The NLC Information Security Policy

Incorporates Acceptable Usage Guidelines

Return to top

1.0 Introduction

The NLC makes extensive use of Information Technology and Information Systems (*IT/IS*) to assist in achieving our charitable objectives. The increasing reliance on *IT/IS* for the delivery of The NLC services makes it necessary to ensure that these systems are developed, operated, used and maintained in a safe and secure fashion.

1.1 Need for an *Information security* Policy

1.1.1 The NLC has an obligation to its staff to clearly define requirements for the use of its information technology (IT) facilities and its information systems (IS). This is so that *users* of *IT/IS* facilities do not unintentionally place themselves, or the organisation, at risk of prosecution, by carrying out computer related activities outside the law.

1.1.2 In addition, certain information that we handle, particularly relating to residents, donors, trusstees and colleagues, has to be processed, handled and managed securely and with accountability. Legislation is the key driver of this requirement, in addition to the criticality and sensitivity of certain information where loss of accuracy, completeness or *availability* could prevent The NLC from functioning efficiently, or where disclosure could damage the organisation's reputation. Unless policy is in place to stipulate control requirements for such information, there is an increased risk that security breaches will be suffered, potentially resulting in a wide-range of adverse consequences.

Normal text that is italicised is defined within a glossary, which can be found at Annex A.

1.2 Legal Requirements

Some aspects of *information security* are governed by legislation; the most notable UK Acts are:

- The Data Protection Act (1998)
- Copyright, Designs and Patents Act (1998)
- Computer Misuse Act (1990)
- Regulation of Investigatory Powers Act (2000)
- Freedom of Information Act (2000) – see The NLC's Open Information Policy
- Human Rights Act (2000)
- Equality Act (2010)
- The potential contractual nature of any correspondence (including by email), and the potential for defamation, breach of copyright, breach of confidentiality, or other offences which might result in litigation against either the organisation or the individual.

For a more detailed explanation of each of the above see www.opsi.gov.uk/acts.htm.

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). This applies from May 2018.

1.3 Purpose

1.3.1 Information plays a major role in supporting The NLC's service delivery and administrative activities. The purpose of this policy is to provide a framework for protecting:

- The organisation's *IT/IS* infrastructure so it performs optimally for its intended use;
- *Key data* and *information*;
- Those who have access to or who administer *IT/IS* facilities;
- Individuals who process or handle *key data* and *information*.

1.3.2 The policy is designed to provide protection from internal and external security threats, whether deliberate or accidental by:

- Defining The NLC's policy for the protection of the confidentiality, *integrity* and *availability* of its *key data* and *information*;
- Ensuring regulatory and legislative requirements are met;
- Establishing responsibilities for *information security*.

1.4 Objective

1.4.1 *Information security* controls are designed to protect The NLC's *users* and The NLC's reputation through the preservation of:

- *Confidentiality* – knowing that *key data* and *information* can be accessed only by those authorised to do so;

- *Integrity* – knowing that *key data* and *information* is accurate and up-to-date, and has not been deliberately or inadvertently modified from a previously approved version; and,

- *Availability* – knowing that the *key data* and information can always be accessed.

1.4.2 The level of security required in a particular system will depend upon the risks associated with the system, the data held on the system and the working environment of the system. This policy applies to all information held in both manual and electronic form.

1.5 Scope

1.5.1 The policy applies to all information systems (including, but not limited to, all hardware, software, networks, email systems, the internet, fax and telephones):

- Owned by The NLC
- Being used for The NLC business
- Connected to networks managed by The NLC
- Including remote access

1.5.2 The policy applies to all information:

- The NLC is handling whether or not it is owned by The NLC.
- Including software owned or licensed by The NLC.

1.5.3 The policy applies to all people:

- Managing or using any system identified in 1.5.1 above.
- Responsible to The NLC and handling information identified in 1.5.2 above.

- This includes all employees, sessionals, volunteers, students, associates, consultants, contractors, agency staff and all other individuals and groups who have been granted access to The NLC's *IS/IT* systems and/or *key data* and *information*.

1.5.2 Heads of service are ultimately responsible for ensuring that this policy is implemented within their respective service and for overseeing compliance by *users* under their direction, control or supervision.

1.5.3 It is the personal responsibility of each person to whom this policy applies to adhere to its requirements. Everyone is responsible for protecting the *confidentiality*, *integrity* and *availability* of the data which they themselves handle.

Return to top

2.0 General Principles and Personal Use

- It is vital that you read this policy carefully. If there is anything you do not understand, it is your responsibility to ask your manager to explain.
- It is essential that you understand that if you fail to comply with this policy that you may be subject to The NLC's disciplinary procedures and/or legal proceedings. Your failure to comply may also result in legal proceedings against The NLC.
- The NLC's equipment is provided for business use so that The NLC can carry out its aims.
- All The NLC *users* are responsible for ensuring that The NLC's computer systems and information contained within them are protected against unauthorised access.
- You should not use The NLC equipment in any way that is going to interfere with the proper running of The NLC, significantly distract you and/or others from your work, interfere with the performance of your or others' duties or breach the rules set out in this policy.
- Use of disk storage and network capacity for personal use must be reasonable and should not impact The NLC's ability to fulfil its business objectives.
- You understand that The NLC may monitor your use of The NLC equipment for security purposes and also to check your compliance with this policy at any time and without notifying you.
- The NLC may scan all incoming and outgoing email messages and attachments for unsuitable content.
- The NLC may decide to limit your ability to use The NLC equipment for personal use where The NLC considers this is appropriate due to possible or actual interference with The NLC business. This would be decided by your line manager with input from human resources.
- Your use of The NLC equipment is subject to all applicable laws and any illegal use will be dealt with in accordance with these laws.
- You must not use The NLC equipment for any business activities that are not related to your work at The NLC.

Return to top

3.0 Security Measures

3.1 Protection of hardware from theft

3.1.1 The The NLC server room is kept locked at all times. Access to the server room is restricted and access is only granted when required, under supervision of a member of the IT team.

3.1.2 Precautions should be taken to ensure that access to The NLC equipment is restricted at all times to authorised personnel.

3.1.3 All The NLC computer equipment is identity tagged and an asset register is maintained by IT. It is the responsibility of line managers to notify the IT team of any movements or changes.

3.1.4 No equipment should be removed from any site without the approval of the IT department, apart from laptops and portable media devices which are the responsibility of each named individual user.

3.1.5 All hardware left in premises which are likely to be unattended should make use of physical security measures such as locking office doors or installing locking devices to secure hardware to the desk. Equipment must never be left in unattended vehicles.

3.1.6 Redundant hardware will be disposed of in accordance with the procedure outlined in section 4.1.

3.2 Protection of hardware from accidental damage

3.2.1 Care should be exercised when eating or drinking near IT equipment. Eating and drinking is not permitted in the server room.

3.2.2 The location of all hardware (computers, printers, modems etc.) should comply with health and safety standards including the stability of the desk surface, and the elimination of trailing cables. Please see the health and safety policy for further guidance.

3.2.3 All personal computers and printers should be switched off when not in use for extended periods, such as overnight or during weekends, except for essential server room equipment.

3.2.4 Removable media (eg USB sticks) with sensitive information should be stored in locked desks or fireproof safes.

3.2.5 Air vents on computers should not be obstructed.

3.3 Protection of data from hardware loss

3.3.1 Backups of data and system programs at all The NLC premises are made daily.

3.3.2 Data should not be held locally on *PCs*, as this is not included in the automatic nightly backup of the network servers. Data should be saved to files on the servers (in most instances, the "shared drive").

3.3.3 Backup media will be stored securely off-site.

3.3.4 Backup recovery procedures will be tested regularly as determined by the Head of IT.

3.4 Software Control

3.4.1 All software must be purchased through the IT department and no software should be installed without permission from IT.

