RNN GROUP

Document Title	Information Communication & Technology (ICT) Acceptable Use Policy (AUP)
Type of document	Corporate
Brief summary of contents	To provide: • Clear guidance in the use of IT equipment • Guidance on password creation and best practice • Additional information on Acts of Parliament • Responsibilities of individuals
SLT member responsible for policy	Tony De’Ath
Date written	14th July 2016
Date last revised	5th December 2019
This document replaces	NNC ICT Policy, RC Staff AUP, DVC Staff AUP
Approval route/consultation	Department Head, SLT Member
Head of Department (HOD) responsible for policy	Chris Muffett
Author of policy	Ian Headley
Contact details	ianheadley@rnngroup.ac.uk
Publication location	Public and portals

Date of final approval	28th July 2016
Date policy becomes live	31st July 2016
Review period	Annual
Links to external standards	ICO, relevant Acts of Parliament as detailed
Related documents	• Mobile phone policy • BYOD policy • Data Protection policy • SAR policy • CCTV policy • Privacy policy
Keywords	IT, ICT, Technology, Acceptable Use, Mobile Phones, Texting, BYOD, Email, Internet, Telephones, Data Protection, Legislation, Password
Training needs	Data Protection

This document is only valid on the day of printing

Controlled Document
This document has been created following the RNN Group policy production guidelines. It should not be altered in any way without the express permission of the author or HOD detailed above.

Information Communication & Technology (ICT) Acceptable Use Policy (AUP)

Version 1.4

5th December 2019

Version Control Table

Date	Version No	Summary of Changes	Changes Made By
14/07/2016	1.0	Birth of policy	Ian Headley
26/07/2016	1.1	Data Protection EEA privacy update	Ian Headley
12/07/2017	1.2	SLT lead change Inclusion of password standards (Section 9) Creation of Section 16, Good Password Structure Additional guidance on Prevent & British Values (Section 13) Legislation update (Section 12)	Ian Headley
08/05/2018	1.3	Changes made to Data Protection Section 11 to reflect new legislation Removal of consent requirements to Section 15 Inclusion of guidance on cyber bullying and use of social media	Ian Headley
05/12/2019	1.4	Password advice updated	Kelly Condon

All or part of this document can be released under the Freedom of Information Act 2000

Table of Contents

Appendices

Policy Outline

The ability of employees to use telephones, texting services, external email and access to the Internet provides new opportunities for the RNN Group as it facilitates the gathering of information and communication with fellow employees, customers and other contacts.

However, any telephone usage, internal text services, Internet and email access (this is not an exhaustive list, all IT related equipment should be considered) opens the Group to new risks and liabilities. It is therefore essential that employees read these guidelines and make themselves aware of the potential liabilities involved in using email and the Internet and any other services provided by the Group.

The RNN Group monitors ALL Internet access on ALL RNN Group provided equipment. This includes monitoring activity even when services are provided by a third party Internet provider.

The aim of this AUP is to give staff a framework within which to carry out their duties in a way that might prevent possible legal redress or disciplinary action.

1. General Points

1.1 Use of telephones, email, internally supplied texting services and the Internet is primarily for work-related purposes.

1.2 The RNN Group has the right to monitor any and all aspects of its telephone and computer systems that are made available to you and to monitor, intercept and/or record any communications made by employees, including telephones, email or Internet communications in line with current legislation. ***See section 12.*** To ensure compliance with this policy or for any other purpose authorised within current legislation, staff are required to expressly consent to the RNN Group doing so, implicit consent is given by use of or when logging into any RNN Group resources or systems. In addition, the Group wishes to make you aware that Closed Circuit Television (CCTV) is in operation for the protection of employees, students and general public.

1.3 Computers, data stored on them (or the network) and RNN Group email accounts are the property of the Group and are designed to assist in the performance of duties. Employees should, therefore, have no expectation of privacy in any data stored or email sent or received, whether it is of a business or personal nature.

