

**RNC Policy: E-Safety**

|  |  |
| --- | --- |
| Responsibility: | Director of Student Support Services and Head of Safeguarding/Teacher in Charge - ICT |
| Approved by SMT: | March 2023 (Interim review October 2023) |
| Approved by Governor Committee:  | Education and Training Committee – November ‘23 |
| Date of next review: | March 2024 |
| EIA Completed: | June 2019 |
| Published on Website:  | Yes |
| Uploaded to Smartlog: | Yes |
| Available to: | Staff/Students/Volunteers/Stakeholder |
| Other relevant policies and reference documents - held on the RNC Intranet: [Policies, Procedures and Resources - Home (sharepoint.com)](https://rncac.sharepoint.com/sites/policiesproceduresresources)* Anti-Bullying and Harassment Policy
* Safeguarding Policies for Children and Vulnerable Adults.
* Guidance for Safer Working Practices for Staff Working with Students
* Student Disciplinary Policy
* Acceptable Use Policy - Computing and IT Systems and Resources
* Bring your own Devices Policy
 |
| **Commitment Statement**RNC is committed to the fundamental values of equality, diversity and inclusion, which creates a supportive environment for all members of our community to live, work and study. Our commitment to equality and diversity means that this policy has been screened in relation to the use of plain English, the promotion of the positive duty in relation to race, gender and disability and to eliminate discrimination to other equality groups related to age, sexual orientation, gender identity, marital or civil partnership status, pregnancy or maternity and religion or belief. We believe that safeguarding has paramount importance and RNC recognises its responsibility and duties within the Government Prevent Strategy to be aware of and where appropriate act to ensure the safety of all students from radicalisation and extremism.This document is available in alternative formats on request. If you think RNC can improve the fairness of this policy please contact the author who has responsibility for the review and update. |

Contents

[1 Introduction 3](#_Toc153195541)

[2. Policy Scope 3](#_Toc153195542)

[3. Roles and Responsibilities 4](#_Toc153195543)

[4. Security 5](#_Toc153195544)

[5. Prevent Policy 6](#_Toc153195545)

[6. Behaviour 6](#_Toc153195546)

[7. Education and Training 6](#_Toc153195547)

[8. Personal Information and Data Protection 7](#_Toc153195548)

[9. Further Information 7](#_Toc153195549)

[Appendix 1 - Staff use of social media 9](#_Toc153195550)

[Appendix 2 - E-Safety guidelines and advice for students 10](#_Toc153195551)

[Appendix 3 – Letter to Parent(s) Guardians(s) 14](#_Toc153195552)

# Introduction

* 1. RNC believes that our students should be able to fully benefit from accessing the wide range of technology available. We believe that all of our students, staff and volunteers should receive guidance to be able to make informed decisions and stay safe by being able to control their online experiences.
	2. All references to ‘staff’ in this policy should be read to include volunteers.
	3. RNC recognises the need to fully assess risks and instigate control measures associated with digital technology. Our approach is to implement safeguards within the College and to support staff and students to identify and manage risks independently. We believe this can be achieved through a combination of security measures, training and guidance, and implementation of our associated policies.
	4. The risks associated with accessing the internet, electronic communication and use of mobile devices require robust control measures as RNC regards the Safeguarding of our students as a priority. The key overarching risks for students and the organisation as a whole are:
* Unwanted contact/grooming
* Cyberbullying
* Harmful content, illegal materials
* Privacy and digital footprint
* Online fraud
* Individuals may be the target of promoting extremism, terrorism or ‘cyber bullying’ on social networks, email etc
* Potential of hacking, data loss and generating undesirable content from College systems, such as ‘spam’ emails or website defacement.
* Potential Health and Safety legislation breaches
* Reputational loss to the College from security or wellbeing issues
	1. The E-Safety Policy encompasses student use of the internet, electronic communications and mobile devices. It highlights the need for robust induction and ongoing guidance for students about the benefits and risks of using new technology, and provides safeguards and awareness for users.
	2. RNC will ensure that staff receive the necessary training to feel confident in providing guidance and support when responding to any E-Safety issues.

