Title	Student IT Acceptable Use Policy
Version	Version 1
Effective Date	12.01.21
Review Date	12.01.24
Lead	
Agreed by	

Student IT Acceptable Use Policy

1.0 Introduction

The purpose of this document is to ensure that all students using computing facilities provided by Newvic, including the internet and email are aware of NewVIc's and their own responsibilities. This document outlines what is and is not acceptable when using computing facilities and specifies the consequences of unacceptable behaviour in accordance with the NewVIc's legal requirements and disciplinary procedures.

1.1 Computing facilities

The network support team manages access to and security of all computing facilities. Computing facilities can be interpreted as any computer hardware or software including databases owned or provided by NewVIc, network access, data storage, and internet and email facilities. This policy covers the use of any computing facilities accessed by NewVIc students when having borrowed equipment to use at home. The College uses several devices to monitor internet activity including a firewall and a web filter/content filter appliance. We monitor and automatically report on any inappropriate attempts to access unsuitable sites.

2.0 Acceptable use

NewVIc supports and encourages the use of college computing facilities for the benefit of students. The internet in particular is a valuable source of information and resources. Examples of acceptable use include carrying out research and using authorised software and hardware as part of your education and student journey.

Only those with authorisation may access NewVIc's computing facilities. Security is maintained through the use of personal passwords, which should be stored securely and changed on a regular basis. Passwords should not be shared.

All use of the college's IT facilities must comply with safeguarding legislation and the Prevent duty guidance.

Please refer to the online remote learning code of conduct for expectations around online learning. Breaches of the code of conduct will lead to disciplinary action.

2. 1 Private use

Reasonable personal use of computing facilities is allowed where there is no conflict with college objectives and college policy. All computer activity is subject to monitoring.

2.2 Unacceptable use

The following are activities that will result in action being taken against users of computer facilities.

Any unauthorised activities related to the use of NewVIc's computer facilities that cause those facilities to be put at risk, e.g.

- using peer-to-peer software without authorisation.
- downloading and/or installing unauthorised and or unlicensed products.
- causing criminal damage to computing facilities.
- deliberate introduction of malicious programs e.g. viruses, trojans, spyware.

Any unauthorised activities related to the use of NewVIc's computer facilities that cause NewVIc's reputation or financial integrity to be put at risk or be damaged, e.g.

- using NewVIc's computing facilities for entering into contracts outside of NewVIc's financial and legal procedures.
- using NewVIc's computing facilities for personal gain.
- attempting to access any college computing facilities without prior authorisation, e.g. using another person's password or making any unauthorised changes to data, as specified in the Computer Misuse Act, 1990.

Any unauthorised activity that may bring NewVIc into disrepute, e.g.

- sending chain-emails or carrying out activities that may encourage spam.
- criminal acts e.g., in relation to child pornography, hacking, credit card and other fraud and extremism, radicalisation and terrorism.
- harassment, including sending inappropriate emails even if sent as a joke.
- making and/or accessing obscene, pornographic or racist materials, any form of prejudicial or discriminatory behaviour or items likely to cause offence to others
- using chat-rooms for inappropriate discourse e.g., sexual / racist or any form of prejudicial or discriminatory behaviour in nature.
- unauthorised uploading or downloading of music and video files in any format, or other materials covered by copyright law.
- using any device, social media or messaging platform to take or send inappropriate comments, images or other material. Examples include but are not limited to cyberbullying and sexting and upskirting.

Any unauthorised activity that is against NewVIc's Student Code of Conduct, eg

- using the college's network to distribute any material including that of a political or religious nature or to organise campaigns, petitions and events without permission, including through social media.
- using the college's name or brand without permission, including on social media
- using the college's network to attempt to send all student emails.

This list is not exhaustive but sets out a framework of approach to misuse of computing facilities. If in doubt, users should check with their tutor.

3.0 Wi-Fi/Wireless access and use of own devices

The internet can be accessed using your personal devices (Smartphones, tablets, laptops) on the NewVIc_MD network. You can access the wireless network using your domain username and password that the college has issued to you.

