Human Resources

ICT User Policy

CEO approval:	Sean Kelly	September 2023
Joint Negotiating Council (JNC) consultation (where applicable):		September 2023
Last reviewed on:	September 2023	
Next review due by:	September 2025	

Contents

1. Introduction 3
2. Scope and purpose 3
3. Monitoring 4
4. Policy rules 4
5. Review of policy 10

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, governors, 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, Colwyn Technologies (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. All users have a responsibility to use the Trust's ICT systems in a professional, lawful and ethical manner.

2.3 Any assets (electronic data or otherwise) created during employment with the Trust remains the property of the Trust during and at the end of employment. The continued use of any Trust assets in another setting or context once employment has ended will require prior authorisation from the Principal and / or a senior manager.

2.4 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.

2.5 Any failure to comply with this policy and / or deliberate abuse of the Trust's ICT systems may be managed through the disciplinary procedure. A serious breach of this policy may be considered as gross misconduct which could lead to dismissal and civil and / or criminal liability. If we are required to investigate a breach of this policy, you will be required to share relevant password and login details.

2.6 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.

2.7 The use of the Trust's ICT network is intended to be as permissive and flexible as possible under current UK legislation, DfE guidelines and the UK General Data Protection Regulations (GDPR). This policy is not intended to arbitrarily limit users' use of systems but to ensure compliance with the legal responsibilities of the Trust and staff, to safeguard the reputation and cyber security of the Trust and to ensure the safety of all users.

2.8 Users should respect this policy and other Trust policies which are in place for their protection.

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 and 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 Colwyn Technologies 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 Colwyn Technologies 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 must not be allowed to use staff computers / laptops. 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. Failure to do so could result in a breach of GDPR.

g) Ensure projectors linked to the network are switched off when not in use.

h) It is agreed that computer devices are supplied for professional use and, therefore, any personal use, such as storing photos, music, videos and games, etc., is not the responsibility of the IT support team or the Trust and is not permitted.

i) Computer equipment is supplied to users on the basis that it will be looked after responsibly and treated as if it were the user's property. Any damage caused to, or any loss of equipment assigned and that may not be considered to be general "wear and tear" may be charged for.

j) 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.

k) You must not use any removable storage devices (RSDs), such as USB sticks or removable hard drives on any of the Trust's IT equipment and particularly where you are unsure of the content or origin.

l) Sensitive data must be stored securely in approved cloud storage and must not be shared with external sources.

m) You must not make any copy of data to any storage systems other than the network storage drives or equipment provided for business use.

n) 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

4.3.1 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 Colwyn Technologies.

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. Users must take every reasonable precaution to secure any data or equipment removed from the Trust's premises.

d) Items of portable computer equipment, such as, laptops, iPads, digital cameras or portable projectors must be securely stored in a locked room or cupboard when left unattended on premises.

e) Mobile devices not provided by us must have up to date anti-virus and anti-malware installed before being connected to the network and must be checked by Colwyn Technologies.

f) You must ensure you have the appropriate permissions and security in place in order to access our network at home.

4.4 Pupil and Staff protection

a) Pupils must be supervised at all times when in an IT suite or using computer equipment.

b) When arranging use of IT facilities, a staff member should be available to monitor pupils at all times.

c) Any non-compliance by pupils should be escalated by staff in accordance with Trust policy.

d) The Trust acknowledges that staff photographs and personal data will not be published without appropriate permissions and consent.

4.5 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. Pupil identities must be concealed when publishing to the public domain.

c) Always alert the Principal / Line Manager and Colwyn Technologies 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 Colwyn Technologies if you receive any messages that make you feel uncomfortable or you think are unsuitable.

4.6 Internet, email and video conferencing

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 not attach a modem, router or other networking device to your computer in order to gain direct and unmonitored internet access as this can introduce viruses and malware onto the Trust's network. Equally, you must not change the configuration of Trust supplied computer equipment to alter network or internet settings unless directed to do so by the IT support team.

d) You must only access those services you have been given permission to use and only use the e-mail services provided by the Trust for any work-related communication. Where e-mail is used on a personal device, the device must comply with required policy and must have a passcode set.

e) You are required to check your work emails daily and agree that the use of e-mail and any attachments is intended for the addressee only and to ensure where reasonably practicable that it is virus / malware free.

f) All Trust e-mails you send should have a signature containing your name, job title and the name of the Academy you work at. Trust approved signatures are obtainable from the Trust and Colwyn Technologies.

g) 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. E-mail has the same permanence and legal status as written hardcopy documents and may be subject to disclosure obligations in exactly the same way. You must, therefore, be cautious when sending both internal and external e-mails. The professional standards that apply to internal memos and external letters must be observed for e-mail.

h) Any e-mail sent in error should be reported in accordance with the Data Breach Policy.

i) Any opinions expressed within e-mails are those of the author and do not represent those of the Trust or respective Academy. The Trust, therefore, accepts no responsibility for any loss or damage arising in any way from the use of an e-mail.

j) E-mail to outside organisations has the same power to create a binding contract as hardcopy documents. Check e-mails as carefully as written contracts, always use a spellchecker and, where appropriate, obtain legal advice before sending.