# Policy Scope

2.1 This policy applies to all members of the College community who have access to the College IT systems, both on the premises and remotely. It also applies to visitors, guests and all other stakeholders of the College using the College’s infrastructure.

* 1. The E-Safety Policy applies to all use of the internet and electronic communication devices such as email, mobile phones, wearable technology, virtual assistants, games consoles, social networking sites, braille note takers and any mobile device that allows internet access.

# Roles and Responsibilities

3.1 Responsibility for the implementation of the E-Safety Policy rests with the Executive Principal, and with Governors for ratification.

3.2 The day-to-day responsibility for E-Safety is delegated to the Designated Safeguarding Officers; Jess Price (Lead), Jeremy Perrott, Victoria Hamilton, Tim Morton. Specialist responsibility for E-Safety guidance is provided by the Safeguarding Committee, ICT representative - Ailsa Macleod and Andy Powell, Technical Support Manager.

3.3 The day to day responsibility for filtering and monitoring of internet accessible material is delegated to the safeguarding officers: Jess Price (Lead), Jeremy Perrott, Victoria Hamilton, Tim Morton. Specialist responsibilities for filtering and monitoring is provided by Andy Powell (Technical Support Manager)

**S**taff****

3.4 All staff are responsible for ensuring the safety of students and should report any concerns immediately to their line manager and to the E-Safety inbox [esafety@rnc.ac.uk](file:///C%3A/Users/mary.kenyonjames/AppData/Local/Microsoft/Windows/Temporary%20Internet%20Files/Content.Outlook/esafety%40rnc.ac.uk)

3.5 All staff are required to inform students of their responsibilities regarding E-Safety and remind them how to report concerns they have about their own E-Safety or the safety of other students using the E-Safety email address. This should be reinforced throughout the academic year.

3.6 When informed about an E-Safety incident, staff members must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it, or those involved. For issues where an immediate response is required a report must be made to a Designated Safeguarding Officer and the incident recorded using the College E-Safety email address esafety@rnc.ac.uk

3.7 All instances of concern whether on personal devices such as phones, laptops, tablets or College devices should be logged using the E-Safety email address esafety@rnc.ac.uk

3.8 Staff should ensure that all students know what to do if they have E-Safety concerns, and who to talk to. In most cases, this will be their Tutor/link worker. Again this should be reported via esafety@rnc.ac.uk.

3.9 The procedure for reporting incidents is the same for staff and students. Emails will be addressed by the E-Safety officers and appropriate actions will be taken. A log of all reports will be recorded, detailing the action taken.

Where any report of an E-Safety incident is made, all parties should know what procedure is triggered and how this will be followed up. Where it is considered appropriate, the Designated Safeguarding Officer may be asked to intervene with appropriate additional support from external agencies.

3.10 All staff are responsible for using the College IT systems and mobile devices in accordance with the College Acceptable Use Policy - Computing and IT Systems and Resources and the E-Safety Policy, which they must actively promote through embedded good practice.

3.11 All staff are required to confirm to say they have read these policies via their Smartlog declaration.

3.12 Staff are responsible for participating in staff training on E-Safety and displaying a model example to students at all times.

3.13 All digital communications between staff and students must be carried out in line with the RNC ‘Guidance for Safer Working Practices for Staff Working with Students’. (Appendix 3)

****ICT teaching staff****

3.14 As part of their induction all new students will meet with a member of Assistive and Digital Technology (A&DT) teaching staff who will go through the E-Safety Policy. Students will not be able to access the College system or student Wi-Fi until this has taken place. A record is kept of all students who attended the session.

****Students****

3.15 All students using College IT systems must adhere to the E-Safety Policy, the Bring Your Own Devices (BYOD) Policy and the Acceptable Use Policy Returning students attend a policy update at the beginning of the year and their attendance is recorded.

3.16 Students are responsible for using the College IT systems and their personal IT/mobile devices in accordance with the College Acceptable Use Policy - Computing and IT Systems and Resources, the Bring Your Own Devices Policy and the E-Safety Policy

3.17 Students are responsible for attending an annual all student E-Safety briefing as part of the PDP programme. E-Safety is also embedded within Assistive and Digital Technology lessons as part of the Assistive and Digital Technology curriculum.