1.4 It is inappropriate use of email and the Internet for employees to access, download or transmit any material that **might intentionally or unintentionally damage the interests of The RNN Group, its students or employees. Obscene, abusive, sexist, racist or defamatory material is included within this category**. Staff requiring further clarification of the above should contact the Head of IT Services and/or the Deputy Head of IT Services. Employees should be aware that such material may also be contained in jokes sent by email. Such misuse of systems will be treated as misconduct and may, in certain circumstances, be treated by the Group as gross misconduct. The RNN Group reserves the right to use the content of any employee email in any disciplinary process.

2 Use of email

2.1 Emails should be drafted with care. Due to the informal nature of email, it is easy to forget that it is a permanent form of written communication and that material of this nature can be recovered, even when it is deleted from computers.

2.2 No contractual commitment should be intimated within the body of an email, as this will only be binding when confirmed by an official purchase order or formal written contract.

2.3 Employees should not make derogatory remarks in emails about employees, students, competitors or any other person. Any written derogatory remark may constitute libel*.* ***See section 1.4****.* Staff requiring clarification in this regard should contact the HR Director***.***

2.4 Employees must not create email congestion by sending trivial messages or unnecessarily copying of emails, this includes the initiation and propagation of chain emails. Employees should regularly delete unnecessary emails to prevent over-burdening the system.

2.5 Employees should make hard copies of emails that need to be retained for record keeping purposes.

2.6 Employees may want to obtain email confirmation of receipt of important messages. Employees should be aware that this is not always possible and may depend on the external system receiving your message. If in doubt, employees should use an alternative method e.g. telephone, to confirm receipt of important messages.

2.7 Reasonable private use of email is permitted but should not interfere with employees work. If you do choose to use the RNN Group's systems for personal use, care should always be taken regarding the size of the email being sent and sizes should always be kept to the minimum possible. The content of personal emails must comply with the restrictions set out in these guidelines and in line with current legislation. Excessive private use of the email system during working hours may lead to disciplinary action and may, in certain circumstances, be treated by the College as gross misconduct. Employees should seek the express prior permission of their line manager for personal/private use***.***

2.8 By sending emails on the Group's system, employees may be processing personal data contained within that email. If employees do not wish the RNN Group to process such personal data, alternative communication means should be used.

2.9 Employees should be aware that all emails can be recovered, even after deletion and could be used as evidence in legal proceedings.

2.10 Ensure that any work related emails sent outside the Group are accompanied by the RNN Group's standard notice that currently includes the following statement (added automatically) :

Please think of the environment before you print this email

This message (including any attachments) is sent in confidence for the addressee only and may contain confidential or sensitive information. The contents are not to be disclosed to anyone other than the addressee. Dissemination, forwarding, printing or copying of this email is strictly prohibited.

Unauthorised recipients are requested to preserve this confidentiality and to advise the sender of any errors in transmission or email admin@rnngroup.co.uk for further advice

Any contractual commitment intimated within this message will only be binding upon the RNN Group when confirmed by an official purchase order or formal written contract

Any views or opinions presented within this email are solely those of the author and do not represent those of the RNN Group

Should you require any further information about the RNN Group then please visit our web site at www.rnngroup.co.uk

****

We may monitor and disclose, in response to an official request, all incoming and outgoing emails in line with current legislation.

We have taken steps to ensure that this email and any attachments are free from any virus, but it remains your responsibility to ensure that viruses do not adversely affect you

****

National Fluid Power Centre Ltd. Carlton Road, Worksop, Nottinghamshire. S81 7HP Registration No 02854049
Create Skills Ltd. Carlton Road, Worksop, Nottinghamshire. S81 7HP Registration No 08998976
Charnwood Training Group Ltd. Carlton Road, Worksop, Nottinghamshire. S81 7HP Registration No 04770081
Aston Recruitment & Training Ltd. Carlton Road, Worksop, Nottinghamshire. S81 7HP Registration No 05157318
Rotherham Education Services Ltd. Eastwood Lane, Rotherham, South Yorkshire. S65 1EG Registration No 08415740
The RNN Group VAT group registration number is 164473106 and incorporates all of the above subsidiarity companies

3 Use of the Internet

3.1 Reasonable private use of the Internet is permitted e.g. lunchtime or breaks, but should be kept to a minimum and should not interfere with work. Excessive private access to the Internet during working hours may lead to disciplinary action and may, in certain circumstances, be treated by the Group as gross misconduct. Employees should seek the express prior permission of their line manager for personal/private use.

