IT ACCEPTABLE USE POLICY (AUP)

Date approved:	20 April 2016
Approved by:	Executive Board
Responsible Manager:	Chief Information Officer
Group Executive Lead:	Group Director Finance, Estates & IT
Accessible to Customers/Students:	Yes

1. Consultation

- Group Services Yes
- Newcastle College: Yes
- West Lancashire College: Yes
- The Intraining Group: Yes
- Rathbone Training Yes
- Newcastle Sixth Form College Yes
- Kidderminster College Yes

2. Applicability of Policy to Organisation

This policy applies to:-

- Newcastle College: Yes
- West Lancashire College: Yes
- The Intraining Group: Yes
- Group Services Yes
- Rathbone Training Yes
- Newcastle Sixth Form College Yes
- Kidderminster College Yes
- NCG Supply Chain Partners Yes

3. Policy Statement

3.1 NCG's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to NCG's established culture of openness, trust and integrity but to ensure that NCG is operating in line with the Counter Terrorism and Security Act 2015 including schedule 6, the Prevent Duty guidance, the Data Protection Act 1998, the Computer Misuse Act 1990 and any other applicable laws. NCG is committed to protecting NCG's learners/customers, employees, partners and the

Company from illegal or damaging actions by individuals, either knowingly or unknowingly.

4. Scope and Purpose of Policy

4.1 This policy applies to learners/customers, employees, contractors, consultants, temporaries and other workers at NCG, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by NCG.

4.2 The purpose of this policy is to outline the acceptable use of computer equipment at NCG. These rules are in place to protect the employees, learners/customers, outsource partners and NCG. Inappropriate use exposes NCG to risks including virus attacks, compromise of NCG information systems and services and legal issues.

4.3 Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP are the property of NCG. These systems are to be used for business and learning purposes in serving the interests of NCG, and of our learners/customers in the course of normal operations.

4.4 Effective security is a team effort involving the participation and support of every NCG employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

4.5 It is the responsibility of staff carrying out the induction of new staff and /or learners/customers to ensure that the requirements of this policy are communicated in an appropriate manner. In clicking the acceptance page at the point of logging-in users are indicating their agreement to the following guidelines and constraints.

4.6 As part of their induction, all learners/customers will be required to sign a copy of their Induction Checklist acknowledging their understanding and agreement to the content of the AUP. This document will be maintained on their tutorial/individual record. Learners/customers will also be given a copy of Social Media Guidelines for their reference (shown at Appendix 1).

5. Linked Policies and Guidelines

Disciplinary (Staff and Student)

Respect and Consideration for Others
Social Media Guidelines

6. Equality and Diversity Statement

In accordance with College procedures, an Equality Impact Assessment was undertaken for this policy on

7. Location and Access to the Policy

7.1 The Acceptable Use Policy is located as follows:

- NCG Intranet: Group Services: Group Policies and Procedures
- NCG Website: Media Centre: Guide to Information: Our policies & procedures

8. Person Responsible for the Policy

NCG Director IT Services

9. Definitions

9.1 **NCG Information Processing Asset** relates to any device or account owned by NCG used to access or process NCG information via any means. This includes but is not limited to Desktop Computers, Servers, Laptops, Tablets, Mobile Phones, email accounts and any other system account.

9.2 **Removable Media** includes any device with external memory support or writeable media. This includes but is not limited to memory sticks, memory cards, portable MP3 players, PDAs, external memory, DVDs, CDs and floppy disks.

9.3 **Social Media** for the purpose of this policy describes any website/application that provides a means for communication, content sharing and participation in social networking e.g. blogging.

10. Background

10.1 While NCG's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of NCG. Because of the need to protect NCG's network, management cannot guarantee the confidentiality of information stored on any network device belonging to NCG.

10.2 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use and if there is any uncertainty, employees should consult their supervisor or manager.

10.3 For security and network maintenance purposes, authorised individuals within NCG may monitor equipment, systems and network traffic at any time in accordance with this policy.

10.4 NCG reserves the right to audit networks and systems on a periodic basis to ensure compliance with this Policy.

11. Security and Proprietary Information

11.1 The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as OFFICIAL OR OFFICIAL – SENSITIVE (for employees) or unclassified (for learners/customers), as defined by NCG Data Classification and Handling Policy. Employees should take all necessary steps to prevent unauthorised access by learners/customers to OFFICIAL OR OFFICIAL-SENSITIVE information.

