. Records will be kept in accordance with our Workforce Privacy Notice, our Retention and Destruction Policy.

## 4. Policy rules

- 4.1 In using the Trust's ICT resources, the following rules should be adhered to. For advice and guidance on these rules and how to ensure compliance with them, you should contact Schools' IT or your line Manager.
- 4.2 The network and appropriate use of equipment
- a) You are permitted to adjust computer settings for comfort and ease of use, but these must be adjusted back after use for the next user.
  - b) Computer hardware has been provided for use by employees and pupils and is positioned in specific areas. If there is a problem with any equipment or you feel it would be better sited in another position to suit your needs, please contact your Line Manager and / or the Principal. Only the Schools' IT will be allowed to move or adjust network equipment.
  - c) Do not disclose your login username and password to anyone (unless directed to do so by a senior manager for monitoring purposes or as stated in clause 2.4).
  - d) You are required to change your password in accordance with the login prompts. Ensure that you create appropriate passwords as directed. Do not write passwords down where they could be used by another individual.
  - e) Do not allow pupils to access or use your personal logon rights to any school system. Pupils are not permitted these access rights as it could lead to a breach of the requirements of Data Protection Legislation, our Data Protection Policy and network security. Allowing pupils such access could put you at risk if your accounts are used.
  - f) Before leaving a computer, you must log off the network or lock the computer, checking that the logging off procedure is complete before you leave.
  - g) Ensure projectors linked to the network are switched off when not in use.

- h) Only software provided by the network may be run on the computers. You are not permitted to import or download applications or games from the internet.
- i) You must not use any removable storage devices (RSDs), such as USB pens where you are unsure of the content or origin.
- j) Pupil or staff data, or any other confidential information should only be stored on encrypted RSDs and not taken off the premises unless it has been encrypted to ensure data protection and confidentiality.
- k) RSDs should only be used for Trust purposes, outside of our premises where they are encrypted or have appropriate password protections.

#### 4.3 Mobile Devices and laptop use

The following rules are for use of any laptop, electronic tablets, mobile phone or other mobile device including those provided by the Trust, referred to as mobile device(s):

- a) Access to our wireless network must be approved by the Principal / Line Manager and Schools' IT.
- b) You must ensure that your mobile device is password protected. This is essential if you are taking the mobile device from our premises.
- c) You must not leave your mobile device in an unsafe place, for example in your car.
- d) Mobile devices not provided by us must have up to date anti-virus installed before being connected to the network and must be checked by Schools' IT.
- e) You must ensure you have the appropriate permissions and security in place in order to access our network at home.

#### 4.4 Internet Safety

- a) Never give out personal information such as your address, telephone number or mobile number over the internet without being sure that the receiver is from a reputable source.
- b) Never give out personal information about a pupil or another employee over the internet without being sure that the request is valid and you have the permission to do so.
- c) Always alert the Principal / Line Manager and Schools' IT if you view content that makes you feel uncomfortable or you think is unsuitable. Remember that any personal accounts accessed on our network will be subject to monitoring.
- d) Always alert the Principal / Line Manager and Schools' IT if you receive any messages that make you feel uncomfortable or you think are unsuitable.

#### 4.5 Internet and email

- a) The internet and email facilities are provided to support the aims and objectives of the Trust. Both should be used with care and responsibility.

- b) Use of the internet at work must not interfere with the efficient running of the Academies and the Trust. We reserve the right to remove internet access to any employee at work.
- c) You must only access those services you have been given permission to use.
- d) You are required to check your work emails daily.
- e) Before sending an email, you should check it carefully and consider whether the content is appropriate. You should treat emails like you would any other form of formal written communication.
- f) Although the email system is provided for business purposes, we understand that employees may on occasion need to send or receive personal emails using their work email address. This should be kept to a minimum and should not affect, or be to the detriment of, you carrying out your role effectively. When sending personal emails from your work email account you should show the same care in terms of content as when sending work-related emails.
- g) The use of email to send or forward messages which are defamatory, obscene or otherwise inappropriate will be considered under the disciplinary procedure.
- h) You should not send electronic messages which are impolite, use obscene language, are indecent, abusive, discriminating, racist, homophobic or in any way intended to make the recipient feel uncomfortable. This will be considered under the disciplinary procedure.
- i) If you receive an obscene or defamatory email, whether unwittingly or otherwise and from whatever source, you should not forward it to any other address, but you should alert the Principal / Line Manager and Schools' IT.
- j) Do not access any sites which may contain inappropriate material or facilities, as described below:
  - i. Proxy
  - ii. Dating
  - iii. Hacking software
  - iv. Pornographic content
  - v. Malicious content
  - vi. Music downloads
  - vii. Non-educational games
  - viii. Gambling

