DOCUMENT DETAILS

Document Name:	Nottingham College ICT Acceptable Use Policy
Document reference	IT/COP/180718
Version	0.2
Issue Date:	July 19
Review Date:	July 2020
Document Author	Drew Keavey
Document Owner	Jo Clifford
Applicability	All staff, volunteers and Governors of Nottingham College, all other parties under contract.
Summary	The purpose of this document is to set out the policy for the acceptable use of College ICT equipment, infrastructure and services

DOCUMENT CONTROL

Version history			
Version	Date	Reason for release/version update	Issued by
0.1	27/04/2018	First draft	Drew Keavey
0.2	14/06/2018	Updates from feedback	Drew Keavey
0.2	05/07/2019	Reviewed & no updates required	Drew Keavey

DOCUMENT APPROVAL

Approving person/body	Job Role (where applicable)	Date Approved
Governing Body		18/07/18
Governing Body		22/07/19

COMMUNICATION

Date sent to OLT	30/07/19
Date sent to Internal Comms	30/07/19
Publication required on External Website?	NO

CONTENTS

1. INTRODUCTION

Nottingham College provides access to a range of ICT equipment, infrastructure, systems and services to students, staff and other stakeholders. This policy defines what is and is not acceptable use of these.

2. OBJECTIVE

This acceptable use policy for ICT equipment, infrastructure, systems and services is designed to protect the College and its employees, students and other partners from harm caused by the misuse of our IT Systems and data. Misuse can include both deliberate acts and inadvertent actions. The repercussions of misuse have the potential to be severe and can cause financial, operation and reputational damage. Examples of potential damage include, but are not limited to, introduction of computer viruses or other malware, legal, financial and reputational damage for loss of data and lost productivity and teaching time due to network downtime.

Everyone who works for the College is responsible for the security of our IT systems and the data on them. As such all employees must ensure they adhere to the guidelines in this policy at all times. Should any employee be unclear on the policy or how it affects their role they should speak to their Line Manager or contact the ICT Services Helpdesk.

All new starters and contractors should be issued with the one page summary of the policy as part of their induction. Logging onto to the College system will require acceptance of this policy.

3. POLICY STATEMENT

3.1. Use of College ICT systems including email and the internet is intended primarily for work related purposes.

3.2. The College has the right to monitor any and all aspects of its computer systems and to monitor, intercept and/or record any communications made by employees, including telephone, email or internet communications. To ensure compliance with this policy or for any other purpose under the Telecommunications (Lawful Business Practice)(Interception of Communications)Regulations 2000 the College will take all reasonable steps to ensure that staff are aware of this right to monitor. Provision of user accounts is subject to acceptance of the terms of the acceptable use policy.

3.3. Computers and email accounts are property of the College and are designed to assist in the performance of your work. You should therefore have no expectation of privacy in any email sent or received, irrespective of whether it is of a business or personal nature.

3.4. It is inappropriate use of email and the internet for employees to access, download or transmit any material which might reasonably be considered to be obscene, abusive, sexist, racist or defamatory. You should be aware that such material may also be contained in jokes sent by email. Such misuse of electronic systems will be considered misconduct and will, in certain circumstances, be treated by the College as gross misconduct. The College reserves the right to use the content of any employee email stored in the College systems in the disciplinary process.

3.5. Users of the College's electronic discussion fora are expected to conduct themselves in a professional manner; respecting College values. Participants should therefore not

express opinions that are inappropriate as described in 1.4 above, nor should they seek to harass or demean another colleague for expressing their views. Forum postings that do not meet these standards will be removed from College systems.

3.6. The Acceptable Use Policy applies to all College devices capable of accessing electronic systems, including but not limited to; desktop and laptop computers, mobile phones, iPad and other tablet devices, e-readers, games consoles and voice over IP telephones.

Use of email

3.7. A guidance document for the effective use of email can be found on the College intranet.

3.8. Emails should be drafted with care. Despite their sometimes informal style, emails are a permanent form of written communication. It is also worth noting that material can be recovered even when it is deleted from your computer.

3.9. Employees should not make derogatory or defamatory remarks in emails about fellow employees, students, competitors or any other person. Any such remarks may constitute libel.

3.10. Employees should not send or receive any material that is obscene or defamatory or which is intended to annoy, harass or intimidate another person.

3.11. Employees should not facilitate the spread of unsolicited email, in particular they should not respond to "chain letter" style emails that request that a message is forwarded to multiple recipients. This extends to emails purporting to give details of new viruses or "scams". If any user receives such an email and has concerns they should forward it to the ICT Helpdesk who can check the authenticity of the claims.

3.12. As outlined in the College financial regulations, no member of staff shall authorise work to be undertaken or goods to be supplied which are subject to contract without approval from the Principal or his/her nominee. As outlined in 4.8 above email constitutes written communication and therefore care must be taken not to make contractual arrangements as these may be binding.

3.13. Sending email does not guarantee delivery. Delivery receipts do not guarantee that a message has been read. If an email is important, consider asking the recipient to confirm by replying.