Usage of Wi-Fi is entirely at the risk of the account holder and if you are using a laptop, then we strongly recommend that the laptop has up-to-date anti-virus and all security updates applied before using the service.

NewVIc cannot be held responsible for the privacy or security of your activities. It is strongly recommended that you take due care when transmitting confidential information such as credit/debit card details over the internet.

The college reserves the right to restrict access to sites which are bandwidth intensive in order to maintain a quality of service across the network.

The Network team cannot guarantee personal devices will connect and cannot offer any support relating to personal devices.

Please be aware that the same principles of acceptable use apply to the use of your personal devices in college, including when accessing private wireless networks. This includes any unauthorised activity, such as accessing extremist websites and other examples as listed above.

4.0 Monitoring

NewVIc retains the right to monitor the use of college computing facilities and monitors all network activity including internet and email activity, use of computer applications and changes to hardware and software configuration.

5.0 Safeguarding

We employ a filtering service to ensure that we protect students from accessing websites which expose them to harm or contain unsuitable or illegal material. We do not allow by default internet researching of terrorism and counter terrorism in the course of student learning. If a student wishes to access any restricted websites for the purposes of academic research, permission needs to be granted by the Assistant Principal/Designated Safeguarding Lead. The request will be considered, taking advice from external agencies where appropriate, before making a decision. Records will be kept of all such requests and monitored.

6.0 Enforcement

Failure to comply with NewVIc's acceptable use policy will result in disciplinary action being taken. Please refer to the disciplinary process.

Email policy

These guidelines cover both internal and external electronic communications:

- **Intranet** - internal email and local web
- **Internet** - external email, web, chat etc

1. **Always use the most efficient and effective means of communication**. Consider the purpose of the message and the availability of the person you are communicating with. Email, telephone, memoranda, face-to-face discussion - all have their place. Use the communication that is most appropriate.
2. **Don't send anything by email that you would not be happy to put your name to on headed paper or that you would not be prepared to say in person**. This includes rude, angry or defamatory messages, or remarks about people.
3. **Contributions to external discussion groups or blogs and all social media platforms via the Internet may be handled in two ways**. If you are commenting on a matter in which NewVIc has a direct interest and as a representative of NewVIc, your comments should be in line with NewVIc policy. If you do not know what NewVIc policy is on a certain issue, or if you are commenting on something in which you have a personal or academic interest, please make this clear**.**
4. **If you wish to disseminate copyright material, please secure written permission from the copyright holder in advance**.
5. **It is illegal to use email to create or transmit offensive, obscene, indecent or extremist images, data or other material.**
6. **Make sure your email is relevant to the person receiving this.** Recipients do not normally welcome unwanted or foolish email. In particular, it is irritating and time-wasting to receive emails that are not directed at you.
7. **All student emails can only be sent by authorised staff.** A list can be found on the College intranet under the IT & Network area.

‘

Policy Monitoring and Review

The effectiveness of the policy will be monitored by the lead in the Senior Leadership Team.

This policy will be reviewed every three years. Where necessary, the review will be more frequent to ensure compliance with current legislation.

Legal Considerations and Relationship with Other Policies

This policy should be read in conjunction with other College policies, in particular (this is not an exhaustive list):

- Safeguarding & Child Protection Policy
- Student Code of Conduct
- E-safety Policy
- Information Security Policy
- Social Media Policy

Legal Considerations and Relationship with Other Policies

This policy should be read in conjunction with other College policies, in particular (this is not an exhaustive list):

- Safeguarding & Child Protection Policy
- Student Code of Conduct
- E-safety Policy
- Information Security Policy
- Social Media Policy
- IT Data retention Policy
- Privacy Notice for Governors

Sharing Information externally

- Please ensure you only share relevant information for a fixed time period then remove the sharing rights.
- Ensure you have the authority to share the information to the external party before sharing.
- External sharing can be monitored.

Data Retention

The College has an IT Data Retention Policy which can be found on the College intranet (IT & Network area).