SOUTH LEICESTERSHIRE COLLEGE

North Warwickshire & Hinckley College

Part of North Warwickshire and South Leicestershire College

ICT/ILT Acceptable Use Policy 2015

Last amendment: 9th Jan 2015.

Contents

CONTEXT

Important Note: North Warwickshire and Hinckley College may revise this ICT/ILT Acceptable Use Procedure without notice by posting the latest version of this document on the North Warwickshire and Hinckley College network system (oneCollege/Extranet/Moodle) and Web site at http://www.nwhc.ac.uk . Accordingly, users of North Warwickshire and Hinckley College Services should consult this document regularly to ensure that their activities conform to the most recent version. In the event of a conflict between any user agreement, the College IT Security Policy and this policy, the terms of these policy and procedures will govern. Questions regarding the IT Security Policy and these procedures and/or complaints of violations of this policy by College users, can be directed to the Group Director E-Services.

This policy should be read in conjunction with the following College policies:

- IT Security Policy
- Social Media – Staff Use Policy
- Procedures relating to misconduct
- Data Protection Policy
- Safeguarding Policy

All the above policies and codes may be found on the College Website and/or college extranet.

1. INTRODUCTION

1.1 North Warwickshire and Hinckley College provides a variety of Internet Services to College users. Use of The Services is subject to the following rules and guidelines. Each learner/ employee/client / stakeholders of North Warwickshire and Hinckley College is responsible for ensuring that the use of all Services provided to such customers complies with the College IT Security Policy and this Acceptable Use Policy document.

ANY USER WHO DOES NOT AGREE TO BE BOUND BY THESE TERMS SHOULD IMMEDIATELY CEASE USING THE SERVICE AND NOTIFY NORTH WARWICKSHIRE AND HINCKLEY COLLEGE E-SERVICES TEAM SO THAT THE USER'S ACCOUNT MAY BE CLOSED.

2. AUTHORISED USE

2.1 Use of College IT/ICT facilities, and their use to access non-College IT facilities, must be for the purpose of research, teaching, training, coursework, associated administration or other authorised use. No 'private/commercial' work is permitted without prior written authorisation from the Principal / Chief Executive. Failure to gain written authorisation to

carry out private/commercial work could lead to disciplinary action. In certain circumstances, the College may offer services to private individuals, which will be charged at the normal fee for such work.

2.2 College IT/ICT facilities include the network, Virtual Learning Environment (VLE) , libraries and learning resource centres, assessment centres, IT workshops, classrooms, computers, printers and the associated services e.g. software, data, email, Web, Ejournals, bulletin boards, cloud services and databases, but do not exclude any other part of the College IT facilities.

2.3 Occasional personal use of the desk top computer, e-mail and web access is permitted provided such use does not disrupt the conduct of College business or other Users.

2.4 Authorisation to use the Services is withdrawn on termination of a staff members' employment contract or on a student ceasing to study at the college.

3. ILLEGAL ACTIVITY

3.1 The use of the Services for any activity that violates any local, regional, and national or international law, order or regulation is a violation of this group of procedures and the College IT Security Policy.

Prohibited activities include, but are not limited to:

3.1.1 Posting or disseminating material, which is unlawful (such as child pornography or obscene material).

3.1.2 Disseminating material, which infringes the confidentiality, copyright or other intellectual property rights of others, (in respect of confidentiality, you assume all risks regarding the determination of whether material is in the public domain).

3.1.3 Pyramid or other illegal soliciting schemes.

3.1.4 Any fraudulent activities, including impersonating any person or entity or forging anyone else's digital or manual signature.

3.1.5 Transmitting or downloading to view words or pictures which are libellous, insulting or abusive could be construed as being libellous because they are capable of harming an individual's or the College's reputation.

3.1.6 Transmitting or downloading material which could amount to harassment of the recipient or any other individual (be that harassment sexual, religious or otherwise)

3.1.7 Unreasonable personal use of the College's ICT/ILT facilities.

3.1.8 Posting or the dissemination of material which has the potential to draw people into terrorism or extremist behaviour in accordance with the College's Prevent Duty.

3.2 When using College IT facilities the user must comply with the College Information Technology Security Policy and all relevant statutory and other provisions, regulations, rules, procedures and codes of practice.

