Information Governance Framework

Schedule 02A

Information and ICT Security Policy

North Lincolnshire Council

www.northlincs.gov.uk

Background Information	
Document Purpose and Subject	To provide a council-wide policy for Information and ICT Security.
Author	Information Governance Team.
Document Owner	Information Governance Team.
Change History	V4.4 – The policy has been amended to reflect the UK GDPR that has applied since 01 January 2021. The Policy has also been updated to replace section 4.0 'Keep it Secure' with the 2021 version that takes account of updated guidance and the content of the Digital Technologies Policy since its move into the IG Framework from the HR Manual. The policy has been amended throughout to become the Information and ICT Security Policy rather than just the Information Security Policy. ICT Security was part of the ICT shared service with NELC and this change reflects the move of this function be NLC only. The policy has been amended to be applicable to North Lincolnshire Clinical Commissioning Group (NL CCG).
File Location	Information Governance Team Shared Storage Area
Retention Period	Permanent Preservation as a Core Policy
Issue Date	……..2021
Last Review	January 2020
Current Review	May 2021
Next Review Date	March 2022
Approved By	Cabinet Member
Approval Date	……..2021

Contents

1. Introduction

Information is an important and valuable business asset that needs to be suitably protected from a wide range of threats such as malicious software, unauthorised access, computer misuse, information technology failures, human error and physical security threats, to ensure citizen's information is handled appropriately, maintain business continuity and minimise business damage.

Information Security may be characterised as the preservation of:

- **Confidentiality**: making sure that information is accessible only to those who need to know and are authorised to have access.
- **Integrity**: safeguarding the accuracy and completeness of information and processing methods; and
- **Availability**: making sure that only authorised users have access to information when required on a need-to-know and have basis.

Without adequate levels of protection there is an impact on the council's ability to fulfil its obligations including the provision of services and meeting legal and statutory requirements.

This policy is part of a suite of Information Governance policies and procedures and should be read in conjunction with the Information Governance Framework and other supporting guidance documents including:

- Council's Code of Conduct,
- Information Security Incident and Data Breach Policy, and
- Digital Technologies Policy.

Any breaches of this policy may lead to action being taken in accordance with the council's Disciplinary procedure.

This policy will be reviewed regularly to ensure that it remains relevant and also that any new digital technologies are included as appropriate.

2. Scope

This policy applies to all council employees, North Lincolnshire Clinical Commissioning Group (NL CCG) and all individuals or organisations acting on behalf of the council.

This policy is also aligned with the requirements for PSN Code of Connection, Information Security Management: Code of Practice for NHS organisations and NHS Data Security Protection Toolkit.

This policy applies to all information assets held by or on behalf of the council irrespective of their format and covers all locations which information is taken and/or accessed.

Schools, who are Data Controllers in their own right, may choose to adopt this policy but where this is not the case it is expected that they will have their own appropriate policy.

3. General Guidance

Employee's use of digital technologies will be monitored where necessary and reasonable, including anything created, stored, sent, or received when using the council's digital technologies.

When using the council's digital technologies, you must:

- Not give your passwords to any other person.
- Protect all information and ICT equipment in your custody.
- Only use corporately managed equipment provided by ICT and not personally owned equipment or non-council applications (i.e. employee's own laptop, computer or personal email), unless these have been approved by ICT Services;

Employees must inform the Information Governance Team of all Information Security Incidents and the ICT Solution Centre of any ICT Security Incidents.

Please see the Information Security Incident and Data Breach Policy for further information.

Please see the council's Digital Technologies Policy for further detail on the use of digital technologies.

Please direct any questions about the information in this booklet to the Information Governance Team using the following email – informationgovernanceteam@northlincs.gov.uk

4. Information and ICT Security Guidance

4.1. Introduction

Information is a valuable key council asset. It is the responsibility of all employees who access or use information to do so responsibly and so they comply with legislation, such as the UK General Data Protection Regulation / Data Protection Act 2018, the Freedom of Information Act 2000 and Environmental Information Regulations 2004. Information Governance (IG) is the overarching term used to cover all elements of managing information.

This policy summarises the Information Governance requirements that must be complied with by everyone and supports the mandatory Information Governance and UK GDPR training and awareness raising procedures in place.

Employees not complying with Information Governance requirements could face disciplinary action and in serious cases they could potentially face action including criminal proceedings and an unlimited fine. Non-compliance could also result in the council being fined up to a figure of approximately £18 million by the Information Commissioner's Office (ICO) and damage to reputation. The ICO is the regulator of the UK General Data Protection Regulation / Data Protection Act 2018.

