Title: - **Third Party Network Access Policy POL016**

Scope: - Shared Digital, Camden, Haringey and Islington Councils.

Effective - At approval date

Revision History: Third Party Network Access Policy POL016

Version	Date	Amendment Details	Version	Author
Initial Draft	10/11/2017	Draft for comment	0.1	Victoria Griffiths
2nd Draft	13/12/2017	Updated from feedback Mike Cann received from Anne Woods Haringey Council SIRO	0.2	Victoria Grififths
3rd Draft for review	13/12/2017	Homoginised document for use across Shared Digital environs	0.3	Michael Cann
4th Draft	13/02/2018	Updated from feedback from Shona Nicolson and Antoinette Carter Data Protection Lead and Head of Info Gov. and Bus. Support LBI	0.4	Victoria Griffiths
5th Draft	19/02/2019	Updated from feedback from Joanne Reeves and Rahika Devesher, Camden Council Lawyers	0.5	Victoria Griffiths
6th Draft	21/03/2018	Updated from feedback from Anita Hunt, Feedback & Information Governance Manager, Haringey.	0.6	Victoria Griffiths
Approved	30/04/2018	Approved by Islington CGG	0.6	Michael Cann

Review Schedule

This policy will be reviewed for relevance and accuracy in ***November 2018*** by the Network Security Manager and then *annually* afterwards by the Network Security Manager alongside all other security policies.

Contents

1.0 Overview

1.1 It is a requirement that the Councils connection to the PSN and NHS networks meets a minimum standard for 3rd parties accessing its network and, by definition,controls and authorises anyone accessing the network. Without adequate management controls the level of threat to the council's systems and data is increased.

1.2 GDPR Article 5 and the Data Protection Act 2018 requires all registered organisations to apply appropriate technical and organisational measures needs to be taken to prevent unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

1.3 This policy, when used in conjunction with other policies within the security policy framework is focused on reducing this risk.

2.0 Scope and Applicability

2.1 Security is everyone's responsibility. This policy applies to employees, Councillors, contractors, consultants, temporary staff, including interns and volunteers and other workers of the Council, including all personnel affiliated with third parties and Shared Digital.

2.2 This policy pertains to all third parties using any ICT infrastructure, system or data held by or operated on behalf of the Council. See 'Definitions' for this policy's intent on what a third party is. This policy also pertains to any Shared Digital individual dealing with third parties wishing to use the council's infrastructure.

3.0 Normative References

3.1 This document forms part of an ISO/IEC27001 aligned ISMS.

3.2 Control 9 of ISO/IEC27002 is applicable.

3.3 ICT Third Party Approved Connection Policy

3.4 ICT Third Party Minimum Device Requirements Policy

3.5 ICT Third Party Network Access Audit Policy

3.6 ICT Third Party Standard Network Access Procedure

3.7 ICT Third Party Administrative Network Access Procedure

3.8 ICT Third Party Network Access Audit Procedure

3.9 Third Party Network Access Form – User

3.10 Third Party Network Access Form – Sponsor

3.11 Third Party Network Access Form – Risk Analysis for Administrative Access

3.12 Third Party Network Access Form – Third Party Organisation

3.13 Camden Council Third Party Code of Connection Agreement

4.0 Terms and Definitions

4.1 For the purpose of this document, the terms and conditions given in ISO/IEC 27001 and ISO/IEC27002 apply.

4.2 Standard ICT terminology is used.

4.3 PSN – Public Services Network

4.4 NHS – National Health Service

4.5 **Third Parties**

Third parties are defined as anyone not employed directly by the council and includes partners such as the NHS, other local authorities, as well as suppliers who require access to the council's network. All partners who are part of partnerships are considered third parties for the purposes of network and data access. All council Schools are considered third parties.

Third Parties are individuals and organisations which fall into the following categories. These will include, but not be limited to:

4.5.1 **Contracted staff and trusted partners**

4.5.1.1 Outsourced support services

4.5.1.2 Temps and agency staff that are not employed through council nominated agency worker supply organisations.

4.5.1.3 Staff working within the Local Health Community (e.g. Primary Care Trust)

4.5.2 **Third Parties requiring administrative access to Council systems**

4.5.2.1 External IT support staff

4.5.2.2 Suppliers (including Suppliers of IT goods, systems or services)

4.5.2.3 Auditors not employed directly by the council

4.6 **Sponsor**

Sponsors are defined as council employees who sponsor and take responsibility for third parties. A sponsor can be either a system owner or a service director or their explicitly nominated representative.

4.7 **Restricted data**

The Council and Shared Digital are permitted to hold data to the level of "sensitive" as classified by Central government. GDPR places additional requirements on certain classes of special category data found within Personally Identifiable Data (PII), security by design must be incorporated into any system handling the following data:-.

race;

ethnic origin;

politics;

religion;

trade union membership;

genetics;

biometrics (where used for ID purposes);

health;

sex life; or

sexual orientation.

4.8 **Information Security Incidents**

Information Security Incidents include, but are not restricted to, the following:

4.8.1 The loss or theft of data or information, including encrypted devices.

4.8.2 The unauthorised or accidental disclosure of, or transfer of data or access to information which includes the transfer of data to those who are not entitled to receive that information.

4.8.3 Attempts (either failed or successful) to gain unauthorised access to data or information storage on a computer system.

