	London Borough of Hammersmith & Fulham **CABINET** **14 JULY 2014**

MAINTAINING COMPLIANCE WITH PUBLIC SERVICES NETWORK CODE OF CONNECTION	
Report of the Cabinet Member for Finance – Councillor Max Schmid	
Open Report A separate report on the exempt Cabinet agenda presents exempt correspondence relating to this matter.	
Classification - For Decision **Key Decision:** Yes	
Wards Affected: All	
Accountable Executive Director: Jane West, Executive Director of Finance and Corporate Governance	
Report Author: Howell Huws, Head of Business Technology	**Contact Details:** Tel: 020 8753 5025 E-mail: Howell.Huws@lbhf.gov.uk

1. EXECUTIVE SUMMARY

1.1. The Public Services Network (PSN) is a UK Government Wide Area Network, whose main purpose is to enable connected organisations, including local authorities and central government, to communicate electronically and securely at low protective marking levels. H&F make use of the PSN to access a range of applications to carry out its business, including paying housing benefits and issuing parking tickets.

1.2. H&F needs to maintain compliance with the PSN code of connection (CoCo) to secure continued access to the PSN. Without this access, the Council could not carry out these vital business functions.

1.3. The PSN Authority (PSNA) issued new CoCo requirements for unmanaged user devices (see Appendix 1) and has moved from reasonable controls to a zero-tolerance approach. An unmanaged user device is any device not provided, configured and maintained by the Council. The most typical example of an unmanaged user device is a home PC used to provide remote access to the Council network from home.

1.4. The PSNA's new requirements oblige H&F to physically separate IT services accessed from unmanaged user devices into PSN and non-PSN services. This paper sets out how H&F can maintain compliance with the PSN Code of Connection.

2. RECOMMENDATIONS

2.1. That officers seek to agree a risk-tolerant approach with PSNA.

2.2. That in the event that it is not possible to agree this risk-tolerant approach, approval be given to implement the fully PSN compliant solution for H&F remote access at a project cost of £147,991and additional revenue costs per year of £49,457, making a total cost of £395,276 over five years.

3. REASONS FOR DECISION

3.1. H&F need to maintain compliance with the PSN code of connection to secure continued access to the public sector network for a range of applications to carry out its business.

4. INTRODUCTION AND BACKGROUND

4.1. The PSN is a UK Government Wide Area Network, whose main purpose is to enable connected organisations, including local authorities and central government, to communicate electronically and securely at low protective marking levels. H&F make use of the PSN to access a range of applications to carry out its business, including paying housing benefits and issuing parking tickets. In paying housing benefit, for example, the Council makes use of systems provided by the Department for Work and Pensions (DWP).

4.2. The PSN CoCo provides a minimum set of security standards that organisations must adhere to when joining the PSN. H&F needs to maintain compliance with the PSN CoCo to secure continued access to the PSN.

4.3. The PSN CoCo is intended to maintain security of PSN Data, which is any data sent over the PSN as a bearer. So DWP-owned data sent over the PSN as a bearer (as is the case when H&F staff use DWP systems in order to pay housing benefits) remains DWP data and the recipient must comply with any data handling requirements imposed by DWP.

4.4. The PSN was preceded by the Government Secure extranet (GCSX). H&F were compliant with the GCSX CoCo. However, in August 2013 the PSNA issued new requirements to the connected organisations for connection via unmanaged user devices (see Appendix 1). Unmanaged user devices are those which are not under the control of the organisation and are used for remote access to the IT systems of the organisation. The Council makes extensive use of unmanaged user devices for remote access to the IT systems, with 2,000 staff able to work this way, and 300 staff making use on a typical day.

4.5. This change was accompanied with a change in emphasis from the previous acceptance from GCSX for reasonable controls implemented by the organisations to a zero-tolerance approach. H&F and many other Councils have made representations to the Cabinet Office about the additional burdens that this approach brings.

4.6. The new PSNA requirements oblige H&F to physically separate services into PSN and non-PSN services. This paper sets out how H&F can maintain compliance with the PSN Code of Connection by implementing a solution compliant with PSNA's requirements specified in CESG/PSNA document "AP7 - Transitioning to PSN: Managing the Risk from Unmanaged End User Devices".

5. PROPOSAL AND ISSUES

5.1. Hammersmith & Fulham Bridge Partnership (HFBP) provide the Council's ICT services, while Colt provide the Council's virtual desktop solution, including the remote access solution. To achieve the required physical separation of services into PSN and non-PSN services, HFBP propose working with Colt to provide additional infrastructure for a separate remote access solution to support connection of up to 400 concurrent users from unmanaged devices. HFBP will configure this solution to restrict these users to access non-PSN services only.