3.18 Students are expected to seek help and follow procedures if they are worried or concerned. If they believe an E-Safety incident has taken place involving them or another member of the College community they should speak to a staff member or Designated Safeguarding Officer or contact the E-Safety email esafety@rnc.ac.uk.

3.19 Students must act safely and responsibly at all times when using the internet and/or mobile technologies.

# Security

4.1 Appropriate security measures include the use of enhanced filtering and protection of firewalls, servers, routers, workstations and laptops etc to prevent accidental or malicious access of College systems and information.

4.2 Anti-virus software is used to scan computers, internet traffic and emails to automatically block the majority of damaging programs.

4.3 Network traffic is scanned to prevent viruses and other ‘malware’ entering college systems.

4.4 Emails are automatically scanned to remove the majority of unwanted spam content according to manufacturer/service provider standards.

4.5 RNC has a contractual duty, as part of its agreement to connect to the JANET network, to be able to track and report on suspicious network traffic, virus infection or abuse, and a legal responsibility to be able to provide suitable logs to law enforcement agencies.

# Prevent Policy

RNC seeks to identify and remove any risks of radicalisation and/or extremism to students, staff and volunteers. The Prevent Strategy and Duty and risk assessment identifies measures in place to reduce this risk emanating from online sources.

# Behaviour

6.1 Online communication can take many forms, such as email, text, video conferencing/webcam chat, gaming and instant chat. It is essential that all students and staff are aware of existing College policies that refer to acceptable behaviours when communicating online.

6.2 All staff and students must be aware of the E-Safety guidelines and advice for students and staff (appendix 1)

6.3 The College expects all users of technologies to adhere to the standard of behaviour set out in the Acceptable Use Policy - Computing and IT Systems and Resources.

6.4 The College will not tolerate any abuse of IT systems. Whether offline or online, communications by students and staff should be courteous and respectful at all times.

6.5 Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the student and staff disciplinary policies and procedures.

6.6 Where conduct is considered unacceptable, the College will deal with the matter internally. Where conduct is considered illegal, the College will report the matter to the police.

# Education and Training

7.1 With the current unlimited nature of internet access it is impossible for the College to eliminate all risks for staff and students. The College will support staff and students through training and education. This will provide them with the skills to be able to identify risks independently and manage them effectively.

* 1. All students are initially timetabled for ICT. This ensures that they are aware of their responsibility to adhere to the safety guidelines laid down by the College, and to ensure that they understand how to use technology safely and how to keep their information safe while using the internet. Students are also encouraged to think of others and ensure that their personal information and the information they have about others is not communicated in a way that could be unsafe.
	2. Parents of under 18 students are informed of the potential risks associated with own data use and that we are only able to monitor the Student Wi-Fi (Appendix 3)

**For students**

7.4 Students attend an E-Safety induction as part of their initial induction to RNC. During pre-entry assessment students are asked about their internet use. This information, alongside any staff concerns, is used to inform the scope of IT topics required by each student during their study.

7.5 Issues associated with E-Safety apply across the curriculum and students should receive guidance on what precautions and safeguards are appropriate when making use of the internet and technologies. Students should also know what to do and who to talk to when they have concerns about inappropriate content, either where that material is directed to them, or where it is discovered as part of a random search.

7.6 Within classes students are encouraged to question the validity and reliability of materials researched, viewed or downloaded. They are encouraged to respect the copyright of other parties and to cite references properly.

**For staff**

The Designated Safeguarding Officers and members of the ICT and Technical Support teams have an overview of any E-Safety issues. They are the Designated E-Safety Officers for the College. Staff take part in training identified by the E-Safety Officers which is recorded on CPD records. All staff are required to complete annual E-Safety awareness training through Smartlog. Any new or temporary users receive training on the College IT system and are required to sign the relevant policy declarations: E-Safety; Acceptable Use Policy - Computing and IT Systems and Resources Declaration and Bring Your Own Devices Policy.