3.2 The sites accessed by employees must comply with the restrictions set out in these guidelines. Accessing inappropriate sites may lead to disciplinary action and may, in certain circumstances, be treated by the Group as gross misconduct.

3.3 All Internet activity is filtered and logged even if the Internet services are being provided by a third party. Details of sites visited, filtered and/or blocked under the Prevent Duty or Investigatory Powers Act 2016 may be released to authorised staff for investigatory purposes and may, in certain circumstances, be used in disciplinary action or provided to the relevant authorities.

4 Use of College Mobile Devices

4.1 As the RNN Group is embracing emerging technologies, some mobile phones (Smart Phones) are provided with access to the Internet and the Group's email systems, therefore the framework set out within this AUP applies to these devices and laptop cards with GPRS access also. ***See Mobile Phone Policy for details.***

5 Use of Texting Services

5.1 Texting services are provided for Group's business and by authorised users only, personal or inappropriate use may lead to disciplinary action.

6 Use of Bring Your Own Device (BYOD)

6.1 In using your own device on RNN Group networks, you are accepting the BYOD Acceptable Use Policy (AUP), acceptance of same will be required before use.

6.2 When you use your own device, the RNN Group does not guarantee that you will be able to use every online or networked facility it provides to its own equipment. The RNN Group accepts no responsibility for personal devices.

6.3 The RNN Group reserves the right to prevent access to any of its systems.

6.4 Personal data is transmitted at the risk of the person sending same.

6.5 It is the individual's responsibility to ensure that all use of personal devices complies with the RNN Group's policies on Prevent, eSafety, copyright, Data Protection and handling of sensitive or confidential information.

7 Use of Telephones

7.1 Reasonable private use of the Group's telephone systems is permitted e.g. for urgent personal use, but should always be with prior agreement from the employee's line manager. Excessive private use during working hours may lead to disciplinary action and may, in certain circumstances, be treated by the Group as gross misconduct.

8 Copyrighting and Downloading

8.1 Copyright applies to all text, pictures, video and sound, including those sent by email or available on the Internet. Files containing such copyright protected material may be downloaded, but not forwarded or transmitted to third parties without the permission of the author of the material or an acknowledgement of the original source of the material, as appropriate. This includes images downloaded from search engines to be used for promotional purposes.

8.2 Copyrighted software must never be downloaded. Such copyrighted software will include screen savers.

8.3 The RNN Group does not specify a maximum file size that staff are permitted to download, but it does expect common sense to prevail when downloading files. This includes the downloading of large format images and multimedia files.

8.4 RNN Group employees should not import non-text files or unknown messages on to the Group's systems without having them scanned for viruses. If employees are in any doubt as to the sender or content of a file or message, then files should not be imported.

8.5 RNN Group employees must never engage in political discussions whilst using the Group provided computer systems.

9 General Computer Usage

9.1 Employees are responsible for safeguarding their passwords for the Group's systems. For reasons of security, individual passwords should not be printed, stored on-line or given to others. User password rights given to employees should not give rise to an expectation of privacy.

9.2 Passwords are an important aspect of computer security and are the primary authentication method for access to IT resources. The Group's standards for password creation is set to a minimum of sixteen characters. See section 16 for advice and guidance for good practice in password creation.

9.3 Users who have partial access to a system must not attempt to gain access to functions for which they have no authority. The user's line manager must request additional functions in writing to IT Services.

9.4 Employee's ability to connect to other computer systems throughout the network does not imply a right to connect to those systems or to make use of those systems unless authorised to do so. Employees should not alter or copy a file belonging to another user without first obtaining permission from the creator of the file.

9.5 Staff who observe practices contrary to any parts of this policy must report them to their line manager at the earliest opportunity. All incidents must be reported to IT Services, these details will be logged with the Head of IT Services who will then initiate the appropriate investigations.