All employees with ICT access must undertake the council's mandatory Information Governance and UK GDPR e-learning package and the PurplePhish User Awareness and Education. For non-ICT users, the equivalent mandatory 'Keep it Safe' booklet training must be regularly read and understood. Managers will ensure this is part of the induction of any new employees.

4.2. UK General Data Protection Regulation/Data Protection Act 2018

The UK General Data Protection Regulation / Data Protection Act 2018 sets out how organisations such as the council must look after personal information and gives everyone various rights in relation to their personal data, including the right to request access to their personal information, to ask that inaccurate information is corrected or to ask for their information to be erased. Personal information is that which could identify someone. The Data Protection and Confidentiality Policy provides more detail.

Every employee is responsible for making sure that the personal information they use and access at the council is managed in accordance with the seven principles of the UK General Data Protection Regulation that require personal information to be:

1. Processed lawfully, fairly and in a transparent manner.
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.
3. Adequate, relevant and limited to what is necessary.
4. Accurate and where necessary kept up to date.
5. Kept in a form that permits identification of data subjects for no longer than is necessary, and
6. Processed in a manner that ensures appropriate security.
7. To comply with the accountability requirements the council must meet.

Organisations such as the council must demonstrate compliance with the UK General Data Protection Regulation as required by principle 7. This is the responsibility of the Information Governance Team.

The Data Protection Act 2018 sets out the Data Protection framework in the UK, alongside the UK General Data Protection Regulation. It contains three separate Data Protection regimes:

- Part 2 – sets out the general processing regime (UK GDPR), including setting out exemptions from compliance with the General Data Protection Regulation.
- Part 3 – sets out a separate regime for law enforcement authorities.
- Part 4 – sets out a separate regime for the three intelligence services.

4.3. Incident Management

Reporting concerns

If you become aware of or suspect that an information security incident or a potential data breach has occurred, you must report it immediately to the Information Governance Team and to a manager. ICT Security Incidents must also be reported to the ICT Solution Centre.

See the Information Security Incident and Data Breach Policy in the Information Governance Knowledge Base on Top Desk for details about how to report an incident.

All NELC CCG information security incidents must be reported through the CCG Incident App in the first instance.

It is important that any incidents are appropriately dealt with as soon as possible to limit the escalation of the incident and to minimise the distress of those affected. The Data Protection Officer must report serious incidents to the Information Commissioner's Office (ICO) within 72 hours.

You must not attempt to resolve a security incident or potential data breach yourself.

4.4. Good Information Handling Management

Not leaving things unattended

Information must not be left unattended in areas where there is public access or where employees could see it who have no right to see it. Take care at the end of meetings to ensure no confidential papers are left behind.

Mobile phones can contain personal information and have their call histories compromised and therefore must be always kept secure and not left unattended.

Keys and access cards must not be left unattended as they can give intruders or other employee's access to restricted areas, they are not authorised to be in.

Clear desks

Desks must be cleared at the end of each working day or when the desk is unoccupied and any information that needs to be protected must be locked away. Employees should also take care to protect information whilst they are working so that it is not seen by others who should not see it.

To minimise the risk of mixing up information and accidentally releasing it to someone who should not see it, only information relating to the current task should be on the working area of the desk at any one time.

Laptops must also be locked away overnight or taken home and locked away or stored out of sight within the home.

When leaving desks for long periods, users must ensure they are logged off the network and the computer switched off to ensure the computer's encryption is activated.

Photocopiers / Printers / Scanners/ MFDs

Care should be taken not to leave documents behind, particularly when they are on the glass and not visible. When sending work to devices that are not pass card or key code controlled, care must be taken not to leave information unattended.

When collecting printed documents, a check should be made to ensure all pages are present and correct to avoid leaving behind any information in the document handler or potentially jammed in the device and to ensure someone else's information is not mixed up with yours or printed on the reverse of your information.

Care must be taken to ensure documents are printed single sided when this is necessary, to prevent information about another individual being printed on the reverse in error.

When using auto enveloping a check should be made to make sure the process is working correctly including that there are the correct number of letters in envelopes and that single sided printing has been engaged where necessary.

Where a team has rules stating that only specified printers can be used to print personal or confidential information these rules must be abided by.

Any documents left unattended should be returned to the appropriate person. If it is not possible to identify the employee, the documents should be securely disposed of.

Whiteboards

Be wary of what could be revealed by information left on a whiteboard. Whiteboards used in meeting spaces must be cleaned at the end of the session.