11.2 Learners/customers, employees and sub-contractors are to keep passwords secure and are not to share accounts. Authorised users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly; user level passwords should be changed every six months.

11.3. All NCG information processing assets should be secured with a password-protected screensaver with the automatic activation feature set no longer than 15 minutes, or by logging-off) when the asset will be unattended. Users can manually lock Windows PC's by pressing the 'Windows' key and 'L' if logging out is deemed unnecessary.

11.4 Use of encryption of information is to be in compliance with NCG Data Classification Policy.

11.5 Because information contained on portable computers is especially vulnerable special care should be exercised. Laptops and Tablets are to be protected in accordance with the "Wireless Usage Policy".

11.6 Postings by employees from an NCG email address to newsgroups should only be made in the course of business duties.

11.7 All NCG information processing assets used by the employee or learner/customer that are connected to the NCG Internet/Intranet/Extranet, whether owned by the employee or NCG, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.

11.8 Employees must use caution when opening e-mails received from unknown, untrusted or suspicious senders. In addition employees must exercise extreme caution when clicking links and opening attachments within emails or providing information if the email source is unverified.

11.9 Under no circumstances should personal or sensitive personal data e.g. learner information (as defined by the Data Protection Act 1998) or NCG data, which could negatively impact the commercial interest of NCG, be stored on personal removable media or personal cloud storage accounts such as dropbox, google drive etc.

11.10 The use of corporate removable media and USB-related storage devices with internal or external memory support and related software for data storage that are used for business interests incorporate appropriate technical and organisational controls. NCG employees are expected to secure all such devices used for this activity whether or not they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain personal or sensitive personal data e.g. learner information and/or NCG data.

11.11 **NCG Remote Working (Use of Remote Desktop Services / Client -** NCG recognises the importance regarding the use of Remote Desktop Services (RDS) / Remote Desktop Client (RDC) on Personal Portable devices such as mobile phones, tablets etc. to access NCG systems or services such as email, files, documents shares is often convenient and such use is permitted subject to the following requirements and guidelines. Users must at all times give due consideration to the risks of using personal devices to access NCG information such as:

11.11.1 The device must run a current version of its operating system and be up to date both for the device's operating system and its applications.. *(A current version is*

defined to be one for which security updates continue to be produced and made available to the device).

11.11.2 An appropriate passcode/password must be set for all accounts which give access to the device.

11.11.3 A password protected screen saver/screen lock must be configured.

11.11.4 The device must be configured to “autolock” after a period of inactivity *(no more than 10 minutes).*

11.11.4 All devices must be disposed of securely.

11.11.5 The loss or theft of a device using RDS/RDC must be reported to NCG IT Services.

11.11.6 Any use of personal devices by others (family or friends) must be controlled in such a way as to ensure that these others do not have access to restricted NCG information assets.

11.11.7 Do not leave mobile devices unattended where there is a significant risk of theft.

11.11.8 If a personally owned device needs to be repaired, ensure that the company you use is subject to a contractual agreement which guarantees the secure handling of any data stored on the device.

Note: It is not the responsibility of NCG IT Services to administrate Personal Portable Devices

12. Unacceptable Use

12.1 The following activities are prohibited. Some employees and learners/customers may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g. systems administration staff may have a need to disable the network access of a host if that host is disrupting production services or conducting illegal activities).

12.2 Under no circumstances is a user of NCG systems and services authorised to engage in any activity that is illegal under local, UK or international law while utilising NCG-owned resources.

12.3 The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

13. System and Network Activities

13.1 The following activities are strictly prohibited with no exceptions:

13.1.1 Violation of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by NCG.

13.1.2 Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which NCG or the end user does not have an active license is strictly prohibited.

13.1.3 Exporting software, technical information, encryption software or technology in violation of international or regional export control laws is illegal. The appropriate management should be consulted prior to export of any material in question.

13.1.4 Introduction of unauthorised programs/software into NCG information systems and services (e.g. installing software not tested and approved by NCG Information Security Team, programs/software used for a malicious purpose).

13.1.5 Only equipment owned by NCG may be connected to the NCG network. Personal portable devices must never be connected to the NCG corporate network; however, they may connect to the NCG wireless guest network where available and authorised to do so.

13.1.6 Use of NCG Information processing assets to access/distribute materials that may cause offence to other users e.g. pornographic material, graphic images or material related to terrorism or extremism.