3.14. Reasonable private use of email is permitted but should not interfere with your work. The contents of personal emails must comply with the restrictions set out in the acceptable use policy. 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.

3.15. All emails sent and received by the College system are passed through a third party virus scanning process and therefore considered safe to open. The College does not sanction the use of web based email (other than the College system and College supported systems, such as Office 365) and email received to these systems may not be virus free.

3.16. All emails received by the College are filtered in attempt to remove unsolicited commercial email ("Spam") and phishing attempts to retrieve personal data. Such systems are not fool-proof however and individuals should take care when assessing the

validity of emails asking for information. More guidance can be sought from the ICT Services helpdesk.

Use of the Internet

3.17. Reasonable private use of the internet is permitted but should be kept to a minimum and should not interfere with your work. Excessive private access to the internet during working hours may lead to disciplinary action and may in certain circumstances be treated by the College as gross misconduct.

3.18. The sites accessed by you must comply with the restrictions set out in the acceptable use policy and associated guidelines. Accessing inappropriate sites may lead to disciplinary action and may in certain circumstances be treated by the College as gross misconduct. Any access or attempted access to sites deemed to be in breach of the law will be reported to the appropriate authorities.

3.19. College devices utilising mobile data networks (3G/4G) such as mobile phones, laptops with mobile data capabilities and tablets have limited allocations of data and additional data costs are high so personal use of these devices for internet use should be for exceptional circumstances only.

Copyright and downloading

3.20. Copyright applies to all text, pictures, video and sound, including those sent by email or on the internet unless specifically stated otherwise. Files containing 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 as appropriate.

3.21. Copyrighted software must never be downloaded unless written agreements are in place and registered with the ICT Helpdesk.

3.22. No software should be installed or run on your PC except that authorised by ICT Services.

General Usage

3.23. You are responsible for safeguarding your password for the system. For reasons of security your password should not be printed or given to others. User password rights given to employees should not give rise to an expectation of privacy.

3.24. You are responsible for activities tied to your network account and should not therefore allow another user to use your account except for authorised members of the ICT Services Team for the purposes of troubleshooting and resolution of faults. If you are away from your workstation you should ensure that it is locked. At the end of the working day you should normally log off. If you have cause to believe that your account has been used by someone else please contact the ICT Helpdesk immediately.

3.25. Your ability to connect to other computer systems through the network does not imply a right to connect to those systems or to make use of those systems unless authorised to do so. You should not alter or copy a file belonging to another user without

first obtaining permission from the creator of the file. The College provides shared file storage on SharePoint, OneDrive and the network file shares to allow documents to be collectively altered.

3.26. College data is subject to the GDPR and associated Data Protection Act and where it is necessary to move data out of the college infrastructure the data should be stored in an encrypted format. The ICT Helpdesk can advise on suitable means of securing data.

Monitoring

3.27. All internet accesses are logged and contain the username, website location, time and date. These logs are stored and reports are routinely generated to review bandwidth usage and check security issues.

3.28. In addition to the routine reporting, individual managers may, at their discretion, ask for a report on the usage of some or all of their staff.

3.29. The content of email communications are not routinely monitored by members of the ICT Services team. However, the College reserves the right to monitor email communications to support operational, maintenance, auditing, security and investigative activities.

3.30. The content of email communications are routinely monitored by automated systems to minimise the possibilities of data loss and these systems may automatically alert college ICT services staff to potential breaches of policy.

3.31. Telephone communications are not routinely monitored. However, the College reserves the right to do so to support investigative activities. The College has no capability to record telephone communications at a system level for general handsets however certain systems may have such features to record conversations for staff protection and training purposes – such systems will incorporate a notice to inform both parties of such recording.

4. REFERENCES

Policy Connections

College policies and guidelines which should be reviewed in conjunction with this Policy include:

- Social Media Guidelines
- Data Protection/General Data Protection Regulation Policy
- Network Security Policy
- Freedom of Information Policy
- Information Security Policy
- E-safety Policy

All use of College ICT equipment is subject to the relevant UK legislation, including but not limited to;

- Copyright, Designs and Patents Act 1988. The unauthorised copying or use of software is illegal. Anyone infringing copyright may be liable to a personal fine of up to £2,000 and up to 6 months imprisonment.
- Malicious Communications Act 1988. Under this Act sending indecent, grossly offensive or threatening messages is an offence.
- Computer Misuse Act 1990. Under this Act unauthorised access or modification of computer systems became criminal offences. There are three types of offences under this Act
    - Unauthorised use of a computer or data, with a penalty of up to 6 months imprisonment and a £2,000 fine.
    - Unauthorised access with ulterior intent, with a penalty of up to 5 years imprisonment and an unlimited fine.
    - Unauthorised modification of data, with a penalty of up to 5 years imprisonment and an unlimited fine.
- Criminal Justice and Public Order Act 1994. This extends the provision of the Obscene Publications Act 1959 and Protection of Children Act 1978 to cover storage and transmission of material by electronic means.
- Protection from Harassment Act 1997. Protects from so called “Cyberstalking”.
- Data Protection Act 2018. Further information can be found in the College Data Protection policy which is available on the intranet.