5.2. In addition, HFBP will implement a separate solution using certificates to identify corporately managed devices and enable these to use the existing remote access solution with access to both PSN and non-PSN services.

5.3. GCSX secure e-mail is used for communication with government partners. This e-mail service is provided through PSN and therefore also needs to be secured. HFBP will therefore also build new exchange and fileshare servers and move GCSx mailboxes and fileshares onto these servers. Only remote sessions from corporately managed devices will be able to access these GCSX mailboxes and fileshares.

5.4. The costs for this work are as follows:

Cost element	**Cost £**
HFBP Project Management	21,720
HFBP Technical Services	95,025
Colt Installation Costs	31,246
Implementation costs	**147,991**
HFBP support charges	13,575
HFBP charges for Shared Server – Infrastructure	25,870
Colt – annual charges for firewall pair	4,213
Colt – annual charges for separate non-PSN connection	1,467
Annual costs	**45,125**

5.5. This creates the potential for compliance. However, additional costs may arise in enabling staff to continue to operate efficiently, if they are currently using their own devices to work remotely. Three main categories of PSN usage in H&F have been considered:

- Use for access to Department for Work and Pensions (DWP) systems to enable housing benefits claims to be paid;
- Use for access to Driver and Vehicle Licensing Agency (DVLA) systems to enable parking control notices (PCNs) to be issued;
- Use for GCSX e-mail for secure communications with other public sector bodies.

Usage	**Impact**	**Cost £ pa**
DWP systems	Existing DWP constraints mean that users are already issued with Council laptops when working remotely.	0
DVLA systems	12 additional Council-owned laptops would be required to enable secure remote access to PSN systems.	4,332
GCSX e-mail	Less than 100 staff make use of GCSX e-mail, and it is assumed that these can arrange their work such that they only access GCSX e-mail when in the office. No additional laptops are therefore required.	0
	Total additional costs for laptops pa	**4,332**

5.6. The total additional costs per year are therefore £49,457, as follows:

Cost element	**Cost £**
Annual costs for PSN compliant solution	45,125
Annual costs for additional laptops required	4,332
Total additional costs per year	**49,457**

5.7. These additional costs per year will be required as long as the PSN regime requires this implementation to assure separation of PSN and non-PSN data. The continuously changing requirements of PSN inevitably brings uncertainty around the costs of maintaining compliance. In addition, this requirement may be affected by future developments in the Tri-Borough ICT architecture, particularly with regard to desktops and networks.

6. OPTIONS AND ANALYSIS OF OPTIONS

6.1. Three options were considered.

1. Cease compliance with PSN
2. Issue all staff requiring remote access with corporate laptops
3. Negotiate a risk-tolerant approach with PSN
4. Implement a PSN compliant solution

6.2. The pros and cons of each are listed below.

Option	Pros	Cons
1 – Cease compliance with PSN	Minimal cost	Inability to carry out core Council business including benefits payments and parking control notices
2 – Issue all staff requiring remote access with corporate laptops	Minimum disruption to ways of working	Additional **annual** cost estimated at £360,000 due to requirement to issue staff with Smart Laptops
3 - Negotiate a risk-tolerant approach with PSN	Minimal cost	Failure to agree approach would result in having to adopt a different option, possibly with less time and therefore greater risk of failing to achieve the deadline of April 2015.
4 – Implement a PSN compliant solution	Continue with current operating model enabling optimal use of buildings	Project costs of £147k, plus additional annual costs of £50k Minor disruption to ways of working for staff using GCSx

6.3. Option 3 offers the best balance of enabling current operating model to continue while keeping costs to the minimum. Informal discussions have suggested the Cabinet Office are wanting to be more balanced in their approach and have now encouraged the PSNA to review their position on unmanaged devices, particularly for virtual desktops such as those used by H&F. This is partly in response to representations made by local government regarding the burden imposed by the central government position (see Appendix 2).

6.4. However, the current extent of this tolerance has yet to be tested. If the PSNA are willing to accept the very low levels of risk associated with unmanaged user devices when used with virtual desktops, this may afford an opportunity to avoid the additional expense, and will be discussed as part of the next compliance audit, due in August 2014.

6.5. H&F will continue to make representations to the Cabinet Office that compliance with PSN is not compromised by the use of unmanaged user devices used with virtual desktops in order to avoid the expense if possible. In doing so, it will seek to work with other Local Authorities in a similar position, such as Lambeth, Ealing and Camden.