3.4.2 A register of software will be maintained by IT.

3.4.3 Do not download ANY software or any unauthorised programs without contacting the IT team. You should note that the use of unlicensed software can also have severe legal implications since you may be infringing someone else's copyright or importing a virus.

3.4.4 Do not open emails or attachments from non-trusted sources.

3.4.5 The NLC equipment must not be modified in its setup nor have any additional software installed unless approved by IT.

3.4.6 You may not copy, change, or transfer any software provided by The NLC without permission.

3.4.7 All system software disks will be stored securely in the IT server room. These are the only proof of a legal license to use the software, and may be required to be produced in evidence should the Federation Against Software Theft (FAST) investigate.

3.5 Virus Control

The deliberate introduction of malicious software to a system is a criminal offence under the Computer Misuse Act 1990.

3.5.1 No files should be loaded on to any system from a USB stick, CD or portable disk drive unless they have first been virus checked by IT (this only applies if the portable media device has been used with a non-The NLC computer).
3.5.2 All servers and The NLC *PCs* and laptops have anti-virus software installed.
3.5.3 Where a virus is detected this will be reported immediately to IT who will attempt to "clean" and rebuild the affected PC or laptop and update the anti-virus software.

3.6 Protection of data from unauthorised access

3.6.1 Password controls must be implemented on all systems in use within The NLC. When creating a password you should bear in mind the following:

- Ensure it is a minimum of eight characters long
- Make sure it contains letters and numbers for improved security
- Change it at least once every 45 days and do not re-use previous passwords
- Do not choose a password that is likely to be easily associated with you eg names of your spouse, children or pets.

3.6.2 You must keep all passwords for The NLC equipment safe. Do not write them down in any manner that would make it easy to decipher. Do not tell anyone your login details or password.
3.6.3 If you believe that your account has been accessed without your knowledge, then you should change your password and contact the IT team immediately.
3.6.4 Monitors used in public areas should be tilted away from the public's direct line of sight so that confidential information cannot be viewed.
3.6.5 You must only access information on The NLC equipment and systems about which you have a genuine business need to know. If you access information to which you are not authorised you may be committing a criminal offence (eg under the Computer Misuse Act), as well as a breach of this policy.
3.6.6 Reports containing sensitive information (eg payroll data) which require disposal must be shredded.
3.6.7 Backups and copies of data should be stored securely off-site.
3.6.8 All storage media, including backups, should be clearly marked to avoid confusion over their contents.
3.6.9 Where appropriate, physical controls should be used to prevent unauthorised access.

3.7 Protection of personal data

In addition to the eight Data Protection Principles (see data protection policy) which The NLC undertakes to abide by, there are also several key points to stress:

3.7.1 Everyone, including service *users* and The NLC staff, have a right to respect for their privacy and hence an expectation that information about them will be treated as confidential.
3.7.2 All The NLC staff members have a common law duty of care to protect personal information.
3.7.3 All The NLC departments must have an active policy for informing data subjects of the kind of purposes for which information about them is collected (see 15.2 on privacy notices).
3.7.4 Arrangements (both manual and technology based) for the storage, disposal and handling of information must protect confidentiality. Care should be taken to ensure that unintentional breaches of confidence do not occur (see retention of data policy).
3.7.5 Breach of confidentiality is a serious matter that may result in disciplinary action by The NLC or legal action by a member of the public.
3.7.6 All data requests must be forwarded to the designated The NLC Data Protection Officer.

3.8 Personnel Security

Controls will be deployed to reduce the risks of human error, theft, fraud, nuisance or malicious misuse of facilities.

3.8.1 Security roles and responsibilities will be included in job descriptions where appropriate. These will include any specific responsibilities for the protection of particular assets, or the execution of particular processes or activities such as data protection.
3.8.2 All members of staff are reminded of their obligation to protect confidential information in accordance with The NLC's standard terms and conditions of employment.
3.8.3 Employees will be informed of their *information security* responsibilities during induction training and these will be reiterated as appropriate.
3.8.4 All actual and suspected *security incident*s are to be reported immediately to the IT team.

Return to top

4.0 Information Handling

4.1 Disposal of equipment with sensitive data

4.1.1 The permanent disposal of equipment containing storage media must only be carried out by the IT team, who will ensure that all *personal data* (as defined under the Data Protection Act 1998) and licensed software is irretrievably deleted either before the equipment is moved off-site, or by utilising an approved third party off-site service. Procedures for disposal should be documented.

4.1.2 Damaged storage devices containing confidential or *sensitive* data must undergo appropriate risk assessment by IT, to determine if the device should be destroyed, repaired or discarded. Such devices will remain the property of The NLC and only be removed from site with the permission of the IT team.

4.1.3 The NLC advocates a clear screen policy particularly when employees are absent from their normal desk and outside normal working hours. When away from your desk, screens must be 'locked' by pressing 'Ctrl' + 'Alt' + 'Del' and selecting 'Lock Computer'. In addition, screens on which confidential or *sensitive* information is processed or viewed should be appropriately sited in such a way that they cannot be viewed by unauthorised persons.

4.1.4 Any third party used for external disposal of The NLC's obsolete information-bearing equipment or hardcopy material must be able to demonstrate compliance with The NLC's IT security policy.

4.2 Handling confidential data and documents

4.2.1 Removal off site of The NLC's sensitive *information assets*, either printed or held on computer storage media, should be properly authorised by management. Prior to authorisation, a risk assessment based on the criticality of the information asset should be carried out.

4.2.2 All *users* of information systems must manage the creation, storage, amendment, copying and deletion or destruction of data files in a manner which safeguards and protects the *confidentiality*, *integrity* and *availability* of such files.

4.2.3 Confidential or sensitive data should only be accessed from equipment in secure locations and files must never be printed on a networked printer that does not have adequate protection or security.

4.2.4 The use of USB sticks or any other portable devices for the transference or holding or sensitive data is strictly prohibited.

4.2.5 All employees are required to be made aware of the risk of breaching *confidentiality* associated with the copying (including photocopying or other duplication) of confidential or sensitive documents. Authorisation for copying such documents should be obtained from the document owner where documents are classified as highly confidential or above.

4.2.6 All hardcopy documents of a confidential nature are to be shredded when no longer required. Approved software deletion methods must be employed for similar electronic documents.

4.2.7 Prior to sending confidential information/documents to *third parties*, not only must the intended recipient be appropriately authorised to receive such information, but the procedures and *information security* measures adopted by the *third party* must also continue to assure the confidentiality and *integrity* of the information.

4.2.8 Sensitive data or information may only be transferred across networks, or copied to other media, when the *confidentiality* and *integrity* of the data can be reasonably assured.

4.3 Communication by email, fax and telephone

4.3.1 Email addresses and fax telephone numbers should be checked carefully prior to transmission, especially where the information content is confidential, or where the disclosure of email addresses or other contact information to the recipients is a possibility.

4.3.2 The identity of recipients or requesters of confidential information over the telephone must be verified and they must be authorised to receive it.

4.4 Use of password protection and encryption

4.4.1 The *confidentiality* of information being transferred on portable media or across networks must be protected by use of password protection. Please note that when emailing password-protected documents you should not include the password in the same email.

4.4.2 In some circumstances it may be necessary to protect confidential information from unauthorised disclosure by use of appropriate encryption techniques. However, there are risks attached to this as the information cannot be retrieved if the password is lost or forgotten. You should therefore not use this method without first consulting the IT team.

4.5 Data backup

4.5.1 Whilst "backups" are mostly associated with electronic information, this policy applies equally to information in other formats.