Locking screens

Before leaving a computer unattended for any reason, even if left for a short period of time, i.e. to make a drink or take a comfort break the screen must be locked, by using **Ctrl+Alt+Delete** and then selecting the option to **'Lock Computer'.**

Computer screens should be turned away from windows where they could be seen by others. Use a protective covering, to prevent personal and/or confidential information being seen by those who should not see it. Protective covers for computer screens can be ordered from ICT Services. When installed these must be checked to ensure information is protected from view.

Transporting data and equipment off site

Personal or confidential paper information should not be taken off site unless this is unavoidable, as records are at the biggest risk of loss or theft when transported outside the work environment. Always consider if the information can be summarised or anonymised to minimise the personal or confidential information being taken out of the secure office environment or whether the information could be taken on a council laptop that has encryption.

If paper records do need to be taken off site, they should be placed in a suitable container or bag that prevents others from reading the information and is strong enough for the task. The same applies to laptops and other equipment.

If paper records, laptops or other equipment are to be carried in a vehicle they must be placed out of sight and in the boot if the vehicle needs to be left unattended. Records and equipment must not be left in a vehicle overnight.

Paper records must be stored separately from computer equipment as the computer is likely to be more attractive to a thief.

A log should be considered of what personal or sensitive paper records have been taken off site and where they have been taken.

Buildings / offices

Carefully consider the position of desks, furniture and visual display boards to prevent sensitive information being visible to unauthorised people.

Maintain the security of buildings at all times especially when the building is vulnerable, such as during building works and following evacuations. Only allow authorised access upon re-entry. Access to the secure working areas of the Council's premises is controlled by fob, keypad or proximity card entry systems. Lost or stolen access cards must be reported immediately.

Ensure doors, windows and cabinets are secure and avoid letting people you do not know, follow you into a council building without them proving their staff identity. Challenge anyone who you think could have gained unauthorised access and inform a manager.

Ensure a regular programme for changing key codes if you have these on any buildings/offices.

Visitors to Council Building

Ensure any visitors are briefed on arrival and not left alone where they could access information. When visitors leave the building ensure that any visitor passes are returned and that visitors have signed out of the building.

Leavers

When employees leave the organisation or team make sure their ID badge/proximity card and/or keys/codes are returned or altered as appropriate, remove access to key systems as soon as possible and check that network/shared drive or other shared electronic working area access is removed/altered as appropriate.

Make sure that any paper records not in the usual place of storage are returned to the manager of the team.

Make sure that all electronic records are stored in the correct and agreed place of storage, including those on shared drives, employee personal drives and those within the email system.

Report the loss of any ID badges and keys immediately using the Top Desk system.

The ICT Solution Centre must be informed of all leavers to ensure ICT equipment remains within the council, network access is revoked and that any access changes are made.

4.5. Keeping Information Secure

System Security

Access to the council's network must be authorised by the employee's manager and a New User Request form submitted to the ICT Solution Centre detailing the business requirement and level of access required. This should not be based upon another employee's level of access as this may grant more access than what is required.

As an authorised user including users with higher levels of privileged access, you are responsible and accountable for activities carried out by you, ensuring the safekeeping of your username and password, which must only be used by you.

All ICT systems must be formally authorised by ICT Solution Centre before use and must only be used for the intended purpose and abiding by the terms of any contractual licence agreements. Unauthorised equipment must not be connected to the council's network, except for personal devices connecting to the council's 'guest' wireless system.

Deliberate unauthorised access to, copying, alteration or interference with computer programs or data is strictly forbidden and users must not attempt to bypass, disable, or subvert system security controls.

Passwords

Access to most of the council's ICT systems is controlled using usernames and passwords. The username identifies the user as a valid user of the system and the password authenticates that the user is who they say they are and therefore is authorised to use the system.

Very occasionally, the normal use of a particular system may be by way of a shared username and/or password but usually an employee's user ID and password will belong to them only and they will be held responsible and accountable for all use of the computer system via their user account.

For passwords to give an adequate level of security, they must be correctly chosen, used and managed:

- Passwords should be at least eight characters long.
- Use a mix of upper- and lower-case letters, numbers, and special characters.
- Do not share or give your password to anyone – including ICT!
- Do not make obvious letter or number substitutions to disguise recognisable words for example, 0 for O, 5 for S, 1 for I, as this is a well-known technique and so offers little security.
- Do not write passwords down. If there is a genuine business reason for recording and storing a password it should be kept securely for example in a sealed envelope in a locked drawer or safe

- Do not use the same password for logins or sign-on to different systems.
- Do not re-use passwords (for example alternating the same two passwords)
- Choose passwords that are not easily guessable, avoid words which can be found in a dictionary; and

Avoid using the following words or types of words in any format within your password as they are common and can be easily guessed or cracked:

- Password (Password1)
- Places (Scunthorpe, Lincolnshire)
- Days of the week (Wednesday1)
- Months / Seasons of the year (January2020, Summer2020)

Baseline Personnel Security Standard (BPSS)

Employees who have higher administrative privileges or access to government applications (for example, users who are enabled to reconfigure the network, system administrators, users of the DWP system) should be subject to pre-employment checks which are aligned with the Baseline Personnel Security Standard (BPSS). This includes carrying out a check on unspent criminal convictions.