k) The use of email to send or forward messages which are defamatory, obscene or otherwise inappropriate will be considered under the disciplinary procedure. This includes sending chain letters or unsolicited commercial e-mail, also known as SPAM.

l) 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.

m) 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 Colwyn Technologies.

n) You must not purchase goods or services on behalf of the Academy / Trust via e-mail without proper authorisation.

o) You must not intentionally interfere with the normal operation of the Trust's IT network by downloading excessively large files (over 1 GB) or making use of streaming video or audio feeds, without proper reason. This activity significantly impacts our communication lines and will negatively affect others.

p) Do not **visit or** access any internet sites which may contain obscene, racist or other offensive or inappropriate material. Any downloads for personal use are not permitted. This might include the following examples:

i. Proxy

ii. Dating

iii. Hacking software

iv. Pornographic content

v. Malicious content

vi. Music downloads

vii. Non-educational games

viii. Gambling

q) 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.

r) 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 Colwyn Technologies.

s) Do not upload or download unauthorised software or hardware, whether from legal or illegal sources, and attempt to run on a networked computer, in particular hacking software, encryption, and virus software. Appropriate consent must be obtained from the IT support team and any software agreed will require the appropriate licenses. Before purchasing any hardware or software, consultation must be undertaken with Colwyn Technologies to check compatibility, licence compliance, GDPR compliance and to discuss any other implications that the purchase may have.

t) Do not use the computer network to gain unauthorised access to any other computer network or to access information that you are not authorised to view .

u) Do not attempt to spread viruses or engage in activities that waste technical support time and resources.

v) Do not transmit material subject to copyright or which is protected by trade secret which is forbidden by law. Uploading, downloading or transmitting any copyrighted materials belonging to external parties to the Trust must adhere to the publisher's policies.

w) Never open attachments of files if you are unsure of their origin; delete these files or report to Colwyn Technologies.

x) If any form of video conferencing is being used, including Teams and / or Zoom, users must ensure that they are aware of surroundings and what may be able to be seen and heard through IT used.

y) Any form of video conferencing should be carried out in accordance with best practice guidance.

4.7 Reporting Incidents

a) Users will immediately inform a member of the IT support team at Colwyn Technologies of any websites accessible from within the Academy / Trust that are felt to be unsuitable in any way for pupils.

b) Users must immediately inform a member of the IT support team at Colwyn Technologies of any abuse of the IT systems, including software or hardware, providing the location and names, where possible.

c) Users must immediately inform a member of the IT support team at Colwyn Technologies of any inappropriate content suspected to be on the IT systems. This may be contained in e-mail, documents, pictures, etc.

d) Users must immediately report any breaches, or attempted breaches, in security to the IT support team at Colwyn Technologies, in writing, or via the IT helpdesk.

e) Users must inform the Trust's Data Protection Officer if they have either committed or become aware of a data protection / GDPR breach or a near miss data breach.

4.8 Social networking and use of chatrooms, community forums and messaging using any work or personal device

4.8.1 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, TikTok, SnapChat, 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 obscene, indecent, racist or offensive remarks or comments on the internet or e-mail systems, nor should you entice others to do so.

f) You should avoid communications that might be misconstrued in a way that could damage our reputation, even indirectly. You must not transmit any material that is defamatory or which is intended to offend, annoy, harass, bully or intimidate another person or persons.

g) You should make it clear in social media postings that you are speaking on your own behalf and not as a representative of the Trust, whether in private e-mails or in public areas of the internet. 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 Academy / Trust related topics even if you make it clear that the views do not represent the views of the Academy / 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.

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

a) Violating copyright laws

b) Attempting to harm minors in any way

c) Impersonation of any person or entity, or to falsely state or otherwise misrepresent an affiliation with a person or entity

d) Forging headers or otherwise manipulating identifiers in order to disguise the origin of any content transmitted through any internet service

e) Publishing or otherwise transmitting and sharing any commercially sensitive, confidential, personal or proprietary information 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)

f) Uploading, posting, messaging or otherwise transmitting any content that infringes any patent, trademark, trade secret, copyright or other proprietary rights ("Rights") of any party

g) 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.

h) Stalking" or otherwise harassing any user or employee

i) Collection or storage of personal data about other users

5. Review of policy

5.1 This policy is reviewed every 2 years 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 User Policy for employees

Commented [sl1]: Likely to be included on Face-ed – will need to updated to reflect amendments

Commented [CB2R1]: Agreed

Employee (print name):

Employee Agreement:

I have read and understood the Trust's ICT User Policy.

I will use the computer network, internet and other new technologies in a responsible, judicious and considerate manner in accordance with the ICT User Policy.

I will ensure that every precaution is taken to protect the Trust's reputation and good name.

I will report any breaches of this policy or, any other IT related policy, by any staff member or pupil to the appropriate person.

I understand that network and internet access may be monitored.

I understand my obligations in relation to use of social media in my role in an educational setting.

Please note that failure to follow this policy will result in disciplinary investigation which may lead to disciplinary action being taken. The Trust also reserves the right to report any illegal or criminal violations to the appropriate authorities.

Signed:	**Date:**