3.2.1 Specifically, but not exclusively, the **User must not**:

3.2.2 use or produce materials or resources to facilitate unauthorised corruption, changes, malfunction or access to any IT facilities at the College or elsewhere.

3.2.3 Attempt access to IT facilities includes scanning activities (e.g. port scanning).

3.2.4 display, store, receive or transmit images or text which could be considered offensive e.g. material of a sexual, pornographic, paedophilic, sexist, racist, libellous, threatening, defamatory, of a terrorist or extremist nature or likely to bring the College into disrepute.

3.2.5 forge email signatures and/ or headers, initiate and/or forward 'chain' or 'junk' or 'harassing' email. 3.2.6 play unauthorised games.

3.3 Abide by copyright laws of all material and software made available by the College and third parties and not use, download, copy, store or supply copyright materials including software and retrieved data other than with the permission of the Copyright holder or under the terms of the license held by the College.

4. SECURITY

4.1.1 Users should:

4.1.2 note that the Internet is not secure and information on e-mail sent across the internet may be intercepted and read by unknown third parties;

4.1.3 Not disclose to others her/his College login name/password combination(s) or access or attempt to access IT facilities at College or elsewhere for which permission has not been granted or facilitate such unauthorised access by others.

4.2 The User is responsible for any misuse of the Services that you are using, even if the inappropriate activity was committed by a friend, family member, guest, employee or customer with access to your account. Therefore, you must take steps to ensure that others do not gain unauthorised access to the Services.

4.3 The Services may not be used to breach the security of another user or to attempt to gain access to any other person's computer, software or data, without the knowledge and consent of such person. They also may not be used in any attempt to circumvent the user authentication or security of any host, network, or account. This includes, but is not limited to, accessing data not intended for you,

logging into or making use of a server or account you are not expressly authorised to access, or probing the security of other networks.

4.4 Use or distribution of tools designed for compromising security, such as password “hacking” programs, cracking tools, packet sniffers or network probing tools, is prohibited. The Services may not be used to collect, or attempt to collect, personal information about third parties without their knowledge or consent.

4.5 You may not disrupt the Services. The Services also may not be used to interfere with computer networking or telecommunications Services to any user, host or network, including, without limitation, denial of service attacks, flooding of a network, overloading a service, improper seizing and abuse of operator privileges and attempts to "crash" a host.

4.6 The transmission or dissemination of any information or software that contains a virus or other harmful feature also is prohibited. The Services may not be used to violate the rules, regulations, or policies applicable to any network, server, computer database, or web site that the Customer accesses. You are solely responsible for the security of any device you choose to connect to the Services, including any data stored on that device.

4.7 The College recommends that any files or Services you do choose to make available for remote access be protected with a strong password or as otherwise appropriate.

4.8 When holding data about living individuals, covered by the College Data Protection Policy, register that data and its uses, and treat it in accordance with the principles, as required by the Data Protection Act. Users must not construct or maintain computer files of personal data for use in connection with their academic studies/research without the express authority of the College Data Protection Officer (CDPO).

4.9.1 When responsible for Information Servers or the information held thereon abide by the College Code of Practice for Information Servers and be aware that a User may be considered in law to be a Publisher in certain circumstances.

4.10 When leaving workstations unattended:

4.10.1 Users are solely responsible for their access onto the college infrastructure. If a user leaves their workstation for any period of time, they do so at their own risk.

4.10.2 Users should NEVER leave workstations logged on to the network unattended, and should adhere to the following guidelines:

4.10.3 It is mandatory to log off or, at least, 'Lock Workstation' or 'Lock Computer' when leaving a workstation unattended - even for a few minutes.

(NB - to achieve this the User should press windows key plus "L" to lock the workstation. The User must log in again to unlock the workstation.)

4.10.4 Learner User Accounts are terminated at the end of each academic year. In addition, learner accounts will be terminated when the individual successfully completes a programme of study, is withdrawn from a programme or suspended, pending a disciplinary procedure or when EServices are notified in any other circumstances. The Group Manager EServices is responsible for setting up and terminating learner accounts using appropriate systems.

4.10.5 Staff User Accounts are terminated when the individual ceases employment with the College, is subject to a disciplinary procedure as outlined in the "Procedures relating to Misconduct" or other legal action. The Human Resources department provides the E-Services department with lists of staff leavers on a regular basis. The Group Manager EServices implements the termination of access rights and removal of access codes as soon as possible, upon receipt of this information.