Accessing customers / employees records on systems

Systems that contain personal information or other confidential information must have appropriate security controls and access should be granted on a need to know only basis.

Most systems have an audit trail to log access to records. It is vital that employees do not access systems or records, where there is no legitimate professional reason to do so.

Employees must be aware that accessing personal files of customers, family or friends for non-work-related reasons is a breach of legislation and could result in disciplinary action and in very serious cases action including potential criminal proceedings and an unlimited fine.

Internet Access

The council provides internet access to employees in a way that it is consistent with their council duties. Internet access is also permitted for personal use during employee's non-working hours i.e. during breaks.

The following conditions apply:

- The council monitors the use of web browsing. Managers can request reports detailing an employee's activity if they suspect inappropriate use of web browsing.

- Some websites depending on their category classification are blocked and not permitted for use. These include but are not limited to: Adult material; gambling; dating; hacking; download sites (e.g. software, MP3 or other audio/video); data storage; illegal websites; personal networking and storage; peer to peer sharing; online gaming or malicious websites (e.g. spyware, phishing or fraud sites.) any other unauthorised site or category
- If a website is currently blocked and access is required for business use, a request should be logged with the ICT Solution Centre, which sets out the business need. Please note that access is subject to formal approval and may not be granted if it represents an unacceptable risk to the Council.
- Employees must not visit Internet sites that contain obscene, hateful or other objectionable material, download or view any obscene or indecent (for example pornographic) images, text or other materials whatsoever or other images, text or other materials, which encourage or promote activities, which would if conducted, be illegal.
- Employees must not make or post indecent remarks, proposals or materials on the Internet.
- Employees must not download any copyright work (whether it be a document, photograph, a piece of music or video or something else) unless properly authorised to do so by the copyright owner.
- Employees must not download software from a web site and install on a computer any software without proper authorisation.
- Employees should be aware that some sites might have malicious software such as damaging ActiveX controls, Java applets or JavaScript. Do not reduce the level of security provided by the web browser software by adjusting the browser settings.
- Employees are not permitted to use council systems in connection with any trade or business interests.

Viruses and Malware

Viruses and malware are very destructive and can be introduced onto the council's network in several ways, such as:

- Suspicious emails such as Phishing and Spam
- Malicious email attachments
- Web links
- Removable media
- File Downloads
- Installing software

Avoid being tricked into giving away personal information, (i.e. email address, passwords, bank details etc). If an email looks suspicious, do not click on any links or open attachments, just **delete the email** straight away from all email boxes, including sent items and trash.

Ensure your Anti-Virus software is up-to date and scan all removable media for viruses before use.

Signs that may indicate that malicious software is on a computer or system include:

- Unusual messages, patterns or sounds appearing on the computer, particularly after loading a new file from removable media or from email.
- Unusual or unrecognised files and/or folders.
- The speed and performance of the computer decreasing over a period of time.
- The memory available beginning to reduce, causing applications to run out of memory.
- Files unexpectedly changing in size.
- Files failing to load or run.
- The contents of files unexpectedly changing.
- High levels of disk drive activity.
- Rejected email from other systems warning of an infected email sent by you to them, and
- Inability to log into to or get a response from a computer system.

Malware incidents must be reported immediately to the ICT Solution Centre.

Important Note: Employees are encouraged to report any actual or suspected malware incidents straight away so they can be dealt with as quickly as possible, without fear of any disciplinary repercussions. These attacks are extremely sophisticated and specially crafted to entice or trick you.

All employees are enrolled onto the PurplePhish User Awareness and Education training programme and are required to complete the regular training modules as they become available.

Removable Media Controls

Removable media devices are portable digital data storage devices such as CD's, DVD's, USB memory sticks, SD cards, which can store a vast amount of information.

To protect information the use of any removable media must be minimised and approved by the ICT Solution Centre and supported by a strong business requirement. All removable media must be encrypted, protected with a passcode and must be scanned using the council's anti-virus system before each use. Information must be transferred to the council network place of storage as soon as practicable.