If any suspected breach of the law is brought to the attention of the College it will cooperate fully with the relevant authorities to facilitate a thorough investigation.

In addition to the terms and conditions contained within the College Acceptable Use Policy users are also bound by the JANET Acceptable Use Policy. A copy of this policy can be found on the Janet website.

APPENDIX 1:

Computer Network Acceptable Use Policy – Staff Summary

General Principles

- College provided internet, intranet and email services are considered College resources and as such usage may be monitored for unusual activity.
- Correspondence via email cannot be guaranteed to be private. Any confidential email should be sent using encryption techniques sanctioned by the College.
- Use of internet, intranet, email and SMS services will be subject to monitoring for security and/or network management reasons. Users may also be subject to limitations on their use of such resources.
- The distribution of any information through the internet, computer based services, email and messaging systems is subject to scrutiny. The College reserves the right to determine the suitability of this information.
- Reasonable personal use of the internet and email services is permitted but is subject to the terms laid out below and the operational requirements of the College.

Conditions of Use: Users shall not:

- Visit or attempt to visit internet sites that contain obscene, hateful or other objectionable materials; send or receive by electronic means material that is obscene or defamatory or which is intended to annoy, harass or intimidate another person.
- Use College facilities to solicit non-College business for personal gain or profit.
- Use the internet, email, telephone system or SMS service for any illegal purpose.
- Represent opinions as those of the College without express consent.
- Make or post indecent remarks, proposals or materials.
- Upload, download or otherwise transmit commercial software or any copyrighted materials belonging either to parties outside of the College or to the College itself.
- Install or run any unauthorised software on College equipment.
- Download any software or electronic files without implementing virus protection measures that have been approved by the College.
- Intentionally interfere with the normal operation of the network, including, but not limited to, propagation of computer viruses and sustained high volume network traffic which substantially hinders other users in their use of the network.
- Use Internet, email, telephone or SMS services for inappropriate personal use that is not connected with College business.
- Reveal or publicise confidential or proprietary information which in includes, but is not limited to : financial information, new business ideas, marketing strategies and plans, databases and information contained therein, student enrolment details and business relationships.
- Examine, change or use another users' files, output or user name for which they do not have explicit authorisation.
- Reveal individual passwords, either account logon or system specific, to anyone else.
- Resell any service provided by the College, including but not limited to email, network storage and internet access.
- Perform any other inappropriate uses identified by the Head of IT.

Members of staff who violate any of the guidelines set in the policy may be subject to disciplinary action. The College also retains the right to report any suspected illegal activities to the appropriate authorities. Further guidance can be found in the full IT Acceptable Use Policy document. If there are any queries relating to this document please contact the Head of IT.

APPENDIX 2:

Computer Network Acceptable Use Policy – Student Summary

General Principles

- College provided internet, intranet and email services are considered College resources and as such usage may be monitored for unusual activity.
- Correspondence via email cannot be guaranteed to be private.
- Use of internet, intranet and email will be subject to monitoring for security and/or network management reasons. Users may also be subject to limitations on their use of such resources.
- The distribution of any information through the internet, computer based services, email and messaging systems is subject to scrutiny. The College reserves the right to determine the suitability of this information.
- Reasonable personal use of the internet and email services is permitted but is subject to the terms laid out below and the operational requirements of the College.

Conditions of Use: Users shall not:

- Visit or attempt to visit internet sites that contain obscene, hateful or other objectionable materials; send or receive by electronic means material that is obscene or defamatory or which is intended to annoy, harass or intimidate another person.
- Use the internet, email, telephone systems or other College systems for any illegal purpose.
- Represent opinions as those of the College without express consent.
- Make or post indecent remarks, proposals or materials.
- Upload, download or otherwise transmit commercial software or any copyrighted materials belonging either to parties outside of the College or to the College itself.
- Install or run any unauthorised software on College equipment.
- Download any software or electronic files without implementing virus protection measures that have been approved by the College.
- Intentionally interfere with the normal operation of the network, including, but not limited to, propagation of computer viruses and sustained high volume network traffic which substantially hinders other users in their use of the network.
- Use Internet, email or telephone services for inappropriate personal use that is not connected with teaching and learning.
- Examine, change or use another users' files, output or user name for which they do not have explicit authorisation.
- Reveal individual passwords, either account logon or system specific, to anyone else.
- Resell any service provided by the College, including but not limited to email, network storage and internet access.
- Perform any other inappropriate uses identified by the Head of IT.

Students who violate any of the guidelines set in the policy may be subject to disciplinary action. The College also retains the right to report any suspected illegal activities to the appropriate authorities. Further guidance can be found in the full IT Acceptable Use Policy document. If there are any queries relating to this document please contact the Head of IT.