4.5.2 The NLC business must not be exposed to undue and unnecessary risk as a result of inadequate backup arrangements. Depending on the type of data involved and how frequently it changes, each department must:

- Have arrangements to ensure regular backup
- Run sufficiently frequent backups
- Store backup data remote from the original data
- Periodically test recovery from backups
- Store backup data on resilient disk storage systems

4.5.3 Backups of information, such as data and software, must be made where the possibility of losing the live, working or master copy of the information is unacceptable. In other cases, where not having backups is potentially more costly than making them, or where there is any doubt, backups should be taken.

4.5.4 The member of staff with day-to-day responsibility for managing an information asset is by default responsible for ensuring that any necessary backup procedures are in place, adequate and tested. This may be the information owner or the manager of a system that stores or processes the information.

4.5.5 Where aspects of administering an information asset, eg a computer system, are shared between different individuals or groups it must be clearly established who is taking responsibility for backup arrangements.

4.5.6 Staff responsible for archiving or making backups should make themselves aware of the The NLC data retention policy relating to the type of data being handled.

4.5.7 The staff member responsible for an information asset is also responsible for ensuring that all owners of information held in the asset are aware of the backup arrangements. Where appropriate there should be liaison between the person responsible for managing backups and data owners with the aim of ensuring that the arrangements are suitable.

4.5.8 Staff identifying potentially inadequate backup arrangements, for information which The NLC has responsibility, must inform their line manager.

4.5.9 Backup media must be securely disposed of, when no longer required, in a way that ensures that information will not be disclosed to unauthorised persons.

4.5.10 Recoverability of backed up data should be periodically tested (ensuring that the recovery procedure does not accidentally destroy more recent files).

Return to top

5.0 Business continuity management

The NLC recognises that IT systems are increasingly critical to its business and that the protracted loss of key systems/user areas could be highly damaging in operational terms. The organisation therefore seeks to counteract potential disruptions to our information processing facilities and to protect *critical systems* from the effects of major failures and disruption by implementing appropriate controls.

5.1 Data Storage

Key data must be held on a network resource (ie the 'S:' drive) so that it is backed up through a routine managed process. Where this is not possible, provision must be made for regular and frequent backups to be taken.

5.2 Backup Media

A controlled and fully auditable process for the handling, transportation, storage and retrieval of backup media containing *key data* will be implemented by the IT team.

5.3 Continuity Strategy

Heads of Service are responsible for their own service's contingency plan, its ongoing review and maintenance. These service strategies form part of the wider organisational plan and are designed to ensure the *availability* of services in the event of unexpected disruption.

The IT department will be responsible for the technical aspects of all contingency plans and can provide advice. They will maintain a disaster recovery plan to ensure that all *critical systems* can be restored if necessary.

Return to top

6.0 User Authorisation

Access to computing facilities is via individual username and password, which allows access to login to central computing services, make use of private file space, run software, access and use email facilities, share and transfer files and gain access to the Internet.

6.1 Eligibility

6.1.1 The following are eligible to register as *users*:

1. Any person holding a contract of employment or sessional agreement with The NLC.
2. Any volunteer or student holding an agreement with The NLC.
3. Where necessary, any associate/consultant holding an agreement with The NLC.

6.1.2 With the exception of access to material intended for the general public, use of information systems and networks shall be restricted to registered *users*.

6.2 Registering Users

6.2.1 Line managers are responsible for informing IT of new starters, using the form at Annex B.
6.2.2 Access privileges will be modified/removed – as appropriate – when an individual changes jobs/leaves, as notified to IT by the line manager and/or human resources.

6.3 Acceptable Use

- Accounts are issued for individual use only. For security purposes, *users* may not share, loan or give away account or password information to any other person.
- User accounts are to be used only by the assigned user of the account for authorised purposes.
- Passwords should not be shared, written down, emailed or published. Default passwords should be changed as soon as practically possible.
- Attempting to obtain another user's account password is strictly prohibited. *Users* are required to change their password if they have reason to believe their account has been compromised in any way.
- *Users* are required to take all necessary precautions to prevent unauthorised access to computing resources.

***Users* must be aware of and understand this policy before accepting and using an account.**

6.4 Staff leaving The NLC's employment

6.4.1 When a member of staff leaves the employment of The NLC, their email account is ended as part of the termination process carried out by human resources.

6.4.2 Prior to an employee leaving, or to a change of duties, line managers and/or human resources should ensure that:

- The IT team is informed of the termination or change, and, where appropriate, the name is removed from authority and access lists
- Where relevant, supervisor's passwords allocated to the individual should be removed and consideration given to changing higher level passwords to which they have access
- Reception staff and others responsible for controlling access to appropriate premises, are informed of the termination, and are instructed not to admit in future without a visitors pass
- Where appropriate, staff working out notice are assigned to non-sensitive tasks, or are appropriately monitored
- Departmental property is returned. In addition to computer equipment, particular attention should be paid to the return of items which may allow future access. These include ID cards, access cards, keys, manuals and documents.

6.4.3 The timing of the above requirements will depend upon the reason for the termination, and the relationship with the employee. Where the termination is mutually amicable, the removal of such things as passwords and ID cards may be left to the last day of employment. Once an employee has left, it can be impossible to enforce security disciplines, even through legal process.

6.4.4 Prior to leaving, the employee's manager should ensure that all PC files of continuing interest to the organisation are transferred to another user before the member of staff leaves. It is good practice to have a 'handover' meeting in which the manager notes all the systems to which the member of staff had access.

6.4.5 Managers must ensure that staff leaving The NLC's employment do not inappropriately wipe or delete information from hard disks. If the circumstances of leaving make this likely then access rights should be restricted to avoid damage to The NLC information and equipment.

Return to top

7.0 Internet

Use of the internet by The NLC *users* is permitted and encouraged where such use supports the goals and objectives of the organisation. However, *users* must ensure that they:

- **Comply with current legislation;**
- **Use the internet in an acceptable way;**
- **Do not create unnecessary business risk to The NLC by their misuse of the internet.**

7.1 Unacceptable usage

In particular, the following is deemed unacceptable use or behaviour by *users*:

- Visiting internet sites that contain pornographic, obscene, indecent, hateful or other offensive or illegal material (for example, material that contains racist terminology or nudity) except where you are expressly required to do so in the course of your work.
- Using The NLC equipment to participate in online gambling or multi-player online games, or for soliciting for personal gain or profit.
- Using the internet to perpetrate any form of fraud, or software, film or music piracy.
- Posting or transmitting indecent, offensive or defamatory (including libellous or slanderous) material on the internet including when blogging or in message rooms. When posting material, it is your responsibility to comply with all applicable laws – such as copyright and harassment laws.
- Successful or unsuccessful attempts to gain unauthorised access to information resources, commonly know as 'hacking';
- Violating copyright, license agreements or other contracts, for example, copying and using software for business purposes from a site where there is a clear limitation for personal use only;
- Undertaking deliberate activities that waste staff effort or resources.
- Breaching The NLC's *information security* policy.
- Violating any UK laws pertaining to the unauthorised use of computing resources or networks.

The NLC reserves the right to block access to any internet site that is interfering with the operation of normal The NLC business (eg where the amount of traffic is interfering with access to other work-related material on the internet).

7.2 Downloading files and software

- **No file should be downloaded from or via the internet unless doing so is expressly permitted by the IT team and it is in connection with the user's job.**

- **Downloading software onto The NLC equipment** Downloading (including any software available for free on the internet) without obtaining permission from the IT department can affect the *integrity* of The NLC's systems and create unnecessary interference and downtime.

- **Particular attention must be paid to any specified licensing specifications or other similar conditions. *Users* are not permitted to enter into any agreement on behalf of The NLC.**

7.3 Personal use of the Internet

- Personal use of the Internet should only be during employees' free time and should always take second place to the carrying out of work duties.

- It is not acceptable for resources and, in particular, employees' time to be wasted in casual surfing of the internet. However, personal use is permitted provided all guidelines within this policy are adhered to and use is not excessive. Personal access may be withdrawn if it is being abused.