9.6 All staff will be required to agree to this AUP at logon.

9.7 Any attempt by a member of staff to steal data, intellectual property or equipment may lead to disciplinary action.

10 Software Installations / Copying

10.1 All software and hardware must be purchased through and installed by the IT Services Department.

10.2 It is a criminal offence, and contrary to the RNN Group's policy, to install software for which the Group is not in possession of a bona fide licence.

10.3 Taking copies of copyrighted software is illegal and is prohibited by the Group.

11 Data Protection

Data Protection legislation regulates the collection and processing of personal data, both electronically and paper based.

Personal data including addresses, phone numbers etc., can only be supplied by the Data Controller (RNN Group) when an official request has been received in writing. No personal information, whether this is regarding a member of staff or a student (past or present), should be accessed or disclosed at any time, unless this request is from the Data Protection Officer at the RNN Group as detailed within the Data Protection Policy.

Any enquiry of this nature, in person, by phone, or electronically must be asked to contact the Data Controller (RNN Group) with an official request in writing, even if that person says they are the parent, guardian, carer or the Police. Further detail can be located within the RNN Group's Data Protection Policy, Data Subject Access Request (DSAR) policy and the Procedure for Providing Reference/Attendance Letters.

When you give your personally identifiable information to the RNN Group, it may be used by the Group and its affiliates for the purposes of, for example, providing you services and sending you correspondence, it may additionally be transferred to entities other than the RNN Group's affiliates, these entities may be located in countries outside the European Economic Area ("EEA"), including the United States.

Each of the countries outside the EEA have different privacy laws that afford varying levels of protection for your personally identifiable information and such laws may not be as comprehensive as those that exist in the EEA.

Additional protection has been put in place by the RNN Group in the form of Third Party Data Agreements for the purposes of passing personal data and restrictions are in place for the passing of data from the third parties to other entities.

You can obtain details of the companies and countries to which your data has been transferred to by contacting the RNN Group's Data Protection Officer as detailed in the Data Protection Policy.

12 Legislation

Legislation covered within this policy:

Investigatory Powers Act 2016 (previously known as The Regulation of Investigatory Powers Act 2000 (RIPA))

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (Lawful Business Regulations)

The Data Protection Act 2018

Freedom of Information Act 2000

The Human Rights Act 1998

The Privacy and Electronic Communications (EC Directive) Regulations 2003

The Counter-Terrorism and Security Act 2015

The Computer Misuse Act 1990

The Terrorism Act 2006

Privacy and Electronic Communications (EC Directive) Regulations 2003 and amendment to the Regulations 2011

Police and Justice Act 2006

Crime and Disorder Act 1998

The Protection of Freedoms Act 2012

Serious Crime Act 2015

Copyright, Designs and Patents Act 1988

Equality Act 2010

Limitation Act 1980

Malicious Communications Act 1988

Digital Economy Act 2017

Prevent Strategy 2011

The Care Act 2014

The Children Act 1989 and 2004

Education Act 2002

Keeping children safe in education 2016 (Education Act 2002)

Childcare Act 2006

13 Linked Policies and Guidance

Policies and guidance linked to this policy:

Mobile Phone Policy

BYOD AUP

CCTV Policy

Data Protection Policy

Data Subject Access Request Policy

Cookies Policy

Privacy Policy

Personal Data Breach Procedure

What is the Counter Terrorism Act?

The Counter Terrorism and Security Act 2015 has introduced the Prevent Duty for various bodies including all FE colleges, adult education providers and independent learning providers with SFA funding or with over 250 students enrolled. Ofsted include Prevent compliance and engagement in all inspections.

What is the Prevent Duty?

Section 26 of the Counter-Terrorism and Security Act 2015 places a duty on all FE and training providers, as listed in Schedule 3 of the Act, to have "due regard to the need to prevent people from being drawn into terrorism".

The Prevent duty is also part of the Safeguarding duty for providers but one that extends to all learners of all age groups and also staff.

What are British Values?