4.11 If a User has sufficient reason to believe that their security details have been compromised, they must report it immediately to the College's EServices department so that the account can be disabled until further notice. Failure to inform E-Services will result in the user being responsible for any activity occurring on the account.

5. INAPPROPRIATE CONTENT

5.1 There may be content on the Internet or otherwise available through the Services which may be offensive to some individuals, or which may not be in compliance with all laws, regulations and other rules. For example, it may be possible to obtain access to content, which is pornographic or offensive. North Warwickshire and Hinckley College cannot assume any responsibility for the content contained on the Internet or otherwise available through the Services. You must assume the risk of accessing content through the service, and except as prohibited by law, North Warwickshire and Hinckley College shall not have any liability for any claims, losses, actions, damages, suits or proceedings arising out of or otherwise relating to access to such content. Content questions or complaints should be addressed to the content provider.

5.2 Other than any statutory obligation, the College will not be liable for any loss, damage or inconvenience arising directly or indirectly from the use of, or prevention of use of, any IT facility provide and/or managed by the College.

5.3 Whilst the College takes appropriate security measures against unauthorised access to, alteration, disclosure, destruction or accidental loss of personal and other data it cannot and does not give any warranties or undertakings to the USER about security, confidentiality or integrity of data, personal or other. The same applies to other IT material submitted to or processed on facilities provided or managed by the College or otherwise deposited at or left on its premises.

5.4 North Warwickshire and Hinckley College reserve the right to refuse to post or to remove any information or materials, in whole or in part, that it, in its sole discretion, deems to be offensive, indecent, or otherwise inappropriate regardless of whether such material or its dissemination is unlawful. North Warwickshire and Hinckley College has no obligation to monitor transmissions made on the Services. However, North Warwickshire and Hinckley College has the right to monitor such transmissions and to disclose the same in accordance with its service agreement.

5.5 By using the Services to reproduce, publish, display, transmit and distribute content, a user is warranting that any content that the user may reproduce, publish, display, transmit, or distribute complies with this Policy. Through these actions, a user also authorises North Warwickshire and Hinckley College and its partners to reproduce, publish, display, transmit and distribute such content as necessary for the College to deliver the content in a timely manner.

5.6 All data/programmes created/owned/stored by the user on or connected to College IT facilities may, in the instance of suspected wrong doing, be subjected to inspection by college or by statutory authorities. Should the data/programs be encrypted the User shall be required to provide the decryption key to facilitate decryption of the data/programs.

6. OBSCENITY

6.1 The following issues require consideration: -

6.1.1 It is a criminal offence to publish or distribute obscene material; “publish or distribute” includes processing (including simply viewing the material), showing or distributing indecent photographs of a child or children (including computer generated photographs);

6.1.2 In accordance with the requirements under the Precent Duty the College does use a filtering mechanism as a means of restricting access to harmful content. Where the College becomes aware of a student or staff member accessing such content we may refer the matter to the Safeguarding Team.

6.1.3 It is an offence to display indecent material in public. The Internet and Intranet are public places.

6.1.4 Users must not view, copy, store or download any obscene material or send it using the College's computer systems.

7. DISCRIMINATION AND HARASSMENT

7.1 Users are reminded that they must comply with the College's policies and procedures relating to discrimination and harassment and that these policies and procedures extend to any information distributed on the College's computer systems or via the Internet; and

7.2 Users may not send e-mail containing, or otherwise put on the College's computer system, or on the Internet, any material which discriminates or encourages discrimination or harassment on race, racial or ethnic grounds or on grounds of gender, sexual orientation, marital status, age, ethnic origin, nationality, religion or disability. (Refer to College Single Equality Scheme Policy on www.nwhc.ac.uk)

8. ELECTRONIC MAIL

8.1 The Services may not be used to send unsolicited bulk or spam messages. This includes, but is not limited to, bulk mailing of non-college commercial advertising, informational announcements, charity requests, petitions for signatures, and political or religious messages. Such messages may only be sent to those who have explicitly requested it. The Services may not be used to send messages to any individual who has indicated that he/she does not wish to receive messages from you.