Return to top

8.0 Social Networking Sites

8.1 What is social networking?

8.1.1 Social networking is the use of web-based and mobile technologies to interact and share information online (including video, audio, photographs and text) publicly or privately with one another.

8.1.2 Social media includes a wide variety of internet-based applications such as Facebook, LinkedIn, Twitter, YouTube, Blogster, Flickr, MySpace and wikis (Wikipedia, for instance). This list is not exhaustive and the lack of explicit reference to a specific site does not limit the extent of the application of this policy.

The NLC does not discourage staff from using such services. Used appropriately, social networks are a highly useful resource for the organisation, bringing opportunities to understand, engage and communicate with our service *users*, partners, donors and potential employees in new ways. However, it is also important to ensure that we balance this with our duties to our service *users* and partners, our legal responsibilities and our reputation.

The following points aim to provide this balance to support innovation whilst providing a framework of good practice.

8.2 Professional use of social networking sites

8.2.1 Staff who use social networking sites will be considered to be representing The NLC if they:

- Use a The NLC email address as their contact email;
- State in their profile that they work for The NLC;
- State in a discussion online that they work for The NLC;
- Post comments/information about The NLC on social networking sites;
- Use social networking sites to communicate with service *users*;
- Use networking sites from The NLC computers.

This list gives examples of how someone can be linked to The NLC and is not exhaustive.

8.2.2 It is important to ensure that *users* of online services know when a social networking application is being used for official The NLC purposes. To assist with this, all The NLC representatives must adhere to the following requirements:

- They must only use The NLC issued email addresses for user accounts which will be used for official The NLC purposes;

- The use of The NLC's logo and other branding elements should be used where appropriate to indicate The NLC's support. The logo must not be used on social networking applications which are unrelated to or are not representative of The NLC's official position.
- The NLC representatives should identify themselves as such where appropriate on social networking applications. For example, through providing additional information in user profiles.
- The NLC representatives should ensure that any contributions they make are professional and uphold the reputation of the organisation.
- If approached by a media contact about content on a site relating to The NLC, employees should not comment and should instead direct the query to the Head of Communications.

8.2.3 Staff seen to be using social networking websites to represent The NLC must:

- Remember that your online presence reflects the organisation. Be aware that your actions captured via images, posts, or comments can reflect that of our organisation.
- Be respectful to the organisation, other employees, service *users*, partners, and competitors. Take care not to allow interaction on these websites to damage working relationships.
- Ensure that you do not conduct yourselves in a way that is and/or could be seen as bringing The NLC into disrepute;
- Ensure that any comments you post on these websites could not constitute bullying, harassment or discrimination;
- Ensure that you do not contravene the Data Protection Act by posting information about The NLC, its staff or service *users* or any *third party*.
- Respect copyright laws, and reference or cite sources appropriately. Plagiarism applies online as well.
- Not breach The NLC's policies, including misconduct, equal opportunities, safeguarding and bullying and harassment policies. Online breaches of these policies will be dealt with in the same way as other such instances.
- Not publish any content which may result in actions for defamation or other claims for damages.
- Not use these sites for the promotion of personal financial interests, commercial ventures or personal campaigns.
- Ensure that information you post on your blog complies with The NLC's confidentiality and disclosure of proprietary data policies. This also applies to comments posted on blogs, forums, and social networking sites.
- Not reference or cite company clients, partners, or customers without their express consent.
- Not use the The NLC logo without written consent.

8.2.4 The NLC reserves the right to restrict access to personal networking sites if it should be necessary.

8.2.5 Security and identity theft

Staff should be aware that social networking websites are a public forum and should not assume that their entries on any website will remain private.

Staff must be security conscious and take steps to protect themselves from identity theft, for example by restricting the amount of personal information that they give out. Social networking websites allow people to post detailed personal information such as date of birth, place of birth and favourite football team, which can form the basis of security questions and passwords. In addition staff should:

- Ensure that no information is made available that could provide a person with unauthorised access to The NLC, its systems and/or any confidential information; and
- Refrain from revealing any sensitive and/or confidential information regarding The NLC on any social networking website.

8.2.6 Recruitment

At no stage during the recruitment process will human resources or line managers conduct searches on prospective members of staff on social networking websites. This is in line with The NLC's equality and diversity policy.

8.3 Personal use of social networking sites

8.3.1 The NLC recognises that many members of staff use the internet for personal and recreational purposes outside working hours and that many staff participate in social networking.

8.3.2 The NLC permits employees to access social networking websites on the internet for personal use before and after work hours and during the one-hour break at lunch.

8.3.3 The NLC respects an employee's right to a private life and so long as their personal internet presence does not make any reference to The NLC and the organisation cannot be identified, the content is unlikely to be of concern to the organisation. However, the organisation must also ensure that its reputation and confidentiality are protected and therefore the following conditions apply:

- If employment at The NLC is referred to in any way then the information posted would need to comply with the conditions outlined in 8.2.
- Social media activities should not interfere with work commitments.
- Personal blogs should have clear disclaimers that the views expressed by the author in the blog are the author's alone and do not represent the views of The NLC.
- Staff with personal profiles that they use outside The NLC must remember that service *users* will be able to view their profile if it is set with public access. Staff must take steps to prevent themselves from revealing inappropriate or unprofessional information.

Return to top

9.0 Email

Electronic mail (email) provides an efficient method of conducting much of The NLC's business. All members of staff whose duties require it should have a The NLC-provided email account which is to be used for all email communications carried out on The NLC business.

9.1 Email best practice

Do:

- Proof-read emails before sending them to make sure your message is understandable and appropriate. Emails should be polite, to the point, and professional.
- Draft email correspondence with care to avoid any potential misinterpretation. For instance, consider whether you are at risk of causing offence or entering into a contract (intentionally or otherwise). It is almost impossible to stop an email once it has been sent, so check messages instead of regretting them later.
- Note that emails are admissible as evidence in legal proceedings and have been used successfully in court.
- Exercise extreme care when receiving emails with attachments from third parties, particularly unidentified third parties, as these may contain viruses.
- Avoid sending large files where possible. The use of appropriately licensed compression software (eg .zip files) is advised. Extremely large files should be sent by means other than email.
- Avoid 'Mail Storms' – long discussions sent to a distribution list – consider verbal communication instead.
- Report any virus incidents or apparent breaches of security immediately to the IT team. In order to ensure appropriate corrective action is taken, and no unnecessary panic is caused by hoaxes, do not taken it upon yourself to issue warnings to other employees.

Do not:

- Use email to transmit or solicit material that is defamatory, libellous, pornographic, obscene, hateful, harassing, threatening, discriminatory or otherwise illegal.
- Email material that incites criminal activity, or which may otherwise damage The NLC's reputation.
- Email material to which a *third party* holds an intellectual property right, without the express written permission of the right-holder. For instance, emailing an academic work which is protected by copyright.
- Email material that could be used in order to breach computer security, or to facilitate unauthorised entry into computer systems. This could be a password or link which provides access to The NLC systems.
- Send messages that could imply the creation of a contract without express authorisation.
- Send messages that contain adverse comments about a colleague or any person with whom you are working.
- Create email congestion by sending chain emails, trivial or unnecessary personal messages or by copying emails to those who do not need to see them.
- Send sensitive or emotional emails. If you are angry, re-read it after you have calmed down. Never draft an email solely using CAPITALS – use normal sentence case. WRITING SOLELY IN CAPITALS GIVES THE APPEARANCE OF SHOUTING.
- Impersonate any other person when using email or amend messages received.
- Knowingly allow anyone else to send email using your account. *Users* will be deemed liable for any email activity from their accounts.
- Send email to large numbers of people unless you are sure that it is directly relevant to their job. Sending unsolicited mail to many *users* ('spamming') is wasteful of user time and can disrupt the service, via performance delays, for other *users*.