Removable media must not be used for the download of or storage of personal or special category personal information.

Managers are responsible for keeping a record of USB devices used within their teams including the type of information held on the device.

Lost or stolen removable media devices must be reported as an ICT security incident to the Solution Centre.

Monitoring

The council ICT network, telephony system and other electronic information is monitored to ensure adequate protection against security threats. Computer use is also monitored to ensure it is in line with user policies and procedures.

Social media

Employees are personally responsible for anything they say online and should keep in mind the security of information and what could be revealed unintentionally.

Please note: the use of digital technologies including Social Media by employees is monitored by the council, where necessary and reasonable. Inappropriate use or breach of this or any other council policy could lead to disciplinary action.

BYOD (Bring Your Own Device)

Smart Phones and tablet devices are becoming a common fixture in today's mobile environment. As standard mobiles are being replaced with new devices such as iPhones, iPads and Android devices these present opportunities and security risks therefore must be securely managed.

The Council has implemented a Mobile Device Management solution (MDM) that allows you to "Bring Your Own Device" whilst providing a layer of security required on such devices. Council work must only be carried out within the secure area on an authorised personal device.

PIN codes or passwords must be applied to devices. Default or easy to guess PINs or passwords must not be used and passwords should:

- Be at least 5 characters in length (4 characters where this has been configured by ICT Services);
- Contain a mixture of letters and numbers and ideally a combination of uppercase, lowercase, numbers and special characters;
- Be as random as possible, and in particular not contain recognisable words or any other strings associated with the user;
- Not contain more than two identical characters;

Devices should be locked when unattended to prevent unauthorised persons from being able to view council information.

Unapproved 3rd party applications must not be installed onto a corporate Smartphone or Tablet.

Approved applications such as Anti-Virus Software and Mobile Device Management (MDM) Software must not be uninstalled, security configurations applied must not be disabled and employees must not jailbreak/root the device.

Anyone losing a council or personal device containing any work-related information or used to access work related information must inform the Data Protection Officer, the ICT Solution Centre and a manager, as soon as possible.

4.6. Keeping Communications Secure

Don't be conned into giving out information

Depending on your role you may handle enquiries from organisations or individuals either inside or outside of the council. You may be asked to give out personal or sensitive information that the requester is not entitled to have. The requester's identity must always be checked before giving out information and ideally, they should be asked to write or email their request. Identity must not be checked by reading out a caller's address and asking them to confirm they live there.

Don't be bullied or tricked into giving out information – seek assistance from your manager or the Information Governance Team.

Being overheard

Conversations about personal or sensitive topics should not take place in locations where they could be overheard by someone who should not hear them. People overhearing a conversation may not be entitled to know the information being divulged and may know the individuals being discussed.

Care should be taken in touch down areas, kitchens and other shared council facilities and when windows are open. Care should be taken when making telephone or video calls that nobody can overhear your call if you are not using headphones or a plug-in handset. Care should also be taken outside the council such as whilst, for example working at home, travelling by public transport, sat in a café or when in your car.

As an employee you are bound by confidentiality not to divulge information you may see or hear whilst working. If you can overhear a colleague talking about a matter you consider to be private, please ask them to stop the conversation or move to a private area. Please don't continue to listen to something you should not be listening to.

Check who answers the telephone and be wary of leaving messages

Always check that the person who answers a telephone call is who you intended to call. Care should be taken not to divulge the reason for the call until you have established you are speaking with the correct person. Again, identity must not be checked by reading out a caller's address and asking them to confirm they live there.

Care should be taken if you need to telephone someone on their home or mobile phone when you are invited to leave a message. The message could easily be picked up by someone else. You should always leave your direct dial telephone number and ask the person to call you back, unless you have previously agreed that messages can be left.

Voicemail on your council telephone may contain personal or sensitive information therefore voicemail boxes should be kept secure with a pin code. Remember to change it from the default PIN.

Use secure email for personal/commercially sensitive information

When emailing personal or sensitive information internally and to another public sector organisations, such as the NHS, Police or DWP your normal northlincs.gov.uk email address can be used and is secure.

When emailing personal or sensitive information to any other 3rd party outside the council it must be sent using 'MOVEit', which sends it securely.

Not sending information securely means it is at risk of interception.

Do not email work information to a home email account

Sometimes it is tempting to email council work related information to a home email account, possibly to finish some work at home. Work information must never be emailed to a home account as security cannot be guaranteed.