13.1.7 Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

13.1.8 Using a NCG computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

13.1.9 Making fraudulent offers of products, items, or services originating from any NCG information processing asset.

13.1.10 Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the NCG user is not an intended recipient or logging into an NCG system or account that the NCG user is not expressly authorised to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service and forged routing information for malicious purposes.

13.1.11 Port scanning or security scanning is expressly prohibited unless prior notification to Director IT Services is made.

13.1.12 Executing any form of network monitoring which will intercept data not intended for the NCG employees' host, unless this activity is a part of the NCG user's normal job/duty.

13.1.13 Circumventing user authentication or security of any NCG information processing asset

13.1.14 Interfering with or denying service to any user (for example, denial of service attack).

13.1.15 Using any program/script/command, or sending messages of any kind, with the intent to interfere with or disable a user's authenticated session, via any means, locally or via the Internet/Intranet/Extranet.

13.1.16 Providing information about, or lists of, NCG employees to parties outside of NCG without prior authorisation

13.1.17 "Home Drives", or "My Documents" network locations are made available for the storage of educational and business related files only. Home drives are monitored on a regular basis and any media or files that are not educational or business related may be deleted. You should keep your Home Drive free from unwanted or out of date documents. Storage of un-related NCG, unwanted or out of date files may have an adverse effect on system backups.

14 Email and Communications Activities

14.1 The following email and communication activities are strictly prohibited, with no exceptions:

14.1.1 Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

14.1.2 Any form of harassment or inappropriate content (for example, but not limited to; terrorism, extremism, offensive language and/or images) via email, telephone or paging, whether through language, frequency, or size of messages.

14.1.3 Unauthorised use, or forging, of email header information.

14.1.4 Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

14.1.5 Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

14.1.6 Use of unsolicited email originating from within NCG's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by NCG or connected via NCG's network.

14.1.7 Posting the same or similar non-business related messages to large numbers of non-business related newsgroups (newsgroup spam).

14.1.8 Use of corporate email should be for NCG business purposes only e.g. corporate email accounts should not be used to subscribe to anything for personal purposes e.g.newsletters, social media etc.

15. Social Media Activities

15.1 Use of social media by employees or learners/customers, whether using NCG’s property and information processing assets or personal computer systems, are also subject to the terms and restrictions set out in this Policy. Limited and occasional use of NCG’s systems to engage in social media is acceptable, provided that it is done in a professional and responsible manner; does not otherwise violate NCG’s policy; is not detrimental to NCG’s best interests; and does not interfere with an

employee's regular work duties. Use of social media from NCG information processing assets is also subject to monitoring.

15.2 NCG's Data Classification Policy also applies to Social Media. As such, employees are prohibited from revealing any material covered by NCG's Data Classification Policy when engaged in the use of social media.

15.3 Employees and learners/customers shall not engage in the use of any social media that may harm or tarnish the image, reputation and/or goodwill of NCG and/or any of its employees. Employees are also prohibited from making any discriminatory, derogatory, offensive or harassing comments when using social media

15.4 Employees and learners/customers may not attribute personal statements, opinions or beliefs to NCG when engaged in the use of social media. If an employee is expressing his or her beliefs and/or opinions in blogs the employee may not, expressly or implicitly, represent themselves as an employee or representative of NCG. Employees assume any and all risk associated with social media.

15.5 All laws pertaining to the handling and disclosure of copyrighted or export controlled materials, NCG's trademarks, logos and any other NCG intellectual property may not be used in connection with social media

16. Social Networking Sites

16.1 This refers to the use of Web software that supports social networking and media sharing.

16.2 NCG permits the use of some social networking sites but usage will be monitored and any excessive or inappropriate use will be addressed. NCG reserves the right to withdraw access to social networking sites at any time.

16.3 The use of social networking should be for business, educational and learning purposes. It may be used in addition to, but not as a substitute for, the requirement to use NCG specific systems as outlined in the ILT strategy.

16.4 Any posts or comments to social media sites referencing NCG or its Divisions must not damage reputation, confidentiality or working relationships of the business.

16.5 NCG employees and students/customers must not utilise NCG information processing assets to engage in political activities where this might be construed as representing the NCG.

17. Monitoring

17.1 Use of the Internet/Intranet and email may be subject to monitoring for security, safeguarding, network or other management reasons, and users may also be subject to access limitations on such resources.

17.2 The distribution of any information through the Internet, computer-based services, email and messaging systems may be scrutinised by NCG. NCG reserves the right to determine the suitability of this information and withdraw the users rights to such services.

