Code Of Connection

Version 1.2

# Norfolk County Council Third Party Code of Connection

Complete the items in **RED**

Contents

[Norfolk County Council Third Party Code of Connection 1](#_Toc181777449)

[Introduction and scope 1](#_Toc181777450)

[Code of Connection 2](#_Toc181777451)

[Appendix 1 Agreed Tasks of Work 6](#_Toc181777452)

[Appendix 2 Equipment List 6](#_Toc181777453)

[Appendix 3 Information to be Shared 6](#_Toc181777454)

[Version Control 7](#_Toc181777455)

## Introduction and scope

This document is in 2 parts. The Code-of-Connection is followed by the Data Sharing questions. Please read the Code of Connection and agree to this by signing the attached Code-of-Connection. Finally, also complete the data sharing questions to be reviewed by the IG team.

Norfolk County Council’s information systems and physical assets, including supporting processes, systems, networks, and equipment, must be appropriately protected to ensure that the Council can continue to operate and provide its service delivery. A Norfolk County Council Information System also includes any cloud-based Software as a Service system that is run on behalf of the Council by a service provider. A “connection” includes a physical or virtual data circuit into the Council’s data centre(s), or into the data centre(s) of a partner providing a service for the Council, or a user ID used to authenticate into a Council Information System, or an API.

The Council’s supply chain and partners have a responsibility to provide appropriate and continued protection for the full life span of any information shared or application/systems used and must ensure any additional parties authorised to access services also comply.  This applies to information, products, services, applications, systems, and infrastructure.

All staff and individuals with access to The Council’s information have an individual responsibility to ensure that information and service access is handled securely and appropriately.

## Code of Connection

Protocol 1 Code of Connection / Network Security Agreement THIS AGREEMENT is made on the <Date> (“the Effective Date”) between:

Norfolk County Council

having its principle office at County Hall, Martineau Lane, Norwich. NR1 2DH

(hereinafter referred to as “NCC”) and <Third Party’s name>

(hereinafter referred to as ‘the Business Partner) whose registered office is situated at: <location>

Whereas, NCC has determined that connection to the NCC Digital Services network, of one or more of the Business Partner’s computer systems located at the Business Partner’s premises at <insert name of relevant premises> (hereinafter referred to as the “communications link”) is advantageous in order for agreed tasks of work to be completed in an effective manner;

and whereas NCC is prepared to grant the Business Partner the necessary access.

and whereas the Business Partner agrees to adhere to the conditions set out below regulating such access, in order for NCC to ensure that such access does not in any way compromise the interests of NCC or its employees.

NOW THEREFORE IT IS AGREED BETWEEN THE PARTIES AS FOLLOWS:

##### 1 Physical Link Connection

1.1 The communications link connection between the Business Partner (or a third party sub-contracted by the Business Partner to perform the task on their behalf) and the NCC Digital Services network is for use only for the agreed tasks of work contained in Appendix 1 to this Agreement. Should NCC consider that the communications link is being used in any other manner, NCC reserves the right to sever the communications link without notice and without prejudice to NCC’s other rights and remedies arising from such misuse.

1.2 All physical equipment to be connected or used with the communications link should be described in Appendix 2. Should NCC determine that any other equipment has or had access to the communications link between NCC and the Business Partner, NCC reserves the right to sever the communications link without notice and without prejudice to NCC’s other rights and remedies arising from such unauthorised access.

##### 2. Information Security

2.1 No information, data or software may be taken from NCC’s computer systems other than that information, data or software specifically required to perform the task of work as described in Appendix 1 or 3. The Business Partner shall apply appropriate protective measures to any information, data or software taken from NCC’s computer systems and shall use all reasonable endeavours to ensure such information is not released to or accessed by any person other than employees of the Business Partner directly involved with the agreed task of work.

2.2 No information, data or software may be transmitted to NCC by the Business Partner or any other 3rd party source other than that information, data or software specifically required to perform the task of work as described in Appendix 1 or 3.

2.3 The Business Partner shall comply and ensure that its employees will at all times adhere with the Data Protection Legislation (including the Data Protection Act 2018 as enacted or amended) and any Guidance issued by the Information Commissioner).

2.4 In processing personal data on behalf of NCC, the Business Partner shall comply with the Data Protection Legislation all times in accordance with the instructions of NCC as Data Controller and generally do nothing to compromise the Council’s compliance with its obligations as data controller.

2.5 In the event that the actions or inactions of the Business Partner, whether deliberate or accidental, in respect of any unauthorised disclosure or other processing of personal data caused/undertaken by the Business Partner, result in a breach of the Data Protection Legislation, then the Business Partner shall wholly indemnify NCC for any such breach.

