Third Party Access Policy

Purpose and Context

This policy establishes the requirements and procedures for granting third party organisations or individuals' access to the Council's systems, services, and data. The aim is to ensure that such access is managed securely, minimising risks to the Council's information assets and maintaining compliance with legal and regulatory obligations.

Policy Details

Policy Category	Technology Services
Author	Sam Clark
Owner	Service Director – Information & Technology
CLT Approval Date	
IGG Approval Date	
Review Date	

Version

#	Date	Changes
1.0	December 2025	Initial creation

Audience

This policy applies to all external vendors, contractors, consultants, partner organisations, and any other third parties who require access to the Council's systems, services, or data, regardless of the method of access (e.g., remote, onsite, or cloud-based).

Newcastle-under-Lyme Borough Council will authorise and allow third parties to access Council systems, services and data where there is a clearly defined organisational requirement to do so. This may include, but is not limited to the setup, installation, upgrade, maintenance, troubleshooting, fault investigation or feature enhancement on a Council system/service.

Policy Assumptions

Newcastle-under-Lyme Borough Council (NULBC) is a data controller, as defined within the UK General Data Protection Regulation (UK GDPR), 2018.

All Council employees, elected members, agency staff and any other representatives of Newcastle-under-Lyme Borough Council, along with staff, contractors and/or any other representative of third-party suppliers to the Council have an awareness of the UK General Data Protection Regulations.

All users (both Council and third-party staff, contractors, agency staff and any other representatives) should undertake GDPR and cyber security training, on at least an annual basis.

Definitions

- Third Party: Any external individual or organisation not directly employed or engaged by the Council.
- Access: The ability to interact with, view, or manipulate the Council's systems, services, or data.
- Data: Any information processed, stored, or transmitted by the Council.

Policy

1. **Introduction**
   This policy covers the procedures and responsibilities in the provision of access rights to Council systems, services and data by a third party organisation.

2. **Request & Approval Process**
   1. Request Submission: All requests for third party access must be formally submitted by the relevant internal system owner (referred to as the sponsor) via the designated Third-Party Access Request Form.

      The request must include:
      i. Organisation name
      ii. Name of the person who will be remoting in (referred to as the Access User)
      iii. The Access User's email address
      iv. The Access User's direct dial / mobile number (which will be utilised as the multi-factor authentication method to access the Council's systems).
      v. Justification for access
      vi. Specific systems, services, or data required
      vii. Whether the access will be supervised or unsupervised (i.e. screen sharing, direct remote access etc)
      viii. Duration and timeframe of access

2. Approval: Requests must be reviewed and approved by either the Technical Delivery Manager, Technology Service Business Manager or the Service Director with responsibility for IT.

   Access will only be granted where a valid contract or Data Processing Agreement (DPA) is in place, outlining the responsibilities and obligations of the third-party regarding data protection and security.

   Successful requests: Where the request for access is approved, the specified representative from the third-party organisation will receive an email containing instructions on how to gain access. This email will be sent ahead of the 'access date', but no access will be permissible ahead of this time. An email will also be sent to SDP to automatically raise a case.

   The IT Service Desk team will then prepare an account for the Access user to utilise, in line with the requested access level.

   Rejected Requests: Where a request for access is rejected, the Sponsor will be notified of the decision via email.

3. Access Process

1. On the specified day where access is required, the Access User should contact the IT Service Desk via telephone, using the telephone number provided in the request.

2. The IT Service Desk team will then enable the prepared account, set the expiry to the end of the working day (or other dependent on the approved period of time) and create a unique password which will be required to access the Council's systems and update the SDP ticket. This unique and randomly generated strong password will be sent to the email address as listed on the access request.

3. The Access User will then be required to follow the access instructions, where they will need to:

   i. Enter the provided username
   ii. Enter the unique password
   iii. Enter the multi-factor authentication code which will be sent to the direct dial / mobile number (as per the access request)
   iv. Confirm that they have read and will abide by the Council's Acceptable Use Policy.

4. At the end of the access period and/or at the end of the working day, the Access user should re-contact the IT Service Desk to notify them that their remote access has concluded for the day. The IT Service Desk team will then disable the account, reset the password and remove the MFA details and close the SDP ticket.

Where access is requested over multiple days, the Access user will need to repeat this process each day, as the account will expire at the end of each working day.

4. Control Measures

- Principle of Least Privilege: Third parties will be granted only the minimum level of access necessary to perform their agreed tasks.
- Time-Bound Access: Access rights will be limited to the approved period. Extensions must be formally requested and re-approved.
- User Accounts: Individual, non-transferable user accounts must be created for each third-party user. Shared accounts are strictly prohibited.
- Authentication: Strong authentication methods (such as multi-factor authentication) must be used where technically feasible.
- Access Reviews: All third-party access will be subject to regular review and audit by the Information Security Team to ensure ongoing necessity and compliance.