Whilst The NLC provides staff with access to email systems for the conduct of The NLC-related business, incidental and occasional personal use of email is permitted so long as such use does not disrupt or distract the individual from the conduct of The NLC business (ie due to volume, frequency or time expended) or restrict the use of those services for other legitimate *users*.

9.2 Privacy and security

9.2.1 Email, like all methods of communication, cannot be assumed to be secure. It cannot be assumed that email will be correctly delivered or that the sender is as claimed in the mail headers. Steps must be taken to minimise the risk of interception or breaches of confidentiality. These steps include:

- Not divulging your user passwords to anyone (including in email)
- Not knowingly allowing anyone else to send email from your account

9.2.2 You should also consider the following guidelines when sending email:

- Ensuring that you identify and use the correct recipient email address
- Considering anonymising references to specific individuals
- Confirming the identity of an email sender where there is reason to question this
- Adopting a risk-based approach to deciding what information is appropriate to be sent by email.
- Mark sensitive information as "private and confidential".
- Remember that the recipient of an email may forward the message on to others.
- Do not forward emails which contain earlier emails without first ensuring that none of the earlier emails contain anything which would, justifiably, annoy a potential recipient, or does not contain confidential information.
- **Where an issue is particularly sensitive or confidential, email is unlikely to be a sufficiently secure method of communication and should be avoided.**

9.2.3 *Users* should be aware that deletion of an email message by both sender and receiver does not mean that the message no longer exists on their systems or on the systems through which it passed.

9.2.4 *Users* may not, under any circumstances, monitor, intercept or browse other *users*' email messages.

9.3 Managing your email account

- You should check your inbox regularly or ensure that someone else is able to check your inbox using delegated authority.
- Where appropriate, a manager may obtain access to an email account of a member of their team where that member is absent, to ensure that business correspondence is effectively dealt with.
- Ensure you utilise the 'Out of Office' assistant when you know you will be absent from work.
- You must delete emails on a daily basis from your inbox to prevent a build-up. A build up can prevent you from effectively monitoring and managing your emails.

10.0 External email accounts

- External email accounts are email accounts which are usually web-based eg Hotmail, Yahoo, Gmail. These accounts may not be secure as they bypass The NLC's external antivirus scanning systems. It should be noted that these external companies may retain a copy of the mail, over which The NLC has no control.
- You must not use external email accounts to transfer confidential information for home use.
- You must not use your 'Out of Office Assistant' to forward messages automatically to any external email system without the prior agreement of the IT team.

Return to top

11.0 Telephones

The NLC provides telephones (including mobile phones and PDAs) for its business. You may use The NLC's telephones for a reasonable level of short personal calls. The following behaviour may result in disciplinary action:

- Long telephone conversations except in exceptional circumstances. If you think you may need to make an urgent long telephone call you should seek permission first from your line manager;
- Continued excessive use of The NLC's telephones even for short personal calls;
- Overseas calls, other than for The NLC's business; and
- Calls to premium rate numbers.

Personal calls should be kept to a minimum since the The NLC telephone lines should be kept clear for business calls.

Return to top

12.0 Mobile and Remote Working

12.1 Risks of mobile and remote working

12.1.1 The NLC information that is held or processed on systems outside of The NLC premises is generally more exposed to being compromised, corrupted or lost than information that is held or processed on systems within The NLC premises. This is down to various factors including:

- Portable devices may be stolen, lost or left on public transport;
- When used in public, data displayed on laptop computers may be subject to viewing by unauthorised persons;
- Physical security in the home may be lower than that of The NLC premises, and some domestic properties may be more prone to burglary resulting in the theft of laptops and *PCs*;
- Data is likely to remain on mobile or remote systems after accessing The NLC systems without some *users* being aware (ie cached web pages and email attachments);
- The NLC has no jurisdiction over who can use privately owned equipment, and when this has been used to access The NLC information, data may be available to be viewed by unauthorised persons;
- The security of machines outside The NLC premises in terms of security patching and virus protection may be lower than those within The NLC and exposure to hacking attaches and virus contamination may be higher;

- Unserviceable privately owned equipment containing The NLC data is likely to be repaired through commercial arrangements where data may be viewed by repair staff during that process.

12.1.2 Although technical controls provide an essential element of protection, these only deliver a percentage of the required protection; the most effective defence is awareness and good working practices.

12.2 Remote Access Service

12.2.1 Microsoft Remote Desktop is The NLC's remote and mobile access service. It is compatible with Microsoft and Apple systems and can be used wherever internet connectivity is available.

12.2.2 Microsoft Remote Desktop provides the means for *users* to access systems and data remotely in a secure and controlled way which minimises risk. It also prevents shared files being lost through the transfer of data between their storage facility and remote computers. When one user has accessed a shared document, anyone else trying to access it at the same time is informed that it is in use, and they will be granted read-only access to it.

12.2.3 In theory, any user with a valid The NLC computer account can be set up to access The NLC systems remotely via Microsoft Remote Desktop. However, as there is a cost attached to each new license, authorisation must first be obtained from your line manager. They will assess whether or not you have a genuine need to access The NLC systems remotely.

12.2.4 Alternatively, anyone who simply needs to access their email is permitted to use The NLC's Outlook Web Access facility, which is independent of Microsoft Remote Desktop. Access details can be obtained from the IT team. However, please be aware that this service does not offer the same security features as Microsoft Remote Desktop. Common sense must be applied to maintain the security of documents and it must not be used to access or detach confidential attachments as this information will be cached locally on the machine from which the access is made.

12.3 Remote Workers' Responsibilities

12.3.1 Remote workers must be familiar with their responsibilities under the Data Protection Act.

12.3.2 Remote workers are responsible for the safekeeping and protection of The NLC mobile devices that have been issued or loaned to them. They must prevent unauthorised persons from using them and they must not loan them to others without prior authorisation.

12.3.3 *Users* of privately-owned computers that are, or have been, used to create, process, store or access The NLC data are responsible for ensuring that non-members of The NLC do not gain access to that data when using their computers.

12.3.4 Remote connections to any The NLC IT services are subject to the same rules and regulations, policies and practices as they would be if they were physically on The NLC premises.

12.3.5 Remote workers are to take heed of the environment in which they are working and apply appropriate common-sense measures to protect The NLC-owned mobile devices and The NLC data on both The NLC-owned and privately-owned devices.

12.4 Mobile Working on The NLC Premises

12.4.1 The NLC mobile devices are not to be left unattended on The NLC's premises unless they are in a locked room or cupboard, with access restricted to local staff, or secured by an appropriate security device.

12.5 Mobile Working outside The NLC Premises

12.5.1 When working outside The NLC's premises, mobile workers are to be extra vigilant and apply appropriate precautions to protect portable computers in their care.

12.6 Working in Transit

12.6.1 Extra care must be taken when working in transit to prevent the disclosure or compromise of The NLC information. Any unauthorised disclosure of personal information due to negligence on a user's part could make that user liable to prosecution under the Data Protection Act 1998 (or other legislation).

12.6.2 Sensitive information must also be safeguarded against being viewed by unauthorised persons and must not be accessed or processed in public places where it could be overlooked by anyone who is not authorised to view it.

12.7 Transporting Laptops and Portable Devices

12.7.1 Constant vigilance must be applied to reduce the possibility of loss or theft of The NLC mobile devices, or the disclosure of The NLC information on either The NLC portable devices, or privately-owned equipment, whilst in transit.

12.7.2 In a bid to reduce the chance of being 'mugged', those carrying laptop computers in public places may prefer to use bags other than those provided with the equipment, so that it is not obvious that they are carrying a valuable piece of equipment. However, in making this decision, the risk of damaging the laptop if it is accidentally dropped whilst not in its proper carrying case should be taken into account.