- k) Do not send malicious or inappropriate pictures of children or young people including pupils, or any pornographic images through any email facility. If you are involved in these activities the matter may be referred to the police.
- l) Under no circumstances, should you view, download, store, distribute or upload any material that is likely to be unsuitable for children or young people. This material includes, but is not limited to pornography, unethical or illegal requests, racism, sexism, homophobia, inappropriate language, or any use which may be likely to cause offence. If you are not sure about this, or come across any such materials you must inform the Principal / Line Manager and Schools' IT.
- m) Do not upload or download unauthorised software and attempt to run on a networked computer, in particular hacking software, encryption, and virus software.
- n) Do not use the computer network to gain unauthorised access to any other computer network.
- o) Do not attempt to spread viruses.
- p) Do not transmit material subject to copyright or which is protected by trade secret which is forbidden by law.
- q) Never open attachments of files if you are unsure of their origin; delete these files or report to Schools' IT.
- r) Do not download, use, or upload any material from the internet, unless you have the owner's permission.

4.6 Social networking and use of chatrooms, community forums and messaging using any device. The internet provides unique opportunities to participate in interactive discussions and share information using a wide variety of social media, such as Facebook, Instagram, Twitter, Linked In, blogs and wikis. Employees' use of social media can pose risks to our ability to safeguard children and young people, protect our confidential information and reputation, and can jeopardise our compliance with our legal obligations. This could also be the case during off duty time.

- a) You should exercise caution when using social networks. You should not communicate with pupils over social network sites. You must block unwanted communications from pupils. You are personally responsible for what you communicate on social media.
- b) You should never knowingly communicate with pupils in these forums or via personal email account or personal mobile phones.
- c) You should not interact with any ex-pupil of the Academies who is under 18 on such sites.
- d) Communication with pupils should only be conducted through our usual channels. This communication should only ever be related to our business.
- e) You must not post disparaging or defamatory statements about:
  - i. our Academies or the Trust;
  - ii. our pupils, parents or carers;

- iii. our trustees / members or employees;
- iv. other affiliates and stakeholders.
- f) You should avoid communications that might be misconstrued in a way that could damage our reputation, even indirectly.
- g) You should make it clear in social media postings that you are speaking on your own behalf. Write in the first person and use a personal email address when communicating via social media.
- h) If you disclose that you are an employee of our trust, you must also state that your views do not represent those of your employer. You should also ensure that your profile and any content you post are consistent with the professional image you present to pupils and colleagues. Take care to avoid posting comments about Academies / Trust related topics even if you make it clear that the views do not represent the views of the Academies / Trust, your comments could still damage our reputation.
- i) If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from making the communication until you have discussed it with the Principal / Line Manager.
- j) We recognise that employees may occasionally use social media for personal activities whilst at work. We authorise such occasional use so long as it does not involve unprofessional or inappropriate content and does not interfere with your role or your productivity. While using social media at work, circulating chain letters or other spam is never permitted.

**The following acts are prohibited in relation to the use of our ICT systems and will not be tolerated:**

- k) Violating copyright laws
- l) Attempting to harm minors in any way
- m) Impersonation of any person or entity, or to falsely state or otherwise misrepresent an affiliation with a person or entity
- n) Forging headers or otherwise manipulating identifiers in order to disguise the origin of any content transmitted through any internet service
- o) Uploading, posting, messaging or otherwise transmitting any content that without the right to transmit under any law or under contractual or fiduciary relationships (such as inside information, proprietary and confidential information learned or disclosed as part of employment relationships or under nondisclosure agreements)
- p) Uploading, posting, messaging or otherwise transmitting any content that infringes any patent, trademark, trade secret, copyright or other proprietary rights ("Rights") of any party
- q) Uploading, posting, messaging or otherwise transmitting any unsolicited or unauthorised advertising, promotional materials, "junk mail", "spam", "chain letters", "pyramid schemes", or any other form of solicitation.



- r) "Stalking" or otherwise harassing any user or employee
- s) Collection or storage of personal data about other users

## 5. Review of policy

- 5.1 This policy is reviewed annually by the Trust in consultation with recognised trade unions. We will monitor the application and outcomes of this policy to ensure it is working effectively.

### Raleigh Education Trust

#### ICT responsible user policy for employees

**Employee (print name):**

**Employee Agreement:**

I have read and understood the Trust's ICT responsible user policy.

I will use the computer network, internet and other new technologies in a responsible way in accordance with the rules set out in the policy.

I understand that network and internet access may be monitored.

I understand my obligations in relation to use of social media.

**Signed:**

**Date:**