Council work must never be performed on a home computer. If there is a need to work from home, the council's home working solution must be used to provide a secure means of access to work files and systems.

Do not use your own file sharing solution, such as Drop Box

The MOVEit system that is used to email personal and sensitive information can also be set up to allow file sharing between the council and external organisations in a similar way to Drop Box.

File sharing solutions, such as Drop Box must not be downloaded or used for council work, because the security of information cannot be guaranteed. Further information about MOVEit can be found in the ICT Knowledgebase on Top Desk.

Ensure correct recipients for email before hitting send

It is your personal responsibility to check that you are sending an email to the right recipient, therefore prior to sending any email, carefully check to ensure you have selected and spelt the correct email addresses for the people you want to receive the email, placed them in the correct 'To', 'Cc' or 'Bcc' field. It is very easy to mis-select the email address of a person with the same or a similar name or put an address in the wrong field, thereby disclosing personal or confidential information to an unauthorised person and causing a data incident to occur.

Before pressing the send button when you have written an email a second check must be carried out to make sure you have entered the correct email address for the intended recipient and to make sure you have attached the correct attachment.

An additional check should also be carried out to ensure there is no information on the bottom of the attached document that should not be there and that there is nothing in the email thread that should not be forwarded on.

If emails are regularly sent to a group of people, creating an email distribution group can save the need to key in each individual email address. But a check of the group members **must** be carried out to make sure you have selected the correct email group and to ensure all the group members still need to receive the information.

Care must also be taken to make sure you haven't accidentally caught a button on your keyboard and auto populated an incorrect email address or selected a group email when you intended to email individuals.

When sending an email to a group of people who should not know who else is receiving the email or where others should not see other private email addresses care should be taken to use the blind carbon copy (bcc) function so the recipient cannot see other recipients.

Calendars in Outlook

The Calendar function within Outlook can store attachments, links to Teams Meetings, emails within appointments, and room bookings which can be viewed by others. Take care when saving information within the calendar, meeting or room booking entry that no personal or sensitive information is saved within the appointment. The 'Private' feature can be used to mark any appointments others should not see.

Instant Messaging

Instant Messaging (i.e. WhatsApp or Microsoft Kaizala) is a useful tool for quickly checking information but should not be used for communicating authorisations, decisions, historic or other information that must be retained for statutory or council purposes e.g. it needs to be retained as a council record or be part of an audit trail.

Only Instant Messaging tools authorised by the Data Protection Officer should be used to communicate personal or sensitive information.

Telephone/Video Conferencing Calls

The installation of third-party conference client software applications (excluding Microsoft Teams) is not permitted on council devices. If you are invited to join a web meeting from a third-party organisation it is acceptable for you to join as an attendee using the link provided in the invite.

During calls:

- Ensure that only authorised attendees are part of the meeting.
- Only share / discuss the personal, sensitive or confidential information that is absolutely necessary to do so.

- **Do not** answer any other calls or participate in any other discussions.
- Pay attention when someone new joins the call and always ask them to identify themselves.
- If at any time you have any concerns about the confidentiality of the call, terminate the call immediately.
- If during the call you are unable to adhere to any of the above points the call should be ended.

Care should be taken about what information could be viewed during a video call, such as council information and detail in your home environment. The background can be blurred, or a picture added to prevent the background from being viewed.

Be mindful when screen sharing ensuring you select the right information to share and not to disclose anything unintentionally.

Ensure correct address when posting

Before posting information a second check **must** be carried out to make sure the information being placed in the envelope matches the address on the front of the envelope, that the contents of the letter match the address on the letter and that no additional information is accidentally being included. The quality of envelope used should be considered to ensure it is strong and secure enough for the contents. Using a double layer of envelopes should be considered and/or the use of envelopes that don't tear easily.

Care should be taken when checking address information – for example, Google Maps can sometimes be wrong.

If you need to post information you must use the full postal address and avoid using abbreviations.

The use of facilities such as 'special delivery' mail should be considered for highly sensitive personal or confidential information or the use of a carrier who provides a 'desk to desk' delivery service.

Information being hand delivered must be placed and delivered in a correctly addressed and sealed envelope.

An appropriate return address must be printed on the back of the envelope as this would allow the return of the post if it were to be delivered to an incorrect address.

Redaction

Before releasing or publishing information that requires redaction or anonymisation a check should be carried out to make sure the correct version is being sent and that the expected redaction has been applied.

Take care when carrying out redaction or anonymisation that it is not possible to identify individuals whose identities should be kept confidential. The Data De-identification Policy in the Information Governance Knowledge Base on TopDesk provides further detail.