12.8 Data Backup

12.8.1 All remote *users* are personally responsible for ensuring that any The NLC data on their machines (whether The NLC-owned or privately-owned) is regularly and frequently backed up and that backup media is handled and stored in accordance with IT guidelines.

12.9 Security of equipment in the home and the protection of data

12.9.1 *Users*, who access, produce or store The NLC information on privately owned computer equipment, whether portable or static, are responsible for the security of them. In order to protect The NLC information, such machines are to be protected by a firewall, operate anti-virus software, and be kept up to date with security patches.

12.9.2 You should take all reasonable steps to minimise the visibility of computer equipment from outside the home, and to secure windows and doors when the home is unoccupied.

12.9.3 Person identifiable data files must not be sent via email to a user's home mail box. The Information (Data Protection) Commissioner has advised that Internet mail is not secure and should not be used to transmit confidential information.

12.9.4 You should secure confidential data or reports that you are not actively using in the most secure area of your home.

12.9.5 All electronic files used at home *must* be protected at least by file level password control.

12.10 Incident reporting

12.10.1The loss of any The NLC-owned information must be reported to the respective line manager and, where applicable, the IT team.

Return to top

13.0 Mobile Devices

The NLC permits the usage of mobile devices, including but not limited to, Personal Digital Assistants (PDAs), tablets, Smartphones, mobile phones and BlackBerries, to carry out The NLC's business. Portable media can be a very useful resource if used appropriately, but care needs to be taken over their use, and of the data that they hold.

13.1 Issue of mobile devices

13.1.1 All mobile devices for authorised The NLC business are provided by the IT department, who keep an inventory of all such devices. Staff must sign to accept terms and conditions.

13.1.2 All The NLC supplied mobile devices and their contents remain the property of The NLC and are subject to regular audit and monitoring.

13.2 Security of Hardware

13.2.1 *Users* must be aware that the device contains The NLC data, and take appropriate action to protect the device from being lost or stolen. The guidelines outlined in section 12 must be followed.

13.3 Security of Data

13.3.1 Only devices from approved suppliers should be attached to the The NLC data network either directly or through a The NLC PC or laptop. This should ensure that appropriate security controls have been built into the implementation.

13.3.2 Once received, the user is not authorised to change any security device settings without reference to the IT team, as they may affect the security of the device, or stop it functioning with the supplied service. (This does not apply to resetting the PIN).

13.3.3 Minimum security requirements for the most common types of portable device are detailed in Annex C. Please seek advice from IT if necessary.

13.3.4 If a The NLC owned device is lost or stolen, then IT should be contacted as a matter of urgency, so that the The NLC data network can be protected from the device.

13.3.7 Only applications provided with the device, or provided/approved by The NLC can be run.

13.4 Personal Devices

13.4.1 Personal mobile phones with cameras and personal digital cameras are permitted in the office but must not be used to collect and store data that belongs to The NLC.

Return to top

14.0 Confidentiality

- Generally, confidential information includes any information which is not available to the public. It includes information which would damage the business of The NLC if it became known to those outside the organisation. It may also include the information of third parties who are providing services or working in partnership with The NLC. This also covers information where it is confidential internally, such as appraisals etc.
- It is important that you take all necessary measures to maintain the confidentiality of information that is transmitted or contained in The NLC Equipment including through using encryption and ensuring the security of hardware (including laptops). Contact the IT department for details of how to do this.
- You should limit the number of people to whom you send confidential information to only those with a genuine need to know.
- You should label confidential communications as "CONFIDENTIAL" and state explicitly how you expect the recipients to deal with this information.
- You must never post confidential or sensitive The NLC information on any internet site, including social networking sites (eg Facebook).
- Before sending confidential information by email, consider sending it by internal post or courier instead.

Return to top

15.0 Data Protection

15.1 Data Protection Principles

All staff must follow these principles when processing and storing data concerning individuals, whether this is processed and stored in electronic format or in paper form:

- All information covering personal data must be obtained and processed both fairly and lawfully; and in most circumstances the consent of the data subject must first be obtained, usually in writing
- Personal data shall be held only for one or more specified and lawful purposes
- Personal data held for any specified purposes must not be used or disclosed in any manner incompatible with those purposes
- Personal data held for any specified purposes must be adequate, relevant and not excessive in relation to that those purposes
- Personal data held must be kept accurate and up to date
- Personal data held for any specified purposes must not be kept for any longer than is absolutely necessary for those purposes
- Adequate security measures must be taken against unauthorised access to, alteration of, or disclosure or deliberate destruction of, personal data as well as against accidental loss or destruction of personal data

Staff must follow these principles in processing administrative data:

- Staff should ensure that dissemination of information by phone, fax, e-mail, printed materials or any other means occurs only to those approved or entitled to receive the data
- Confidential or sensitive information contained on printouts must be shredded after use, unless filed securely in locked cabinets or storage rooms
- Storage of non-electronic forms of confidential or sensitive information must be safeguarded against unauthorised viewing as well as against accidental loss
- Data storage on tapes, CD, DVD, USB or other computer-related media should involve the latest back-up copy being stored off The NLC's premises by the designated staff responsible for the security of that data

15.2 Privacy Notices

As an organisation, not only are we responsible for ensuring that we process all personal information fairly and lawfully, according to the principles outlined above; we must also make information readily available to the data subject on our data handling processes. In particular, we must provide information on:

- Who we are;
- The purpose for which we are processing someone's information;
- Any other information that the individual may reasonably need to know in regard to the use of their data.

Best practice for meeting this requirement is the application of a 'privacy notice' to all data collection media, eg application forms, the website, and leaflets for service provision. This is particularly vital where:

- You are collecting sensitive information; or
- The intended use of the information is likely to be unexpected or objectionable; or
- Providing personal information, or failing to do so, will have a significant effect on the individual; or
- The information will be shared with another organisation in a way that wouldn't be expected.

Privacy notices must be clear and honest, and appropriate to the level of understanding of your intended audience (particularly in the case of children and young people). A sample privacy notice can be found at Annex E. Clearly it would not be practical to include so much information on, for example, a leaflet or small advert, but where you are requesting personal information, individuals must be aware that they can access this information. In this situation, consideration could be given to including a link to a privacy notice on the website, or explaining it orally.

Guidance on drafting privacy notices can be found on the Information Commissioner's Office (ICO) website: http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/privacy_notices.aspx. Alternatively, support may be sought from human resources.

Return to top

16.0 Defamation

- Defamation is the publication of a statement that adversely affects the reputation of a person or an organisation. Publication can be by way of the internet or by email.
- You must not send or circulate, internally or externally, any information that is defamatory. In particular, you must not send or circulate, internally or externally, any information that contains negative comments about an individual or organisation without first checking that the contents of the information are accurate.
- A person or organisation defamed can sue you or The NLC for damages. Although the law recognises that it is a defence if the information is 'true', the onus is on you or The NLC to prove that.

Return to top

17.0 Copyright

- The owner of copyright has the exclusive rights in certain works such as documents, articles and books, so that they cannot be copied or used in certain ways without the consent of the copyright owner.
- You must not download, store, copy or transmit to third parties the works of others without their permission as this may infringe copyright. Copyright is most likely to be breached when you download material from the internet or copy text and attach it to an email message.
- You should note that you infringe someone's copyright where you use either the whole or a substantial part of their work without permission, subject to certain exceptions.