8.2 The Services may not be used to collect responses from unsolicited email sent from accounts on other Internet hosts or email Services which violates this Policy or the acceptable use policy of any other Internet service provider. Moreover, unsolicited email may not direct the recipient to any web site or other resource that uses the Services. Activities that have the effect of facilitating unsolicited commercial email or unsolicited bulk email whether or not that email is commercial in nature are prohibited.

8.3 "Mail bombing or spamming" is prohibited. That is, you may not send numerous copies of the same or substantially similar messages, nor may you send very large messages or files to a recipient with the intent to disrupt a server or account. The propagation of chain letters is similarly prohibited, whether or not the recipient wishes to receive such mailings.

8.4 The College is not responsible for the forwarding of email (or content) to an external provider or sent to any account that has been suspended or terminated.

Such email will be returned to the sender, ignored, deleted, or stored temporarily at the College's sole discretion.

8.5 In respect of viruses, users should note:

8.5.1 That in case of any queries or doubt the E-Services department should be contacted immediately;

8.5.2 the exchange of executable files using internet e-mail may expose the College's systems to the risk of viruses;

8.5.3 unsolicited attachments should be discarded unless there is good reason not to discard them;

8.5.4 Downloading new software from the Internet and opening the following electronic files. .exe, .com, .dll, .bat files is prohibited without prior consultation with and authorisation from E-Services.

9. BULLETIN BOARD/ VIRTUAL LEARNING ENVIRONMENT (VLE) / SOCIAL NETWORKING SITES/INTERNET CHAT AND OFFICE COMMUNICATOR

9.1 The Services may be used by staff to participate in controlled "chat" discussions through Office Communicator or similar **approved** facilities. These discussions are hosted by NWHC and are for staff use only. Students will not have access to any internet chat facilities outside of the VLE unless explicitly authorised by the College. The College network does not normally monitor the contents of the discussion and is not liable for the contents of any communications made via Bulletin Boards or Internet chat. An internal log of all staff messenger communications and / or Microsoft Office Communicator discussions will be kept and made available to the executive as a point of reference for any matters which may arise including, but not restricted to, accounts of harassment, libel or inappropriate material.

(Please refer to sections 3 and 5 and 9.9 of this policy)

9.1.1 The use of social networking sites (including, but not limited to MeeBo, Bebo, Facebook, mySpace) is prohibited on college equipment unless expressly authorised. Staff who wish to create/use/maintain such social internet sites for teaching & learning, marketing or other potential uses, should seek permission and be aware they are bound by the Social Media Staff Use Policy (available on the extranet). The public wi-fi provided by the college, allows use of such sites by staff and students **on their own personal equipment**, within the overall parameters provided within this document. Staff connecting to the public wi-fi system (as opposed to the Staff Wi-Fi facility) using College owned equipment may be deemed to be in breach of this policy.

9.2 The Services may not be used for personal internet chat sessions, to perform personal chat "flooding." Flooding is defined as deliberately repeating actions in quick succession in order to fill the screens of other Internet users with text.

9.3 The Services may not be used to send messages which disrupt another Internet user's equipment, including software, hardware, and user display.

9.4 The Services may not be used to access any chat server in violation of the acceptable use policy of that server. The Services may not be used to manipulate any chat server in order to harass or disconnect other Internet users, or to gain privileges, which have not been authorised.

9.5 A customer may not use the Services to connect to chat servers or channels from which they have been previously banned, or which are on the College banned list.

9.6 The Services may not be used to continue to send chat messages to an Internet user who has indicated their desire to not receive such messages.

9.7 Forging, altering, or obscuring your identity (other than using a nickname from which The College could if necessary determine your real name) while participating in chat sessions is forbidden.

9.8 The use of, and any attempts to, bypass the College web-filtering systems, through anonymous proxy sites is explicitly forbidden, and can result in revocation of the users network account.

9.9 A number of systems will log activity by users. This detail will be held securely, and be available only to senior members of E-Services. This data may be used will be kept and made available to the executive or any external agencies (with due consideration of data protection and statutory rights) as a point of reference for any matters which may arise including, but not restricted to, accounts of harassment, libel or inappropriate material.