British values are defined as "democracy, the rule of law, individual liberty and mutual respect and tolerance for those with different faiths and beliefs"; institutions are expected to encourage students to respect other people with particular regard to the protected characteristics set out in the Equality Act 2010.

What is Extremism?

The government has defined extremism in the Prevent strategy as: "vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs." This also includes calls for the death of members of the British armed forces.

14 IT Services

The IT Services Department is there to assist you. If you require any information or help about the use or set up of your computer, you should contact the helpdesk.

15 Network Account Request Form

In signing the RNN Group network account request form, you are agreeing to adhere to all of the conditions set out in the ICT AUP.

You are also giving unreserved permission for authorised members of staff to access and share with other staff members, data and emails upon leaving employment of the RNN Group. Consent for this type of access is not required as this data is processed as part of the Group's legitimate business interests.

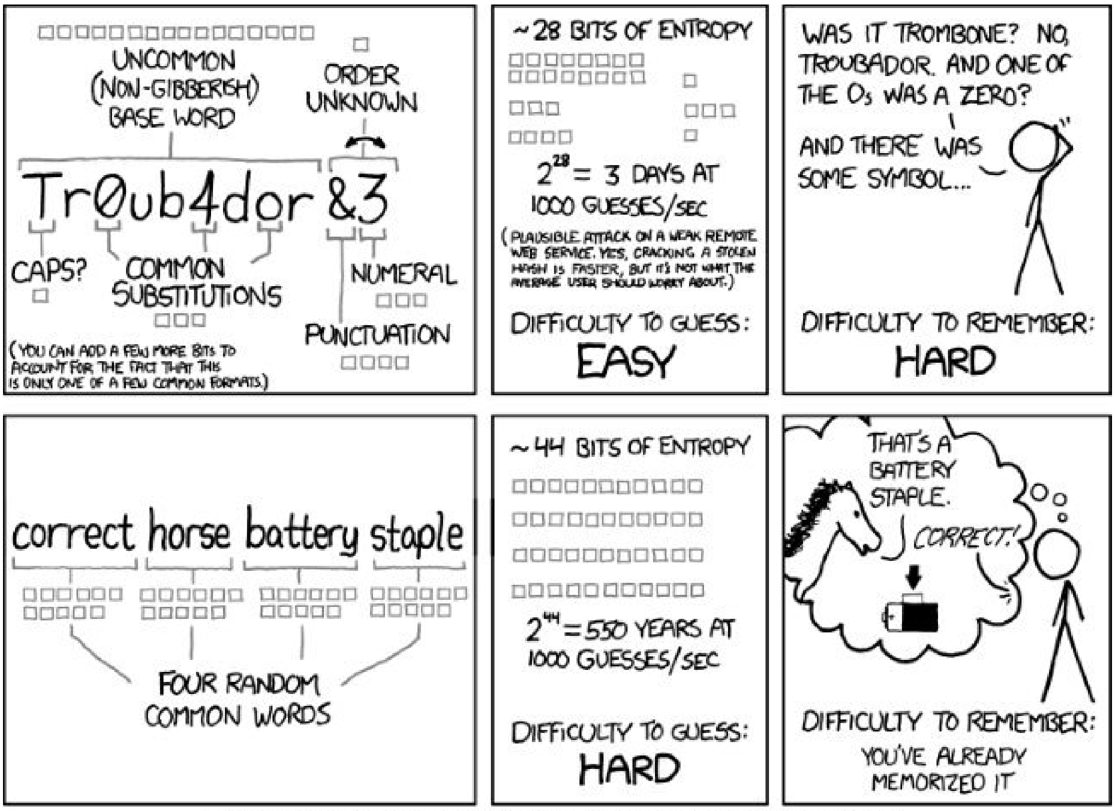
16 Good Password Structure

Password complexity is based on the characters used (uppercase, lowercase as well as symbols) including password length. It predicts how difficult a given password would be to crack through guessing, brute force cracking, dictionary attacks or other common methods.

Best password practices involve employing something memorable to the user but not easily guessed by anyone else. Because password length is one of the most important factors affecting password complexity and overall strength, a longer password can be simpler than a shorter one and still be effective, as you can see from the demonstration graphic within this policy section.