Return to top

18.0 Harassment

- All The NLC staff must be allowed to work in an environment free from harassment of any kind. This includes (but is not limited to) sexual and racial harassment and harassment on the ground of sexual orientation, age, religion, disability and marital status. Harassment affects morale and prevents a person fulfilling their full potential in their work.
- Sexual harassment is unwanted conduct of a sexual nature, or other conduct based on sex affecting the dignity of men and women at work. In the context of this policy this includes sending messages with sexually suggestive material, sexual propositions or abuse of a sexual nature.
- Racial harassment is unwanted conduct based on race, colour, ethnic or national origin affecting the dignity of men and women at work. In the context of this policy this includes sending messages containing offensive insults or 'jokes' based on race and abuse of a racial nature.
- You must not send messages which contain sexual or racist material or which are otherwise abusive or could constitute harassment on any other ground. It is important to note that the recipient may determine what is and is not offensive.
- Harassment is a criminal offence for which the harasser could be imprisoned. Victims of harassment may be able to claim damages from the harasser and The NLC.

Return to top

19.0 Breach of this policy and applicable laws

The NLC reserves the right to implement appropriate disciplinary measures against you in response to any breach of this policy.

Further, as mentioned above, some breaches of this policy may also be illegal. For instance:

- If you knowingly or recklessly obtain or disclose personal information without The NLC's consent, you may be guilty of an offence under the Data Protection Act 1998;
- If you introduce viruses into The NLC equipment, you may be guilty of an offence under the Computer Misuse Act 1998; and
- If you use someone else's copyright protected material without their consent, you may be guilty of an offence under the Copyright, Designs and Patents Act 1988.
- You must comply with the rules under all relevant legislation.

Return to top

20.0 Monitoring

20.1 Why does The NLC monitor communications?

The NLC is ultimately responsible for all business communications but will, as far as possible and appropriate, respect your privacy while you work. It is important, however, that you understand that The NLC may monitor your communications and use of The NLC equipment for reasons which include:

- ensuring that The NLC's procedures and policies are adhered to;
- monitoring standards of service and staff performance;
- record keeping;
- preventing or detecting unauthorised use of The NLC equipment and systems, including compliance with this policy;
- complying with legal obligations and preventing and detecting criminal activities; and
- maintaining the effective operation of The NLC's communications systems.

20.2 What does The NLC monitor?

The NLC may monitor telephone, email and internet traffic data (ie sender, receiver, subject, attachments to emails, numbers called and duration of calls and files downloaded from the internet) at a network level (covering personal and business communications). The NLC may also monitor the content of communications where it appears to the organisation that the use of The NLC equipment is being abused or used inappropriately

A manager may monitor the emails received by a member of his or her team when that member is absent to ensure business correspondence is dealt with.

You should be aware that this monitoring may reveal personal information about you, for instance which websites you visit, the identity of people you email for personal reasons etc.

20.3 How does The NLC monitor?

- Pro-actively – when they investigate a person's online actions as part of an ongoing investigation. Before beginning to monitor, they will go through a number of processes to ensure that the steps taken are reasonable and proportionate.
- Monitoring of past communications – this is an examination/analysis of past communication that can be done as part of an ongoing investigation or randomly eg it may be necessary to perform a check on bandwidth use. If one user has a high level of bandwidth use, The NLC may investigate further.

The NLC may use any information it receives via this monitoring process to investigate any claims of breach of this policy or any law and to instigate appropriate disciplinary or legal proceedings.

20.4 Who monitors and what is done with information elicited from monitoring?

It is the responsibility of the IT department, at the request of the Head of IT, to carry out monitoring to prevent or detect unauthorised use of The NLC Equipment and systems, compliance with legal obligations, and preventing and detecting criminal activities.

The NLC will only disclose information obtained through monitoring to:

- A relevant external agency if required by law; or
- To those directing the investigation ie The NLC management or human resources, for the purposes of criminal, civil or disciplinary purposes.

20.5 How long is monitoring data held?

Information obtained through monitoring will only be held for as long as it is necessary to complete enquiries. Where information is part of disciplinary proceedings, the information will be kept in accordance with the retention period for such proceedings.

20.6 Will I know if I am being monitored?

Wherever reasonable The NLC will consult with you about any suspected breach of this policy before any action is taken against you. However, it may not be practical to consult with you beforehand where illegal behaviour or gross misconduct is suspected.

Return to top

21.0 Questions

If you have any questions about this policy please contact the Head of IT or the Head of Human Resources.

Return to top

22.0 Associated policies, procedures, standards and guidance notes

- Disciplinary policy and procedure
- Bullying and harassment policy
- Equality and diversity policy
- Data protection policy
- Retention of data policy
- Open information policy
- Safeguarding policy
- Business continuity plan
- Health and safety policy

Return to top

Appendix A: Glossary of Terms

Availability	Having complete access to *Information assets* as and when required.
Business Continuity Strategy	Strategy through which single or multiple operations are restored and sustained following unforeseen events that disrupt normal functions.
Confidentiality	The restriction of information to those persons who are authorised to receive it.
Critical systems	Systems that hold or process *key data.*
Information assets	All data, hard copy documentation, hardware, software and services, network infrastructures, Internet gateways, systems documentation, physical environments, support functions and business continuity plans used throughout the organisation, regardless of location.
Information security	Security measures designed to preserve the confidentiality, *integrity* and *availability* of information.
Information security Awareness	*Users*' awareness of their *information security* responsibilities.
IT/IS	The components of computer equipment, software, communications facilities and manual procedures organised to capture, process and output data, and to provide *Information* in support of operations.
Integrity	The completeness and preservation of information in its original and intended form unless amended or deleted by authorised people or processes.
Key data	Data that is critical to the functioning of the organisation, or sensitive, or which The NLC is obliged under law to maintain, and any other data that could harm the organisation if compromised.
Key information	*Key data* that is in hard copy format.
Networked services	Computers and other peripherals connected by a high-speed link that enables many *users* to share the facilities.
PCs	Personal Computers including desktop and laptop computers, which may or may not be connected to *networked services.* In this context all personal computers are included regardless of operating systems and applications used on them.
Protectively marked	Marking applied to information medium that indicates that the information within the medium warrants special handling and protection.
Security incident	An actual or suspected event or series of events that could threaten the confidentiality, *integrity* and *availability* of information.
Sensitive operations	Operations that are associated with *key data* and information where this is regarded as being confidential.
Third party	In the context of this policy, a *third party* is an individual or an organisation that is contracted to work for or on behalf of The NLC, either from within The NLC premises or remotely, and who requires access to The NLC *IT/IS* systems, data or information.
Users	Those to whom this policy applies, ie • All full-time, part-time and temporary staff employed by, or working for or on behalf of The NLC. • All volunteers, students and interns based at The NLC. • Contractors, associates and consultants working for or on behalf of The NLC. • All other individuals and groups who have been granted access to The NLC IS/IT systems and/or *Key data* and *Information.*

Return to top

Appendix B: New IT User Access Request Form

New IT User Access Request Form

This form is to be completed by line managers prior to a new member of staff joining the organisation. The completed form will enable IT to provide your new starter with the appropriate IT equipment, software and access rights, helping to make their first day run smoothly.