6.6. If the indications are that PSNA are unwilling to agree this risk-tolerant approach, Option 4 offers the next best balance of enabling current operating model to continue while keeping costs to the minimum. Option 4 will take six months to implement, and therefore a decision must be taken in early September to enable this to complete in time.

6.7. It is therefore recommended that we seek to agree a risk-tolerant approach with PSNA, with the option to implement the fully PSN compliant solution if this risk-tolerant approach cannot be agreed.

7. CONSULTATION

7.1. Local departmental IT strategy groups and the corporate IT Strategy and Operational Group have been consulted in the formation of this report.

8. EQUALITY IMPLICATIONS

8.1. There is considered to be little or no impact on equality as a result of the issues in this report.

9. LEGAL IMPLICATIONS

9.1. There are no direct legal implications. The works will be procured through the Council's existing arrangements with H&F Bridge Partnership.

9.2. Kevin Beale, Head of Social Care and Litigation Legal Services, tel: 020 8753 2740.

10. FINANCIAL AND RESOURCES IMPLICATIONS

10.1. The estimated one-off cost of the proposal is £147,991 and there is an annual commitment of £49,457 for five years. It is proposed that the one-off cost be funded from use of the IT infrastructure fund. The balance of the fund was £2.7m at the close of 2013/14. The annual cost will be met from the IT Enablers budget which has an annual budget provision of £0.8m.

10.2. Implications verified/completed by: Andrew Lord, Head of Strategic Planning and Monitoring, Phone : 020 8753 2531

11. RISK MANAGEMENT

11.1. Information is an asset rather than a by-product of our services. Information risk management and governance of information is the responsibility of the Council and the designated Senior Information Risk Officer. The report proposals present the best approach to mitigate the risk at the best cost with the least disruption for unmanaged end-user devices.

11.2. The Cabinet Office wrote in their communication of the 6th August 2013 that exposing internal Government services to access from unmanaged end-user devices is not compliant with PSN Information Assurance so Local Authorities must ensure that the risk to information received through the PSN is minimised. They added that they are familiar with the balancing act between access, security and cost. However, the business conducted by Local Authorities and the data underpinning those services must be appropriately protected.

11.3. The PSN Compliance regime ensures that the appropriate measures are in place. The cross-Government move to the Public Services Network (PSN) requires end-to-end trust to facilitate increased interoperation. This trust model has resulted in an increased focus on the compliance of connected organisations.

11.4. Implications completed by: Michael Sloniowski Bi-borough Risk Manager ext. 2587.

12. PROCUREMENT AND IT STRATEGY IMPLICATIONS

12.1. There are no procurement related issues as the recommendations contained in this report relate to an order to be placed under the contract with H&F's strategic ICT provider, H&F Bridge Partnership.

12.2. Implications verified/completed by: Mark Cottis, e-Procurement Consultant 020 8753 2757.

LOCAL GOVERNMENT ACT 2000
LIST OF BACKGROUND PAPERS USED IN PREPARING THIS REPORT

No.	Description of Background Papers	Name/Ext of holder of file/copy	Department/ Location
1.	None		

LIST OF APPENDICES:

Appendix 1: Changes in PSN Compliance approach

Appendix 2 –: Copies of previous correspondence on the issue (exempt)

APPENDIX 1 – CHANGES IN PSN COMPLIANCE APPROACH

In 2012, the PSN has implemented a zero tolerance approach to compliance. At its core, this is about creating a trust model across PSN. The scope of PSN is substantially different to the old GSi and as such needs genuine trust between connected partners. Although some of the eventual increased sharing benefits may not be immediately available, without creating a network of trust it will not be possible to increase the data sharing opportunity that PSN presents. In order to be able to share sensitive data, it is essential that the central government data owners trust LAs as end points and can share data with confidence across PSN; that end-to-end trust is not always there today because not all end points meet the compliance standard.

Additionally, Data Protection laws require all those connected to PSN to protect the data that Government handles on behalf of citizens. The GSi – and now PSN – compliance requirement is to provide this minimum standard for the appropriate protection of data and assets. All connected organisations are aware of their obligations, however some have not implemented the appropriate controls.

The PSN has not allowed exceptions or mitigations to meeting the core standard. All organisations have known about the compliance requirement, which is a minimum standard, since Compliance was introduced. However, some organisations never reached this minimum standard and have instead been submitting compliance applications with remedial action plans that have not been concluded or have received the same IT Health Check (ITHC) failures year on year without remediation. It is these poor behaviours of the few that resulted in PSNA in taking a hard look at the end-to-end compliance position and having to enforce the compliance position across the whole community.