5. Levels of Access

Access levels will be categorised as follows:

- Read-Only: This level of access allows the viewing of information without the ability to modify or delete.
  For example, a third party undertaking a screen sharing with a member of NuLBC staff.

- Administrative (Supervised): This level of access provides the third party with full control over the specified system and/or data associated with the request, alongside a member of the NuLBC IT team.
  For example, a supplier remoting into a Council server to perform an upgrade/installation of a system via a joint remote session.

- Administrative (Unsupervised): This level of access provides the third party with full control over the specified system and/or data associated with the request. Under no circumstances should the third-party make changes to the operating system, underlying server configuration and/or any other setting/policy/configuration outside of the application. This level of access should only be granted in exceptional circumstances and a risk assessment be completed as part of the request form.
  For example, a supplier remoting into a Council server to perform an upgrade/installation of a system without a member of the NuLBC IT team.

The level of access granted will correspond to the specific business need and must be justified in the access request. Where the requestor is unsure on the appropriate level of access, they should contact the Technical Delivery Manager or Technology Services Business Manager for guidance.

Where a supervised session is undertaken, the member of NuLBC Technology Services team always remains in control of the session. Any required changes to the underlying server or network configuration should be conducted through the appropriate change procedure.

6. Security Expectations for Third Parties

Compliance

Third parties must comply with all applicable Council policies, including but not limited to the Data Protection Policy, Information Security Policy, and Acceptable Use Policy. These policies are available on the Council's website.

Confidentiality

All third-party personnel must treat council data as confidential and/or sensitive, at all times. Under no circumstances, should any Council data be copied or moved outside of Council systems without written authorisation.

Security Controls

Third parties are required to implement appropriate technical and organisational measures to safeguard Council data, including (but not limited to) anti-virus, encryption, multi-factor authentication, network security, endpoint protection, patch management, monitoring and logging, secure storage, and secure data transfer protocols.

Incident Reporting

It is the responsibility of the third party to promptly report any data breaches, security incidents (whether actual or suspected), concerns, or queries relating to the security of Council systems or data to the NuLBC Technology Services team without delay. The Council's DPO must be informed in a case of an actual or suspected data breach in order to comply with ICO notification requirements (if appropriate). Such notifications must be treated as a matter of urgency to ensure the Council can take appropriate action in a timely manner.

Monitoring

The Council reserves the right to monitor and audit all third-party activities on its systems to ensure compliance with this policy. This includes, but is not limited to, the use of key logging, screen and session recording, activity logging, and other technical measures designed to capture, review, and assess any actions performed by third parties. Such monitoring and auditing may be carried out at any time, without prior notice, to uphold the Council's data protection and security obligations.

Third parties should be aware that such monitoring may take place.

Training

Third parties are expected to provide regular security awareness training to their personnel who access Council systems, ensuring they are up to date with the latest cyber threats and best practices and evidence of such provided, if requested by the Council

Internal Controls

Third parties should conduct periodic vulnerability assessments and penetration testing on any systems they manage or connect to, promptly remediating any identified risks. As well as maintaining an up-to-date inventory of all devices and software used in connection with Council data and ensure that only authorised personnel are granted access based on the principle of least privilege.

Change Management

Third parties should not make changes to Council systems without prior notification and authorisation by the Council's Technology Services team.

If a third party fails to adhere to the Council's security expectations, this will constitute an automatic breach of the contractual agreements established between the Council and the third party. As a direct consequence, the third party will be held fully liable for any such breach and may be subject to immediate legal action by the Council. This strict approach is necessary to safeguard the Council's data, systems, and legal obligations.

7. **Termination of Access**
   Third party access will be revoked promptly upon completion of the contracted work, expiry of the access period, or upon breach of this policy. The system owner is responsible for ensuring timely removal of all accounts and credentials.

8. **Enforcement**
   Non-compliance with this policy may result in disciplinary investigation (where this policy has not been followed by a Council Officer), termination of contracts, and/or legal proceedings, depending on the nature and severity of the breach.

9. **Monitoring**
   As with all data, the Council takes data security and privacy extremely seriously and works to ensure that any third-party access is limited to only where required.

   Third parties should be aware that all actions performed are monitored.

10. **Rights**
    The Council reserves the right to refuse access where there is insufficient justification, a suitable contract/DPA is not in place, and/or the Council is not satisfied with the third party's access/security measures.

Legislation

Users (including third parties) are reminded of their responsibilities under:

- General Data Protection Regulation (UK GDPR)
- Data Protection Act (2018)
- Computer Misuse Act 1990
- Communications Act 2003
- Online Safety Act 2023
- Common Law
- Data Use and Access Act 2025
- Privacy and Electronic Communications Regulations

This list is not exhaustive. 'Legislation' will include all relevant legislation currently prevailing.

Feedback & Review

This policy will be reviewed in response to significant changes in legislation, Council operations, or identified security risks.

If you would like further information or to provide feedback, please contact the Service Director – Information & Technology.