1. Personal details of new user	
Full name:	
Start date:	
Job title (specify if sessional / volunteer / student / associate etc.):	
Project / Service:	
Primary location (where will their main office be?):	
Line manager:	

2. Email Access	
Create a new email account for this individual:	☐ Yes ☐ No*
*If no, please provide existing email account:	

3. Printer Access	
User should have same access to departmental networked printers as the rest of the office:	☐ Yes ☐ No
Special instructions, if any:	

4. Hardware Requirements			
This user requires the following hardware (in addition to The NLC equipment already available):			
☐ PC	☐ Laptop	☐ Tablet	☐ Mobile phone
Other (please specify):			

5. Software Requirements (NB each additional software licence carries an additional cost which will be charged to your project).	
This user requires specialist software (eg Adobe Acrobat Professional, Microsoft Remote Desktop):	☐ Yes* ☐ No
*If yes, please give details:	

6. Access Requirements

This user requires access to the following folders on the 'network:' Drive (please insert all that apply):			
☐ Other (please specify):			

7. Authorisation (must be signed by line manager)

I confirm that the above-named user requires the outlined equipment and access rights to carry out their role. I will notify IT immediately of any changes.	
Signature:	Date:

Please return this form to the IT department:
TISL, 5 David Mews, LONDON SE10 8NJ

IT Use only	**Sign**	**Date**
Form received:		
Actioned:		
Line manager informed:		
Copy of form sent to HR:		

Return to top

Appendix C: Authorised Device and Controls Table

Please ensure that your devices are configured as below:

Approved Device	Security Requirement
Mobile Phone (including camera phones)	PIN, locked whilst not in use.
USB memory stick	Encrypted if confidential information stored. If the stick has the capability of password or PIN control, the password or PIN should be lodged with your line manager to ensure the ability to retrieve The NLC content should the need arise.
Personal Digital Assistant (PDA), Tablets and Smartphones	PIN (mandatory for phone functions) and password (if available). A 4-digit PIN is the minimum acceptable security measure. Where The NLC confidential data is stored on a PDA it is required that The NLC Anti-Virus (AV) software is also used. If the device is non- The NLC owned, the user must purchase and run a suitable AV solution.
CD/DVD/BluRay	Files should be password protected (if supported by the hardware), once used, data should be removed from CD/DVD/Blu-Ray and CD/DVD/Blu-Ray disposed of appropriately if a rewriteable disk, if not destroyed. Data that is not deemed The NLC specific (deemed suitable for complete public consumption) may be stored unprotected on the disk. Where data is required to be stored on this media for archive/reference purposes, adequate care must be taken to ensure this data does not get disclosed to unauthorised individuals.
Tape	Files should be password protected (if supported by the hardware), once used, data should be removed from tape and tape disposed of appropriately. Where data is required to be stored on this media for archive/reference purposes, adequate care must be taken to ensure this data does not get disclosed to unauthorised individuals.
Other Removable Media	Files should be password protected (if supported by the hardware), once used, data should be removed from the disk and the disk disposed of appropriately. Data that is not deemed The NLC specific (deemed suitable for complete public consumption) may be stored unprotected on the disk. Where data is required to be stored on this media for archive/reference purposes, adequate care must be taken to ensure this data does not get disclosed to unauthorised individuals.

Return to top

Appendix D: Sample Privacy Statement

Website Privacy Policy

General

The NLC respects your privacy and realises how important it is to you that your personal information remains secure. This statement describes how The NLC collects and uses information about people who visit our website. If you have any questions about this statement please contact the The NLC Data Protection Officer.

Your personal data is protected by UK legislation, specifically the Data Protection Act 1998, and the Privacy and Electronic Communications (EC Directive) 2003. We aim to exceed our legal obligations by following best practice and reviewing our procedures regularly.

The NLC is registered as a data controller with the Information Commissioner for the United Kingdom for those purposes for which personal information is collected on this website.

What information does The NLC collect about me and how is it obtained?

You may at times be asked to supply personal information via the The NLC website. Personal information is anything that enables us to identify you in some way, such as your name and email address. For instance, we may collect personal information from you when you complete online forms as part of communicating with The NLC (eg signing up for The NLC events or enquiring about our services), subscribe to our newsletter, make a donation to us or otherwise provide us with personal information. The NLC will only collect personal information when you specifically and knowingly provide it to us.

If you supply such information, we are legally bound by the Data Protection Act 1998 to ensure that such information is only used for the purpose for which it was requested and also to ensure that the data is held securely.

How does The NLC use my information?

We will use your personal information to provide you with the services, products or information you have requested, for administration purposes and to further our charitable aims, including for fundraising activities.

Where stated we may use the personal information you provide to contact you in future about The NLC work. The information which we collect in this way will typically include your name, postal and email addresses, and your bank details if you are supporting us financially. If you do not want this to happen please tick the appropriate box provided.

How secure is the information which I give to The NLC?

The NLC takes the care of your data seriously and undertakes to protect your personal information in a range of ways. In order to prevent unauthorised access or disclosure, we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information we collect online. These measures include the use of secure servers, firewalls and SSL encryption. We follow payment card industry (PCI) security compliance guidelines when processing credit card payments.

However, please be aware that the transmission of information over the Internet is never 100% secure so, while we try to protect your personal information, we can't guarantee the security of any information you submit to us via our website.

How does The NLC use 'Cookies'?

A cookie is a small file which asks permission to be placed on your computer's hard drive. Once you agree, the file is added and the cookie helps analyse web traffic or lets you know when you visit a particular site. Cookies allow web applications to respond to you as an individual. The web application can tailor its operations to your needs, likes and dislikes by gathering and remembering information about your preferences.

We use traffic log cookies to identify which pages are being used. This helps us analyse data about web page traffic and improve our website in order to make sure that the site reflects your needs. We only use this information for statistical analysis purposes and then the data is removed from the system.

Overall, cookies help us provide you with a better website, by enabling us to monitor which pages you find useful and which you do not. A cookie in no way gives us access to your computer or any information about you, other than the data you choose to share with us.

You can choose to accept or decline cookies. Most web browsers automatically accept cookies, but you can usually modify your browser settings to decline cookies if you prefer. If you want to prevent our cookies being stored on your computer in future, you may do so by referring to your internet browser's instructions. You can do this by clicking on the "Help" menu. Please note, however, that if you disable our cookies you may not be able to access certain services or facilities on our site and your use of our site may be restricted. Further information on deleting or controlling cookies is available at www.aboutcookies.org.

What about links to other websites?

Our website may contain links to other websites of interest. However, once you have used these links to leave our site, you should note that we do not have any control over that other website. Therefore, we cannot be responsible for the protection and privacy of any information which you provide whilst visiting such sites and such sites are not governed by this privacy statement. You should exercise caution and look at the privacy statement applicable to the website in question.

Does The NLC share my information with anyone else?

We will not sell, distribute or lease your personal information to third parties unless we have your permission or are required to do so by law. We do sometimes ask third party organisations to contact you on our behalf as part of fundraising activities, but the information gathered in this way remains our legal responsibility and we ensure that data is treated with the same level of care as if we were handling it directly.

How can I access the information that The NLC holds about me?

You have the right to ask for a copy of the information we hold about you (for which we may charge a small fee) and to have any inaccuracies in your information corrected. If you wish to exercise these rights, please write to us or email us at dataprotection@nlc.org.uk

We aim to issue an initial response to all enquiries within five working days, and will offer a full response to all information access requests within forty working days of receipt. It will help us locate your records more easily if you can tell us something about the nature of your contact with The NLC.

How can I make changes to the information that The NLC holds about me?

If your personal details change, please help us to keep your information up to date by notifying us at the above address. It will help us to update your information quickly if you include your full name and address and/or supporter number (if known), together with details of the correction to be made.

How long will The NLC keep my information?

We will retain your information for as long as you have an active relationship with The NLC. If you cease to have an active relationship with us or request to receive no further contact, we may retain some basic information in order to avoid sending you unwanted materials in the future, and to ensure that we don't accidentally duplicate information.

What if I want to limit or stop receiving messages from The NLC?

If you wish to receive no further information from us, at any point in time, this can be done via the above postal or email address.

You may choose to restrict the collection or use of your personal information by following the opt-out instructions on any online form or email you might receive from us. If you have previously agreed to us using your personal information for direct marketing purposes, you may change your mind at any time by writing to our General Data Protection Officer at the above address or emailing us at dataprotection@nlc.org.uk.

Your consent

By providing us with your personal information you consent to the collection and use of that information for the purposes and in the manner described in this Privacy Policy.

We reserve the right to amend this privacy statement. The latest version will be available on our website so please check from time to time. By continuing to use this website you will be deemed to have accepted any changes.

Any alterations to our policy on the collection or use of data will be posted on this website.

Last updated: November 2017

Return to top