17.3 NCG reserves the right to remove any comments on internal websites which may give rise to complaint and apply to have comments removed from external websites.

17.4 The use of NCG information processing assets is subject to UK law and any illegal use will be reported to the relevant authorities and dealt with appropriately. NCG may exercise its right to intercept mail and Internet access under the relevant UK law.

17.5 All information processing assets are the property of NCG and are designed to assist in the performance of employee's or learner's/customer's work. Employees and learners/customers should therefore have no expectation of privacy in any email sent or received, or in the internet sites that they access.

18. Security

18.1 Any NCG infomormation processing asset should not be left unattended in rooms with open access when logged in. Access to NCG information processing assets is restricted by login usernames and passwords provided by IT Services. Audit requirements dictate that NCG systems, services equipment be setup with an automatic screensaver lock.

18.2 Directors of Schools/Service/Heads of Learning/Training are responsible for ensuring that systems are in place within their Departments/Divisions to ensure that notifications are made of any changes to the IT inventory in respect of IT equipment in their department.

19. Inappropriate Usage

19.1 Users who receive unsolicited e-mails should inform IT Group Helpdesk who will instigate appropriate actions to identify the source. If the source is external, measures will be taken to block such mail. If the source is internal, an investigation will be implemented. Internet libel is the publication of a defamatory statement in permanent form, which includes publication on the internet. NCG will undertake swift action if it becomes aware of statements posted on websites which may be considered defamatory.

19.2 Any form of harassment, including defamatory statements, terrorism or extremism related content or any other unacceptable content will be given serious consideration by NCG and appropriate action will be taken.

19.3 If an employee or learner/customer becomes aware of a statement on a website which could be considered defamatory they should contact IT Group Helpdesk with the following information:

Their name and contact details
The location of the statement
The nature of the complaint –i.e. why they object to the statement.

19.4 NCG reserves the right to secure the removal of any such statement, and will carry out an investigation into how such a statement was posted.

20. Enforcement

20.1. Any individual found to have contravened any of the above may be subject to the disciplinary procedures of NCG and may have their access to NCG resources removed. For staff such conduct may result in dismissal for reasons of gross misconduct.

20.2 In regard to an employee, the Director of IT Services will inform the Director of Human Resources or nominated deputy to instigate an investigation. In regard to a learner/customer the Director of IT Services will inform the Director of School /Head of Learning/Training Programme to instigate an investigation.

REVISION HISTORY

Version Number: 10 Dated: 7th September 2015

Appendix 1

SOCIAL MEDIA GUIDELINES

NCG embraces the responsible use of social media to share the qualities and strengths of our organisation. We use social media to promote the events, activities and accomplishments at NCG, and to reach out effectively to our broader community. NCG therefore uses social media to advance the organisation and build relationships with important constituencies like prospective and current learners/customers, staff, alumni and key stakeholders.

Staff and students are encouraged to share news, events or promote work through social media tools but must, follow the same behavioural standards online as they would in real life. The same laws, professional expectations and guidelines for interacting with learners/customers, parents, alumni, media and other NCG constituents apply online as in the real world. Employees are liable for anything they post to social media sites.

1. NCG Policy for Social Media sites, including personal profiles

1.1 Maintain Confidentiality

Do not post confidential or proprietary information about NCG learners/customers, employees, alumni or key stakeholders. Employees must still follow the applicable laws governing the protection of information and act only within the guidance set in this document and other applicable NCG Policies. Employees who share confidential information do so at the risk of disciplinary action.

When posting, the copyright and intellectual property rights of others and of NCG are to be in strict accordance with current legislation.

1.2 Appropriate conduct

When communicating either in a professional or personal capacity within or outside of the workplace, employees must not conduct themselves inappropriately. Inappropriate conduct will be dealt with via the Disciplinary Procedure and/or Respect and Consideration Policy. In some cases the behaviour may amount to gross misconduct. Examples are detailed below:

- Engaging in activities that have the potential to bring the NCG and/or their respective Division into disrepute

- Making comments that could be considered bullying, harassment or discriminatory against any individual
- Posting or re-posting remarks, uploading inappropriate comments, images, photographs etc. that may inadvertently or deliberately cause offence
- Engaging in discussion or anything which may contravene the NCG or Divisional policies or which may cause harm to the business
- Pursuing personal relationships with students
- Posting any material that breaches copyright legislation
- Do not use the NCG name to promote a product, cause, or political party or candidate.