Entity name	Retention	Detail Level
Exchange Server SMTP Log	6month to txt file.	Connection logs made to service to delivery emails.
Bloxx access logs	Rolling. Estimate 3 Months	Every URL visited by each user
Exchange message tracking	Estimated 360 days	Message delivery statistics
Fortigate Firewall Services	Estimate 1 year	Logs IP & protocol connections for diagnostics.

Fortigate Webproxy Services	Estimate 1 year	Logs web page activity
Cacti	Rolling Est two years	Logs traffic stats on college network.
Webserver/Moodle/VMNA	Rolling Log	Logs usage stats
Login/Logout data	Rolling Log	Used to provide user to hostname resolution for support and security purposes such as who has used what computer and when.

10. BANDWIDTH, DATA STORAGE AND OTHER LIMITATIONS

10.1 You must comply with the then current bandwidth, data storage and other limitations of the Services.

10.2 Users must ensure that their activity does not improperly restrict, inhibit, or degrade any other user's use of the Services, nor represent (in the sole judgement of The College) an unusually large burden on the network itself.

10.3 In addition, users must ensure that their activity does not improperly restrict, inhibit, disrupt, degrade or impede the College's ability to deliver the Services and monitor the Services, backbone, network nodes, and/or other network Services.

10.4 Storage of personal data files that may compromise data storage capacity is not permitted. Examples of prohibited uses include, but are not limited to; personal photographs, games, video and music files. **The College reserves the right to remove any unauthorised copyright material without warning**.

10.5 You may not use the College service for commercial purposes. Examples of prohibited uses include, but are not limited to, running servers for mail, http, ftp, irc, and dhcp, and multi-user interactive forums.

10.6 The College reserves the right to review the volume of stored staff/student data files for teaching, training, learning and administrative functions. The Manager of the E-Services Department will review the capacity of servers to cope with data volume and advise the Group Director E-Servicesappropriately. For the academic year 2011/2012 the quotas are set as 2gb per student account and 15gb for staff accounts.

10.7 The College routinely removes all learner / student data on the servers annually. This takes place at the end of each academic year. Appropriate notice is given to all Users of the network by an on-screen reminder at log in. Users are encouraged to save personal work onto a floppy disk, CD/DVD disc, USB memory stick or other approved means. NB For further info of approved data storage consult the E-Services department.

11. VIOLATION OF IT/ICT ACCEPTABLE USE POLICY

11.1 The College does routinely monitor the activity of all accounts for violation of this Policy and will respond appropriately if we become aware of inappropriate use of our Services and reserve the right to interrogate accounts in certain circumstance, such as suspected violation of these procedures. Although North Warwickshire and Hinckley College has no obligation to monitor the Services and/or the network, North Warwickshire and Hinckley College reserve the right to monitor bandwidth, usage, and content to operate the Services; to identify violations of this Policy; and/or to protect the network and the College users.

11.2 The College prefers to advise customers of inappropriate behaviour and any necessary corrective action. However, if the Services are used in a way, which North Warwickshire and Hinckley College or its partners, in their sole discretion believe violate this Policy, North Warwickshire and Hinckley College or its partners may take any responsive or disciplinary actions, they deem appropriate. Such actions include, but are not limited to, temporary or permanent removal of content, filtering of Internet transmissions, and the immediate suspension or termination of all or any portion of the Services.

11.3 Neither North Warwickshire and Hinckley College, nor its partners, will have any liability for any such responsive actions, except as required by law. The abovedescribed actions are not the College's exclusive remedies and may take any other legal or technical action it deems appropriate.

11.4 As provided by the Telecommunications (Lawful Business Practice), (Interception of Communications) Regulations 2000, made under the Regulation of Investigatory Powers Act 2000 the College will intercept and monitor electronic communications for the purposes permitted under those Regulations in accordance with the Code of Practice on Monitoring Electronic communications in the College Information Systems Security Policy.

11.5 These conditions apply to non-College owned equipment e.g. personal Laptops, home PCs, mobile devices when connected to the College network, directly and/or via the VPN, for the duration that the equipment is using the College network.

Breach of these conditions may lead to College disciplinary procedures being invoked, with penalties, which could include suspension from the use of all College computing facilities for extended periods and/or fines. Serious cases may lead to expulsion or dismissal from the College and may involve civil or criminal action being taken against the User.

Last modified Jan 2015

David Evans – Group Director E-Services.