##### 3. Physical Security

3.1 Any of the Business Partners equipment which is electronically connected to the NCC Digital Services network must be located in areas within the Business Partner’s premises which are not readily accessible by the general public. In addition, such equipment shall be located in areas within the premises of the Business Partner in such a manner as to limit physical access to the equipment to only those individuals requiring such access for the purposes of the agreed task of work.

##### 4. Network & Communications Security

4.1 Items of IT equipment approved for use with the NCC Digital Services network may be networked together. However, no other network or communications link may be connected to any of the approved IT equipment while it is connected to the NCC Digital Services network, without the prior written consent of NCC Chief Technology Officer, which consent shall not be unreasonably withheld

4.2 The Business Partner shall ensure their IT infrastructure including (but not limited to) endpoints, communications equipment and servers are suitably protected from malware and cyber-attack.

##### 5. Personnel Access

5.1 Use of the equipment connected to the NCC Digital Services network must be limited to only those personnel directly involved in the agreed task of work. An approved list of appropriate personnel who are qualified and trained to undertake work under this agreement must be agreed with NCC prior to the commencement of the task of work and must include, without limitation, name, location, business telephone number, normal working hours, and Computer User Identifier for each individual involved in the agreed task of work. The Business Partner shall notify NCC and request approval of any staff who are added to the approved list prior to any new person commencing the task of work.

5.2 Computer User Identifiers used by personnel of the Business Partner when accessing the NCC Digital Services network are to be unique. Each Computer User Identifier is to be used only by the individual to whom the Identifier has been allocated. Passwords associated with the user must not be shared, are to be changed on a regular basis (not exceeding 90 days), changed if it is suspected of being compromised and disabled when that user leaves the Business Partner’s employment.

5.3 NCC reserves the right to carry out monitoring and random checks to ensure access to the NCC Digital Services network is only performed by those individuals on the approved list. In the event of non-approved personnel accessing the NCC Digital Services network, or any Computer User Identifier being used by any person other than the agreed individual, NCC reserves the right to sever the communications link without notice and without prejudice to NCC’s other rights and remedies arising from such unauthorised access.

##### 6. Scope of Communications

6.1 The NCC Digital Services network has been created and implemented in a manner which encourages the free exchange of information and services for all NCC personnel operating in NCC. No attempt shall be made by any personnel of the Business Partner to gain access to any information, equipment or services not directly concerned with the agreed task of work. Should any attempt be made to access information, equipment or services not directly concerned with the agreed task of work, NCC reserves the right to sever the communications link without notice and without prejudice to NCC’s other rights and remedies arising from such attempt.

##### 7. Checks and Reviews

7.1 The Business Partner shall provide to NCC full unrestricted access to check the location and integrity of any equipment at the Business Partners premises which has access to the NCC Digital Services network, at any time, and from time to time at the request of NCC.

7.2 In the event of any significant reduction of security levels, whether temporary or permanent, for whatever reason the Business Partner shall alert the NCC Head of Digital Services and notify him/her of any additional security measures being put in place. NCC reserve the right to require that additional measures be implemented if those proposed do not match the required standard.

7.3 The Business Partner agrees to notify NCC of any planned changes to the security specification of equipment with access to the NCC Digital Services Network and obtain his/her consent prior to making the changes.

##### 8. Personnel Behaviour

8.1 The Business Partner shall ensure that all Business Partner personnel with access to, and/or use of equipment connected to the NCC Digital Services network are made aware of, and operate in accordance with, the terms of this Agreement.

##### 9. Notification of Security Incidents

9.1 The Business Partner shall provide to NCC the name of a designated employee, of appropriate seniority, who will act as the point of contact between the Business Partner and NCC in the event that an incident occurs which NCC considers to be in breach of this Agreement, irrespective of whether the event originates from the Business Partner or NCC.

9.2 The designated employee may be asked to supply to NCC any information or data (eg., system log files) from within the Business Partners organisation which is considered by NCC to be pertinent to the investigation of such an event.

9.3 In the event that the Business Partner becomes aware of a breach of this Agreement it shall immediately inform NCC and take all necessary actions to rectify this breach within 24 hours.

9.4 The Business Partner and NCC staff, as nominated by the NCC Head of Digital Services, shall investigate any security incident within one working day of any notification, or as soon as reasonably practicable thereafter. Use of the communication link may be suspended by NCC pending the outcome of such investigation.

9.5 NCC reserves the right to suspend or sever the communications link without notice and without prejudice to NCC’s other rights and remedies arising from such incident.