# Personal Information and Data Protection

RNC must comply with the Data Protection Principles which are set out in the Data Protection Act 1998. Students and staff should refer to the RNC Data Protection Policy and Procedure for guidance on the College’s position in relation to personal information and data.

# Further Information

Useful links for further information:

* Child Exploitation and Online Protection Centre

<http://www.ceop.police.uk/safety-centre/>

* Internet Watch Foundation [Internet Watch Foundation IWF - Eliminating ChildSexual Abuse Online | IWF](https://www.iwf.org.uk/)
* UK Council for Child Internet Safety (UKCCIS)

<https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis>

* Stay Safe Online <http://staysafeonline.org/>
* Get Safe Online <http://www.getsafeonline.org>

## Appendix 1 - Staff use of social media

**In line with Guidance for Safer Working Practices for staff who work with Children and Young People**

* Communication between students and staff, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones, text messaging, emails, digital cameras, videos, web-cams, websites and blogs.
* Staff must not give their personal contact details to students, including email addresses, Facebook (or equivalent) accounts and home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/carers. Email or text communications between staff and students outside agreed protocols may lead to disciplinary and/or criminal investigations. This includes communications through internet-based websites.
* Staff must not request, or respond to, any personal information from the student, other than that which might be appropriate as part of their professional role.
* Staff are not permitted to be friends with any current students on any social networking site unless through an official College account.
* Staff should also consider the suitability of being friends with ex-students, as many of these will be friends with current students.
* If staff use social networking sites they need to ensure that their privacy settings are set appropriately having regard to this policy.
* If staff wish to use digital media sites for teaching purposes they must speak with their line manager and a member of the Marketing Team. Staff will need to undergo relevant training before they can create accounts under the RNC brand.
* The College has a presence on various social networking sites such as Facebook and Twitter. Each account is used for a specific strategic purpose to boost student recruitment and engagement and to position RNC as a national centre of excellence. Ideas for stories are welcome but notice should be given to allow for scheduling.

## Appendix 2 - E-Safety guidelines and advice for students

**Use of the internet**

Students and staff should be aware of the digital footprint left behind by any activity on the internet. Once something is posted online it is very difficult to control what it is used for and often it can never be removed. It can be searched for and will be available on a global level. It can be easy to share more than you are comfortable with being publicly available without realising the risks.

The following provides some general advice to help keep you safe when using the internet.

**Using email**

Electronic mail (email) includes all electronically transmitted messaging systems. Students and staff should refer directly to the Acceptable Use Policy - Computing and IT Systems and Resources before using email.

* Never put personal information such as bank details, passport numbers etc in an email, even if it appears to be a trusted source. Emails can easily be forwarded and we don’t always consider the email thread when forwarding an email.

**Social Networking/chat rooms**

* Students should be aware that RNC staff are not permitted to share personal information or be ‘friends’ with current students on any social network unless specifically linked to a College social media account i.e. RNC Facebook. Students should not be offended or insulted should a ‘friend’ request be ignored or declined.
* Be careful about who you are talking to. Only talk to those you know or trust within a chat room or forum where you know your profile settings are secure.
* Think carefully before accepting ‘friend’ requests from people you do not know in the real world.
* Be aware that it is easy to lie online – someone may not be who they say they are. Just because someone seems nice online does not mean they are like that in real life. College staff will provide support should you require it.
* If you have accepted a ‘friend request’ from someone online that you do not know in real life, limit the information you share with them.
* Make sure your profile settings are set so only people you trust can view your details.
* Never post personal information for just anyone to view, such as your name, home address, email address, date of birth, phone number or bank details.
* Learn how to block contacts, save a ‘chat log’ and know where to go if you are concerned about any online interactions.
* When registering to use a mobile phone on any social networking site, be aware that the site will make your phone number public without asking you first.
* Anything that gets posted on the internet can never be undone. Be aware of what types of pictures you have posted on sites like Facebook, Instagram, Snapchat, YouTube and Twitter etc, especially if you would not want your family or future employers seeing them.
* Remember to check your security settings when apps or websites are updated, your settings could be changed without you realising.
* Never share passwords with anyone, on or offline.
* Never arrange to meet someone you have met on the internet on your own. Always inform staff of plans, go with a friend and meet in a public place. Ensure you have your mobile phone fully charged and with you before you leave the campus.