Mail Merges

Mail merges are used in Microsoft word to send out external communications by combining a list of addresses and names with a particular letter. Before posting or emailing the letters a check **must** be carried out to make sure the mail merge has worked as expected so the correct name and address appear together on the correct letter.

4.7. Sharing Securely

Should I hand it over?

Any sharing of personal or confidential information either on a routine or ad hoc basis must be recorded and appropriate controls applied. This could include:

- a Data Protection Subject Access Request from someone wanting to access their personal information,
- a request made under the Data Protection Act 2018 Schedule 2 for personal information to be released to a third party with a crime investigation remit, such as the Police to enable the investigation of a crime,
- an Information Sharing Agreement,
- a contractual agreement or memorandum of understanding.

Allowing Guests (external users) access to council data via M365

Employees can add Guests to the Microsoft 365 suite of products, such as Teams, OneDrive and SharePoint to share documents and data with external users.

Guests can be anyone outside of the Council who has an email address therefore serious consideration to complying with our data protection and security requirements should be given before any Guest is added.

Before granting access to the M365 product suite, an authorising officer (e.g. the data owner) should confirm that the giving of Guest access is appropriate. You should put controls in place to ensure that Guest details are not shared whilst monitoring your Guest's access ensuring that there remains a continued need to access the information and that the level of access remains appropriate. Please see the M365 Guest Access and Sharing Guidance for further information. (Available on the Solution Centre Service Portal).

Guest access within the M365 product suite shall only be used for official Council business and not for personal use.

These ensure that all parties understand their responsibilities.

4.8. Home and Mobile/Remote Working

Good Practice

All home working and remote working must be authorised and carried out in compliance with council policy. There is a Home Working section in the HR Manual located in the HR area of TopDesk.

Equipment and information that is used outside of the secure office environment is more vulnerable to loss, theft, unauthorised disclosure, compromise, corruption, and deletion and must be given appropriate protection.

Employees are responsible and accountable for protecting information and equipment assets by:

Taking all necessary precautions to ensure the security of any information outside of council premises, including securing loose papers i.e. place in them a secure document folder/bag, taking care about who can overhear confidential conversations.

Laptops and other equipment taken off site must be locked away or kept out of sight if left unattended.

Laptop bags are attractive to thieves therefore keep personal and sensitive paper documents separate to the laptop bag.

You must dispose of personal or confidential information securely by returning papers to a council office and placing in confidential waste facilities, or by using a cross-cut shredder. Electrical or electronic equipment for disposal must be returned to ICT Services.

NEVER put personal or confidential waste in your domestic recycling or refuse bin.

Personal or sensitive information must not be accessed on non-secured Wi-Fi hotspots such as in hotels, cafes. For tips on securing your home wireless network – visit **https://www.getsafeonline.org/protecting-your-computer/wireless-networks-and-hotspots-pyc/**

Not allowing unauthorised users to have access to council equipment, i.e. family and friends

Follow the Clear Desk Policy at home as well as in the office.

Avoiding ‘shoulder surfing’ if working in public places such as on the train and in cafes, prevent information on the screen being overlooked, be warned - the person sat behind you, can read what is on your screen!

Employees must only print personal or commercially sensitive information on personal printers in exceptional circumstances and only where your line manager has approved this.

You must not send council information to your personal email address for home printing purposes.

ICT equipment and council information, including information accessed via Bring Your Own Device (BYOD), must not be taken outside of the UK without authorisation from your line manager.

Authorisation will be on a case by case basis and must be based on the reason for access, what information will be accessed and the countries to be visited. The Digital Technologies Policy provides further detail and depending on the countries to be visited it could be for example, access to information via BYOD would need to be turned off whilst you are out of the UK. In time there will be list of countries in the Digital Technologies Policy that are considered to have adequate safeguards in place and where requests to access council information could potentially be given.

4.9. Procurement

Does your contract have an IG/Information Security section?

Ensure that UK General Data Protection Regulation and Freedom of Information requirements are clearly specified within the conditions of contracts and service specifications for all relevant procured services.

Ensure that the pre-qualification and evaluation of prospective suppliers includes, where appropriate, consideration of capability for ensuring Data Protection. Ensure that due regard is given to Data Protection as part of contract monitoring and management.

Consider the implications of sub-contracting and ensure compliance with the UK General Data Protection Regulation and that the above requirements are passed through the relevant supply chain.

NCSC Cloud Security Principles

During a procurement for a Cloud based solution, ensure that you include statements within your specification questionnaire that allows you to measure the supplier against the 14 Cloud Security Principles. Contact the Councils ICT Security Officer for further information.