##### 10. Indemnities

10.1 The Business Partner shall be responsible for and shall save, indemnify, defend and hold harmless NCC from and against all claims, losses, damages, costs (including legal costs) expenses and liabilities in respect of:

10.1.1 loss or damage to property of NCC whether owned, hired or leased relating to or in connection with the performance or non- performance of the agreement by the Business Partner or those for whom it is responsible in law; and

10.1.2 personal injury (including death or disease) to any person employed by NCC arising from or relating to or in connection with the performance or non- performance of the agreement by the Business Partner or those for whom it is responsible in law.

10.1.3 subject to the express provisions of this agreement, personal injury (including death or disease) to any third party or loss or damage to the property of any third party to the extent that any such loss, damage or injury is caused by the negligence or breach of duty (whether statutory or otherwise) of the Business Partner or those for whom the Business Partner is responsible in law. For the purpose of this clause, ‘third party’ shall mean any party which is not NCC or the Business Partner

10.1.4 loss or damage to NCC’s Digital Services network by malware which is transmitted arising from or relating to or in connection with the performance or non-performance of this agreement by the Business Partner or those for whom the Business Partner is responsible in law.

10.2 NCC shall be responsible for and shall save, indemnify, defend and hold harmless the Business Partner from and against all claims, losses, damages, costs (including legal costs) expenses and liabilities in respect of:

10.2.1 personal injury (including death or disease) to any person employed by the Business Partner arising from or relating to or in connection with the performance or non- performance of the agreement by NCC or those for whom NCC is responsible in law.

10.2.2 subject to the express provisions of this agreement, personal injury (including death or disease) or loss or damage to property of any third party to the extent that any such loss, damage or injury is caused by the negligence or breach of duty (whether statutory or otherwise) of NCC or those for whom it is responsible in law.

10.2.3 save for the provisions of 10.2.1 and 10.2.2 above, NCC will not be liable any loss or damage, howsoever caused, and howsoever arising, from NCC’s unilateral right to sever the communications link in the event of a breach of clauses 1.1, 1.2, 5.3 and 9.5.

##### 11. Duration and Renewal

11.1 This Agreement shall subsist from the last date of signing hereof **for 3 years** and shall automatically terminate thereafter unless renewed by mutual consent in writing. However, either party may terminate upon giving thirty days written notice to the other, or forthwith upon giving immediate written notice to that effect, where the other Party commits any breach of the terms of this Agreement.

##### 12. Jurisdiction

12.1 This Agreement shall be governed by the Laws of England and Wales

##### 13 Statement of Acceptance

13.1 The Business Partner has reviewed the foregoing standards and agree that all measures will be taken by <insert name> to ensure that access to the NCC Digital Services network and/or any equipment supplied by NCC will be exercised only in accordance with the terms of this Protocol.

For and on behalf of Business Partner (to be signed by an accountable senior manager)

Signed:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Position:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Dated:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

For and on behalf of NCC (to be signed by an accountable Head of Service or Service Owner) **Note: This should be the most senior person responsible for the contract and/or relationship between NCC and the supplier**

Signed:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Position:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Dated:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Appendix 1 Agreed Tasks of Work

The Third Party will specify all tasks of work to be undertaken through the proposed connection.

## Appendix 2 Equipment List

The Third Party will specify all equipment and technologies used to connect to NCC.

## Appendix 3 Information to be Shared

This appendix should list all information that will be shared between the parties. The table should detail both personal information (as defined under UK GDPR) and non-personal information. Where personal information is being shared, the lawful basis under Article 6 and / or 9 should also be documented.

*This appendix should be reviewed by the Norfolk County Council IG team prior to signing of the Code of Connection to ensure any information risks are appropriately managed*.

|  |  |  |
| --- | --- | --- |
| **Description of information being shared** | **Is it personal, as defined under UK GDPR?** | **If personal, what is the lawful basis for sharing?** |
| (Example) Names, Age, D.O.B. | (Example) Yes | (Example) Not Applicable |

### Version Control

| **Version**  | **Description**  | **Release Date**  | **Issued By**  |
| --- | --- | --- | --- |
| 0.1  | Draft  | August 2022  | ISO  |
| 0.2 | Cut down | Nov 2022 | ISOBSA |
| 0.3 | Refine against responses | Dec 2022 | ISO |
| 0.4 | Reorder CoCo first and refine | Jan 2023 | BSAISO |
| 0.5 | Update | Feb 2023 | BSAISO |
| 0.6 | Legal Update | March 2023 | NP Law |
| 1.0 | No Change | April 2023 | BSAISO |
| 1.2 | Split Code from policy | Nov 2024 | ISO |