**Webcam chat**

* If chatting on a webcam or on ‘skype’ or ‘face time’ for example, never speak to people that you do not know and trust in real life.
* Remember that webcam feeds can be recorded and faked and always ensure you turn the webcam off after use, preferably ensure the camera is covered.
* If someone asks you to do something you are uncomfortable with while having a webcam conversation, end the conversation and turn off the webcam. Report the incident to a Designated Safeguarding Officer.

**Online gaming**

* If playing games online, again remember not to share information with people you do not know in real life, keep ‘gaming’ friends in games only.
* Online games can be highly competitive and bullying can be common. Ensure you learn the reporting procedures for concerns for the game before you begin playing. Seek support if you are unsure how to do this.

**Mobile technology - Including mobile phones with camera and video functionality**

* Mobile phones and other devices can do much more than make voice calls. Integrated cameras, video messaging, mobile access to the internet, and location-based services are commonplace. Mobile technology users are always contactable, never really ‘switch off’ and as a result, are potentially always vulnerable.
* E-Safety concerns related to mobile technologies are similar to using fixed internet connections except the user is less likely to be in a supervised environment.

**Text messages**

* Never give out your mobile number or location to strangers or put it online. You never know who can view your information.
* Never pass on a friend's mobile number, always ask your friend to pass on their number.
* Avoid putting personal information in texts, such as bank details and passwords.
* Do not register your number on sites that are not secure since you do not know who they are passing your number on to. If ever you are unsure, always seek support from a member of staff.
* When registering on a site only give information you are required to give. This is usually denoted with an asterisk: \*.
* If you receive anonymous texts, ask who the person is but do not give out any personal information. If they refuse to tell you who they are, do not reply again and do not call them. Block their number so they cannot contact you.
* Do not enable the location or photo geo-tagging on your phone unless it is necessary for you to do so for mobility services.
* If you are receiving threatening or abusive messages, make sure to keep them and show member of staff as soon as possible. Screen capture them if you can. If you are unable to do this, seek support.
* Never send picture messages of yourself to people you have never met offline before. Even if they send you one of themselves, you can never be sure that it is really them.
* Be careful about what types of pictures you send to anyone in your contacts since you never know what they could do with them, and you cannot be sure the person you have sent them to will delete them, even if they say they have.

**Sexting**

* This is when somebody sends an inappropriate text or image to other people, for example forwarding self-taken images by text over the internet. A good way of judging whether an image is ‘decent’ is whether you would be happy for a member of your family to see it.

* Avoid sending pictures to anyone that you would not be happy for a family member to see. Once you have sent the image, you have no control over how it is used.
* Students should report any concerns regarding sexting to a member of staff.

**Buying on the internet (including music download sites)**

* When you buy things online you should be aware that, no matter how secure you may think the websites you are purchasing from are, you must consider the potential for online fraud.
* There are some steps you can take to protect yourself from risks:
* Ensure that the website is known to you or has been recommended by a reliable person;
* Look for the https line;
* Look for the padlock symbol;
* Never give out your cash card pin number;
* Use a gift card rather than your bank card.
* Students should always seek staff support if they are unsure about how to purchase safely online.

**Use of images and video**

* The use of images or photographs is popular in teaching and learning and should be encouraged where there is no breach of copyright or other rights of another person. This will include images downloaded from the internet and images belonging to staff or students.
* All students and staff receive training on the risks associated with downloading these images as well as posting them online and sharing them with others. There are particular risks, for example, where personal images are posted onto social networking sites.
* College staff will provide information to students on the appropriate use of images. Our aim is to reinforce good practice as well as offer further information for all users on how to keep their personal information safe.
* Students must not collect images of people and post them on the internet without the permission of those shown in the images.
* Photographs of activities on the College premises should be considered carefully and have the consent of the Student Recruitment Manager before being published. Approved photographs must not include names of individuals unless this has been specifically agreed**.**

**Reporting phishing emails and Texts**

You can report phishing emails to the authorities. You just need to forward your phishing email to report@phishing.gov.uk

You can also report phishing texts to the authorities. You just need to forward your text to 7726.

