Computer, E-mail, Internet & Intranet Policy

Document History			
Author	Andy Barton	**Ref and Document Version**	Computer E-mail Internet & Intranet Policy V10_AB26092025
Reviewed by	Andy Barton	**Reviewed Date**	26/09/2025
Approval	Board of Trustees	**Approval Date**	06/10/2025
Next Review Date	29/09/2028	Policy Number	PRJ-03
Publication	Reception; College website R:/Policies/ComputerE-mailInternetandIntranetPolicy.pdf		

PRJ-03

Introduction

Greenbank provides access to its systems, the internet, e-mail, and intranet services to facilitate and improve the performance of the organisation. This assists individual members of staff to carry out their duties, students to carry out their studies, and clients to have an added-value free wi-fi with internet service wherever they are in the buildings of the organisation.

Information

There is a vast amount of information on the internet and much of this is not related to the work or activities of the organisation. In order to protect Greenbank's reputation, and to ensure that individuals do not abuse the facilities provided, there are certain standards that all staff, students, and clients are expected to adhere to when using its computers.

You must read and familiarise yourself with the contents of this Policy, then sign this document below (or tick the online agreement in the case of the guest free wi-fi network) before Greenbank will allow you to use its computers, the internet, intranet, e-mail, or any services on, or through, its guest or main organisational network. The ticking of any ICT E-mail and Internet (or Electronic Systems) use box on the student Induction Checklist enrolment form, and the signing of that form, is also advising Greenbank that you have read and understood the conditions in this Policy. Users of the free guest wi-fi offered by Greenbank must tick the online box to confirm that they agree with the conditions in this Policy and accept the terms of use to be able to use the service.

Requirements

Users of all of Greenbank's computer and electronic systems should behave responsibly. Examples of the type of behaviour that Greenbank considers as misuse or abuse of our systems include:

1. Accessing or downloading of pornography (whether or not it is legal under UK law).
2. Accessing or downloading from sites which contain information, or access to materials, illegal under UK law.
3. Circulation of chain or 'joke' e-mails (including virus warnings - see below)
4. Posting messages in newsgroups, on message boards, in chat rooms, or on any social media which creates a negative impression of, or tarnishes the reputation of, Greenbank. (Also see Social Media Policy).
5. Excessive use of the internet to visit non-work/study-related sites (including web e-mail)
6. Loading (or the attempt to load) unlicensed or unauthorised software onto the organisation's computer systems.
7. Downloading or loading any software, updates, codes, or scripts, onto any of the organisations computer systems - unless completed by a member of Greenbank's Technical Support department, or an authorised qualified contractor approved by the Network Administrator.

8. Introducing viruses into the organisation's computer systems, or any external systems (including a failure to run virus checking software on files received from an external source).
9. Accepting any online terms and conditions on behalf of Greenbank unless authorised to do so.
10. Using the organisation's computer systems to send or forward fraudulent, abusive, obscene, libellous, or derogatory e-mails or messages, or the posting of any such messages on intranet discussion forums or any social media. (See also Social Media Policy).
11. Access, or attempted access, to modify or delete, any files, folders, intranet documents, or systems on Greenbank's network, which are not part of normal work duties or studies.
12. Uploading any unsuitable or inappropriate material to the Greenbank intranet or website, or any other website.
13. The moving of any computer equipment or peripherals without approval from the Network Administrator or ICT Technician (excluding the moving of laptop computers during the course of normal business activities by staff only).
14. Connecting any computer equipment, wireless device, wi-fi jamming device, keylogger, snooping device, USB memory stick, SD or SDHC etc. card, Hard Disk Drive (including Solid State Drives), or any other peripheral, to any of Greenbank's computer systems without approval from the Network Administrator.
15. Attempting to circumvent Greenbank's safety and security systems, including webfiltering
16. Accessing Greenbank's Server Room, either by forced access or by use of a key, without the approval of the Network Administrator or ICT Technician. All access to the server room be supervised by Technical Support staff approved by the Network Administrator. Exceptions to this rule include authorised master key-holders when every attempt to locate the Network Administrator or ICT Technician has failed. In this case, the authorised key-holder must remain with any visitor/contractor, who has a genuine need to access the server room, to be able to supervise the work required. This cannot be any work on computer network systems.
17. All files containing user-identifiable data need to be approved by SMT or the Network Administrator before being sent externally from the organisation. The exception to this if data is transferred as a regular AND normal part of a staff members job. All such files must be encrypted (zipped with a password).
18. If you have been granted Remote Access to Greenbank's systems as part of your work, you must ensure that the remote computer being used is either issued by Greenbank or is secure enough to be used when connected to Greenbank's central system. This includes up to date reputable anti-virus and firewall software; a fully updated current operating system; and the keeping of that computer safe from use by others when connected remotely. Remote computers must be locked when not being used to avoid usage by others, otherwise this increases the risk to Greenbank's systems and data. The remote user is responsible for all data interactions with Greenbank's systems whilst they are logged in.
19. Any requests for a staff member to access another staff email account and/or staff IT system/drive/account must be put in writing to the CEO with the reason why the request is being made. These requests, if agreed, would be submitted to the Network Administrator via the CEO's office.
20. All Greenbank-issued laptops issued to staff or students, must be returned to Greenbank Technical Support department prior to going on a week or more's Annual Leave, or holiday.

21. Greenbank reserves the right to charge staff, or students/parents/guardians, if any laptops in their custody are lost or stolen.
22. All equipment loaned to staff or students by the Greenbank charity, whether signed for or not, is the responsibility of the person the equipment was initially loaned to. Staff or students cannot transfer the loan – the equipment must be returned to Technical Support, or the Network Administrator must approve the change of loan responsibility. Details are recorded by the Network Administrator - this is the master list to determine absolute responsibility for issued equipment. If you do pass equipment to someone else without approval, you are still responsible for it.
23. All equipment loaned to staff or students must be returned as follows:
    - Staff. Prior to exit interview, or 13th day of the last working month, whichever comes first. Failure to comply would result in a deduction from final salary for equipment not returned.
    - Students. Before the last day of attendance at Greenbank.

    Failure to return equipment gives Greenbank the right to charge for value of the missing items.

This list is not exhaustive. Any of these actions, or any other action, which may damage either Greenbank's ICT systems, or the reputation or image of Greenbank, may result in disciplinary and/or legal action being taken against the employee or student. Additionally, if illegal, such activities would be reported to the police.

Greenbank can monitor the use of its e-mail, internet activity, files and folders access, and reserves the right to do this to ensure that the above rules are not being broken, and to protect both its systems and its reputation.

Greenbank's Network Administrator and ICT Technician are the only people authorised to issue virus warnings or circulate any other IT-related warnings. In exceptional circumstances members of the SMT can issue such warnings after taking advice from the Network Administrator, if reasonably possible. If you believe that your PC, or the network, has been infected: staff must contact the Network Administrator or ICT Technician immediately; students should make contact via their tutor; clients should report the matter to any member of staff, who should then report the matter to the Network Administrator or ICT Technician.

Author: Andy Barton Document Version: V10_AB26092025

Agreed by Greenbank Board of Trustees

Dr Alan Irving, Chairman

Computer, E-mail, Internet & Intranet Policy

I confirm that I have read and understood the latest Computer, E-mail, Internet & Intranet Policy.
Document Version: V10_AB24092025

I confirm that I will also abide by Greenbank's Social Media Policy

Please tick box: ☐ Staff Member ☐ Student

PRINT NAME …….. DEPARTMENT ……..……

SIGNED …….. DATE ……..