4.10. Storing and Disposing Securely

Managing records appropriately and not keeping them longer than necessary

The council has a legal obligation to manage its records as set out by legislation such as the Freedom of Information Act and the UK General Data Protection Regulation / Data Protection Act 2018.

The Records Management Policy and the Records Management Guidance explain how to comply with our obligations, explaining how for example records should be retained and disposed of. These can be found in the Information Governance Knowledge Base on TopDesk.

The UK General Data Protection Regulation requires that any records containing personal information are only kept for as long as necessary. It is good practice to only keep other records for the required length of time.

The Retention Schedule sits as part of the Records Management Policy and can be found in the Information Governance Knowledge Base on TopDesk. It shows the minimum period a record should be kept for and the trigger point that starts the retention period. A review must be carried out when the minimum retention period is reached to decide whether to destroy the record. The destruction of records must be authorised by the Information Asset Owner or Records Co-ordinator.

A project has commenced to consider the retention and destruction of electronic information held for e.g., in shared drives, personal drives, the email system and business systems to determine how to carry out destruction and how to do so in a way that complies with legislation.

A process has been developed to apply retention to emails. From 01 April 2021 any emails that need to be kept as formal records must be assigned a retention period from a drop down list in the email system. Please see TopDesk for further detail.

From 01 April 2022 any emails older than 6 years from the sent or received date, not marked with a retention period will be those emails that do not need to be kept as a formal record and will be deleted.

Good / regular filing

Maintaining good regular filing of both paper and electronic records and keeping a record of what records are held and where they are stored is important. Do you keep information for longer than necessary? Do you keep more than one copy of a record and if so is this necessary? Are you the primary record holder?

Storage of Records

Most records will in the future be digitised with a project underway to implement suitable secure electronic storage.

The council has a Central Record Store for paper records that is secure with controlled access. Only paper records that are needed on a day to day basis should be stored in offices or work areas. Secure buildings with access controls to the building and the storage facility must be used with storage areas sited to avoid damage to records.

Digitisation is also being considered for records in the Central Record Store. Employees must not create their own paper Record Stores in other locations. Each department has a Records Co-ordinator who can provide advice about the Record Store or this information is available from the Information Governance Team via **informationgovernance@northlincs.gov.uk.**

Electronic information must be stored with appropriate access controls on the council network/Microsoft 365 area, or approved Council software application – please agree with your manager and Records Co-ordinator an appropriate electronic solution for your team and please note that the ICT Services and the Information Governance Team are leading a project to introduce Microsoft SharePoint as a replacement for shared drives and this should be factored into discussions.

Microsoft Teams is also now available as a way of collaborating with other council employees and allows information to be presented as part of working together. Teams is currently able to present information from shared drives or SharePoint and OneDrive. During 2021-22 there will be a move away from shared drives to the use of SharePoint and One Drive. Retention periods will be applied to electronic records from a drop down list in a similar way to records stored in the email system.

Local hard drives must not be used for the storage of information and records because they could be accessed by anyone who logs on to the computer and are not automatically backed up.

Microsoft One Note is now available in the Microsoft 365 product suite. OneNote enables you to replace paper notepads and move to creating and storing notes digitally and electronically in a secure way. Any records created or amended using One Note must be updated on applicable systems as soon as practicable.

Records Co-ordinators hold an inventory of stored records for their areas of responsibility showing information including the location and retention period. Stored records must not be removed or moved to another location without authorisation of the Information Asset Owner or Records Co-ordinator.

Confidential waste disposal arrangement

You must dispose of any confidential paper waste using the council's confidential waste facilities. This could be by using the locked confidential waste bins located around the main council buildings, by using the cross cutting shredding facilities, or by using secure bag arrangements.

There is no need to pre shred information before it is collected but anyone who decides to pre shred must have the shredded material collected by the confidential waste carrier and this must not be placed it in the general waste.

Any bags of confidential waste awaiting collection or electronic/electronic equipment no longer required must be kept secure until securely disposed.

Disposal of ICT equipment and removable media

To comply with secure data destruction standards, the Waste Electrical and Electronic Equipment (WEEE) Directive and ensure that personal and sensitive data is not accidentally released, secure disposal of electronic devices must be co-ordinated through the ICT Solution Centre.

Employees should be aware that the normal delete function available on the computer does not securely delete the data (data can still be recovered forensically) and so special products and facilities must be used.

Any unwanted or faulty ICT equipment must be returned to the ICT Solution Centre.

The ICT Solution Centre will advise the appropriate method to return all types of equipment.