## Appendix 3 – Letter to Parent(s) Guardians(s)

Dear Parent/Guardian

**IT Systems and Resources**

**Issue of Equipment**

We will be issuing all students with a laptop for their use while at College, they must use this for all subject areas. The laptop will be set up with their preferred assistive technology. They will have access to Microsoft Office and OneDrive through the College licence. If they require addition software for their course, this will also be installed. The students are responsible for their laptops and must report issues to their IT teacher as they arise. We call in the laptops for periodic checking and all students must return laptops to us at the end of the summer term so we can carry out software updates and maintenance checks.

Some students may also be issued with additional equipment such as Braille displays, again the students are responsible for its safe keeping.

**RNC College Wi-Fi**

Whilst many students make use of the student Wi-Fi at RNC an increasing amount of young people attending RNC have their own data contracts which they also use.

We need to make you aware that the student Wi-Fi system is subject to strict vetting and firewall limitations, in line with most educational establishments offering student Wi-Fi. You also need to be aware that data supplied under contract to your young person and accessed directly by them through their own devices does not pass through any vetting or firewall procedures.

We would recommend that if your young person is at or is coming to College with their own data allowance you ensure that they are aware of the risks of accessing unfiltered internet content. For those under 18 we would recommend that whoever takes out the contract for content on their behalf also ensures the settings are appropriate for those who are under 18 and that any adult content is blocked.

In the halls we also have an additional Wi-Fi called “RNC-Halls” that can be used for connecting games consoles and smart devices such as Amazon Echo, firesticks, Apple TV and Google Home to the internet.

Please ensure that your young person knows to connect to the Wi-Fi rather than using their personal data, especially if this is limited. We would suggest you put a cap on addition data in order to avoid any unexpected bills.

**Testing Electrical Equipment**

Although we do not electrically test students’ personal electrical equipment, we do offer this service if anyone has any concerns. The student will need to contact the technical support team.

**TV Licences**

Student TV Licence – Each student will need a TV licence if they have a TV in their room and it is plugged into an aerial. The law has changed, and the student must be covered by a TV licence if they download, record or watch any BBC programmes including iPlayer – live, catch up or on demand, no matter what device they use.

Your TV licence will cover your young person if their device is powered solely by its own internal batteries and not connected to the mains such as a mobile phone or tablet.

All the halls have brand new 55” SMART TVs in the common rooms that are covered by our College TV licence.

Please let us know if you have any concerns about the above content.

Yours faithfully

**Tic of Assistive and Digital Technologies**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Amendments | Author  |
| 1.0 | May 2017 | Approved at SMT | MKJ |
| 1.1 | November 2018 | Reviewed, addition to 3.2 and of 3.4 re, behaviour monitoringApproved at SMT | MKJ |
| 1.2 | September 2019 | Removed 3.4 as more detailed guidance provided from 3.10 onwardsAmended to clarify applies to staff and volunteers throughoutAmended to reflect that Appendix 4 is aimed at students | MKJ |
| 1.3 | September 2019 | Formatting/numbering updating | EG |
| 1.4 | January 2022 | General updating. Section 2 included wearable tech. Section 3 updated job titles and responsibility. Section 4 included laptops. Section 7 added 7.3 for U18’s. Appendix 5 added. | TA/AP |
| 1.5 | March 2023 | Public WIFI network added for student consoles and devices – appendix 5E&T signed off policy – May 2023 | TA/AP/JP |
| 1.6 | October 2023(Interim review) | 3.3 Added to cover filtering and monitoring responsibilities 3.2 – staff names updated3.11 & 3.15 – declaration no longer completed as recorded on smartlog or via attendance at student induction sessions. 3.14 Job titles updated3.17 – ref to PDP added7.6 ref to Smartlog training addedAppendix 1 removed - E-Safety Policy – Staff Declaration – this is now covered within SmartlogAppendix 2 removed - E-Safety Policy – Student Declaration – students no longer sign this, a register is kept of their attendance for initial policy briefing and annual policy updates.  Appendices renumbered.  | TA/JP |