Therefore, using all of the structures available to us, we can create an extremely strong password that can easily be remembered for example:

Correct horse battery staple 2017


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

17 Cyber Bullying

Cyber bullying: Cyber bullying is the misuse of digital technologies or communications to bully a person or a group, typically through messages or actions that are threatening and/or intended to cause offence, anxiety or humiliation. (see Kidscape: "Advice, what is Cyber bullying" as recommended by the Department for Education).

Examples of cyber bullying can include but are not limited to:

Abusive comments, rumours, gossip and threats made using digital communications and/or technologies – this includes internet trolling.

Sharing pictures, videos or personal information without the consent of the owner and with the intent to cause harm or humiliation.

Hacking into someone's email, phone or online profiles to extract and share personal information, or to send hurtful content while posing as that person.

Creating dedicated websites that intend to harm, make fun of someone or spread malicious rumours.

Blackmailing or pressurising someone to do something they do not want to.

E-safety means limiting the risks that Staff, Learners and young people are exposed to when using technology, so that all technologies are used safely and securely.

Staff are responsible for their actions, conduct and behaviour on the Internet whilst using RNN Group devices and systems. Use of any technology should be safe, responsible and lawful. If you witness misuse by other Staff then this should be reported to your line manager or a member of the Human Resources Department.

Staff must not use their own or the RNN Group's technology to bully others. If you think that you might have been bullied or if you think another person is being bullied, speak with a member of the Human Resources Department.

18 Social Media Guidance

Millions of people use social media on a daily basis across the world. The following guidance seeks to help staff avoid the potential pitfalls of sharing information on the various social media sites, blogging sites and other similar networks.

The best advice that can be given is to employ common sense at all times to help keep yourself safe and to protect your own reputation and that of the College itself.

Think before you post!
Should any material come to the Group's attention that is defamatory, derogatory, offensive, abusive, bullying or in any way contravenes the ethos or reputation of the Group, the Group shall act in accordance with the relevant policy.
General guidance in the use of social media for the Group:

Do not ask students to connect on social media platforms using personal accounts.

Do not accept requests from students to connect on social media.

Before you post something, do think – would you say that aloud to or about the person, thing or organisation you are commenting on. If not, do not post it.

Do not be cryptic. Others may not be able to read between the lines you intend. If you have something to say, say it, but think before you post.

Do consider how you present yourself on social media. Always express your own views and do not refer to other people's personal views in your posts.

Do familiarise yourself with the relevant social media sites privacy settings so that you can restrict access to information you consider personal. If you are not sure how to restrict access to certain groups of people, you should act as though all your information is available to everyone or get advice on privacy settings from someone you trust.

Do not post anything that may offend, insult or humiliate others, particularly on the basis of their sex, age, race, colour, national origin, religion, sexual orientation, disability or learning needs.

Do not post anything that could be seen as threatening, intimidating or abusive. Offensive posts or messages can be seen as cyber-bullying.

Refrain from using swear words on social media as this reflects badly on you and your place of work.

Do consider the appropriateness of your profile picture. Facebook, for example, will display your profile picture even when your information is set to private. If you do not want your profile picture to be viewed, do not upload one.

Review and edit other people's comments, posts and tagged photos on your social media accounts. While you may be diligent in ensuring your account is appropriate, it is possible that you may receive inappropriate comments, pictures or videos from your friends.

Be aware that material published online can remain online for a long time. In fact, they can be around forever. Remember that future friends, colleagues, employers, Universities etc. will be able to find your posts on line for several years to come. Forever is a long time. This is particularly true if you are posting about someone else.

Do not use social media to criticise or complain about the RNN Group. We welcome comments and complaints but these should be made through the appropriate channels.

Do not setup or instigate private group chats with students without the presence of another staff member on social media platforms. Doing this without support can lead to safeguarding issues.

Do think about the source of the content you might wish to share of react to. Liking a photo just because of the content without considering the source is very risky as you could end up unintentionally supporting political/religious/extreme groups.