  Be aware that social media is a very open environment. Consider what could happen if a post becomes widely known and how that may reflect both on the poster and NCG. Search engines can turn up posts years after they are created and comments can be forwarded or copied. If you wouldn't say it at a conference or to a member of the media consider whether you should post it online.

1.3 Maintain professional boundaries

NCG encourages the positive use of social media. Learners/customers may wish to form personal relationships with employees, however to ensure professional boundaries are maintained employees must not accept and/or invite the following individuals to be friends on personal social media accounts or other online services.

- Current learners/customers
- Ex-learners/customers under the age or 18 or vulnerable adults

Breaches of this Policy in this respect may lead to disciplinary action and may lead to dismissal.

There may be times where an employee may know a learner/customer on a personal level (in whatever capacity) prior to them commencing on any programme with NCG. Employees should advise their line manager if this is the case and an individual assessment of the situation will take place.

1.4 Using NCG logos and imagery

Do not use the NCG logo or any other NCG images or iconography on personal or social media sites unless explicit permission has been sought from the Social Media Manager.

2. Representing NCG on Social Media

2.1 If you post on behalf of NCG, the following direction must be adhered to in addition to the AUP and best practices listed above.

2.2 The Social Media Manager is to be informed every time you intend to create a social media account for a Division/Department within NCG.

2.3 Accounts created prior to this guidance implementation must be registered with the Social Media Manager. The Social Media Manager for NCG is to be made an administrator for any of these sites.

2.4 If you are representing NCG when posting on a personal social media profile you must provide a disclaimer to acknowledge this, identifying your views as your own and not necessarily those of NCG. Never pretend to be someone else and post about NCG.

2.5 Departments should consider their messages, audiences, and goals, as well as a strategy for keeping information on social media sites up-to-date. The Social Media Manager is to be consulted on all NCG specific posts.

2.6 Whenever possible, include links back to the NCG (or relevant Division) website. Ideally, posts should be very brief; redirecting a visitor to content that resides within the NCG/Divisional Web environment.

2.9 Ensure that you have all the facts before you post. It is better to verify information with a source first, rather than post a correction or retraction later. Cite and link to your sources whenever possible and if you do make an error, correct it quickly and visibly. Review content for grammatical and spelling errors. This is especially important if posting on behalf of NCG in any capacity.

2.10 Comments on postings should be welcomed as they build credibility and community. However, you can set certain social media sites so that you can review and approve comments before they appear. Comments subject to rejection include:

- Comments including profanity, racist, sexist or derogatory comments
- Product advertisements
- Political support
- Comments that are off topic or SPAM
- Comments that are personal attack on an individual

2.11 Understand that content contributed to a social media site could encourage comments or discussion of opposing ideas. Responses should

be considered carefully in light of how they would reflect on the poster and/or NCG and its' business voice. If you are unsure about posting something or responding to a comment ask your immediate manager for advice.

2.12 Social media will more likely pay dividends if you add value to your followers, readers, fans and users. If it contributes directly or indirectly to the improvement of NCG; if it allows the general public to learn more about NCG; or if it builds a sense of community and helps fans and followers feel more connected to NCG, then it's adding value.

2.13 Photography: Photographs posted on social media sites can easily be appropriated by visitors. Consider adding a watermark and/or posting images at 72 dpi and approximately 800x600 resolution to protect your intellectual property. Images at that size are sufficient for viewing on the Web but not suitable for printing.

3. Recruitment and selection

3.1 NCG may view relevant social media websites as part of the pre-employment process. Any information which relates to an applicant's protected characteristics under the Equality Act 2010 will not be used as part of the recruitment and selection process. Any breach of this may result in disciplinary action.

4. Monitoring

4.1 Use of the Internet/Intranet and email may be subject to monitoring for security and/or network management reasons and users may also be subject to access limitations on such resources.

4.2 The distribution of any information through the Internet, computer-based services, email and messaging systems may be scrutinised by NCG. NCG reserves the right to determine the suitability of this information and withdraw the users rights to such services.

4.3 NCG reserves the right to remove any comments on internal websites which may give rise to complaint and apply to have comments removed from external websites.

4.4 The use of computing resources is subject to UK law and any illegal use will be reported to the relevant authorities and dealt with appropriately. NCG may exercise its right to intercept mail and Internet access under the relevant UK law.

4.5 Computers and email accounts are the property of NCG and are designed to assist in the performance of employee's or learner's/customer's work. Employees and learners/customers should therefore have no expectation of privacy in any email sent or received, or in the Internet sites that they access.