4.8.4 Unauthorised or accidential changes to information or data or system hardware, firmware, or software characteristics without the Council's knowledge, instruction, or consent.

4.8.5 Accidential unauthorised loss or access to, or destruction of personal data. This includes disruption or denial of service to a system.

5 General Policy

5.1 General Third Party Requirements

5.1.1 All third parties must have a signed contract with the Council.

5.1.2 All third parties must conform to the Council's security policies and requirements.

5.1.3 Only authorised connection methods are allowed. Please see Third Party Approved Connection Policy for further details.

5.1.4 Third parties must inform the council regarding any security incidents. See Definitions.

5.1.5 Sponsors must report to Shared Digital any security incidents raised by third parties.

5.1.6 A central register of all third party connections and accounts must be maintained by the Council containing at least the following:

- 5.1.6.1 Description of the service
- 5.1.6.2 Key contacts at the council for the service
- 5.1.6.3 Key contacts at the 3rd party for the service
- 5.1.6.4 Start date for the service
- 5.1.6.5 Expected life span of the service
- 5.1.6.6 Emergency handling process for terminating or suspending the service
- 5.1.6.7 Risk assessment results

5.1.7 Third Parties must meet council administration standards:

5.1.8 There must be authentication of individual users, not groups of users. No generic accounts are permitted.

5.1.9 Protection with regards to the retrieval of passwords by ensuring that adequate measures are in place to ensure that all passwords are secure

5.1.10 System access monitoring and logging - at a user level

5.1.11 Role management so that functions can be performed without sharing passwords.

5.1.12 Password administrative processes must be properly controlled, secure and auditable.

5.1.13 Usernames and access will be denied until the authorization process is completed successfully.

5.1.14 Third parties must manage usernames and password information to the standard outlines in the Password Policy.

5.1.15 Third parties with access to "Official data" must be cleared to council standards. Any third party who has access to the Shared Digital network and who has regular access to Official information or information that originates from the PSN should be at least cleared to the 'Baseline Personnel Security Standard'

5.1.16 Third parties who process personal data on behalf of the council will be registered Data Controllers. Until clarification is received from the ICO it is recommended Third parties that process personal data on behalf of the Council should be registered as Data Controllers with the Information Commissioner and must be able to provide this evidence to the council on request from the council.

5.1.17 All third party devices used to access the council's network must meet the minimum third party device requirements as outlines in the Third Party Minimum Device Requirement Policy.

5.2 Standard Account Creation Requirements

5.2.1 A service director or system owner [Sponsor] must request an account be created.

5.2.2 The sponsor or authorised person must confirm when access is no longer required.

5.2.3 The 3rd party account will be set to expire on the termination of the contract.

5.2.4 Shared Digital will review third party accounts on an annual basis.

5.2.5 Third party accounts will be managed according to the standard Shared Digital policy on accounts.

5.2.6 The following need to be complete and signed for each account:

5.2.6.1 Third Party Network Access Form – User

5.2.6.2 Third Party Network Access Form – Sponsor

5.2.6.3 Third Party Network Access Form – Risk Assessment

5.2.6.4 A signed Third Party Network Access Form – Third Party Organisation needs to be on file for the Organisation of each user account.

5.3 Administrative Account Creation Requirements

5.3.1 A service director or system owner [Sponsor] must request an account be created.

5.3.2 The sponsor or authorised person must confirm when access is no longer required.

5.3.3 Shared Digital will review third party accounts on an annual basis.

5.3.4 Third party accounts will be managed according to the standard Shared Digital policy on accounts.

5.3.5 The following need to be signed and complete for each account:

5.3.5.1 Third Party Network Access Form – User

5.3.5.2 Third Party Network Access Form – Sponsor

5.3.5.3 Third Party Network Access Form – Risk Assessment

5.3.5.4 A signed Third Party Network Access Form – Third Party Organisation needs to be on file for the Organisation of each user account.

5.3.6 This account will have a specified end date. It will be disabled on that date.

6 Roles and Responsibilities

6.1 Everyone is responsible for security.

6.2 **The Sponsor** [see Definitions] is responsible for the third party account throughout its life.

6.3 **Shared Digital** is responsible for the technical creation of the account.

6.4 **Shared Digital** is responsible for the annual review of all third party accounts.

6.5 **The Network Security Manager** is responsible for any violations or exceptions to this policy.

7 Compliance

7.1 Compliance Measurement

The Shared Digital team will verify compliance to this policy through various standards and methods, including but not limited to, internal and external auditors, periodic walk-through's, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

7.2 Exceptions

Any exception to the policy must be approved by a SIRO in advance.

7.3 Non-Compliance

An individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Non-Compliance, resulting in a data breach will be reported to the ICO within specified timescales where required.

8 Risk Management

8.1 Risk management for each Council is defined within their Risk Management Policy. Shared Digital will adhere to these policies.

9 Policy Review

9.1 This policy will be reviewed by the process owner and updated alongside the security operating procedures on a regular basis, not to exceed 12 months.

10 Policy Signoff

Role	Name	Date
Process Owner **Network Security Manager**	**Mike Cann**	
CIO	**Fabio Negro**	
SIRO Camden Council	**Andrew Maughan**	
SIRO Islington Council	**Mike Curtis**	
SIRO Haringey Council	**Andrew Meek**	