NHS Counter Fraud Authority

Proxy Gateway

Data Protection Impact Assessment

May 2021

V4:0 Published Version

NHS fraud.
Spot it. Report it.
Together we stop it.

Executive Summary

The purpose of the Proxy Gateway is to manage the internet requests of users and provide various functions including blocking, inspecting and allowing traffic. The Proxy provides a more secure way of browsing the internet by acting as a “proxy” for users. This involves receiving user requests and sending them onto the website and receiving the response before returning it to the user. By doing this it allows for rules and policies to be in place as the user request is run through the rules and policies before it is sent on, if the website category is blocked then so is the request.

The proxy gateway contains a summary of requests that are sent through the proxy as well as a note detailing if any rules were triggered. The proxy also contains information regarding user searches on the likes of Google.

The DPIA was originally completed in 2018 and it remains current. Version changes have been as a result of redactions, and there have been no amendments to the use or functionality.

This document is deemed OFFICIAL and any information viewed/obtained within it should be treated in the appropriate manner as advised and set out in the Government Security Classifications (May 2018).

More information in relation to this data classification, including the requirements for working with these assets can be found here:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf

In particular please note that:

ALL routine public sector business, operations and services should be treated as OFFICIAL - many departments and agencies will operate exclusively at this level. There is no requirement to explicitly mark routine OFFICIAL information. Baseline security measures should be enforced through local business processes. A limited subset of OFFICIAL information could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media. This subset of information should still be managed within the ‘OFFICIAL’ classification tier, but may attract additional measures (generally procedural or personnel) to reinforce the ‘need to know’. In such cases where there is a clear and justifiable requirement to reinforce the ‘need to know’, assets should be conspicuously marked: ‘**OFFICIAL–SENSITIVE’**

Table of contents

Document Control					
Completed By	**Ref**	**Document owner**	**Version No**	**Issue Date**	**Amendments**
Security & Operational Support Analyst	DPIA / Proxy Gateway	DPO	V0.1	16/10/2018	All
Security & Operational Support Analyst	DPIA / Proxy Gateway	DPO	V0.2	26/10/2018	Updates from Security and Operational Support Analyst
Security & Operational Support Analyst	DPIA / Proxy Gateway	DPO	V0.3	08/11/2018	All
Security & Operational Support Analyst	DPIA / Proxy Gateway	DPO	V1.0	28/11/2018	Final
Security & Operational Support Analyst	DPIA/Proxy Gateway	DPO	V2.0	31/03/2019	Redacted to prevent security risks to the organisation when published
Security & Operational Support Analyst	DPIA/Proxy Gateway	DPO	V3.0	08/11/2019	Final review and redaction
Security & Operational Support Analyst	DPIA/Proxy Gateway	DPO	V4.0	01/05/2021	Further redaction for external publication

Prefix	
Reference:	DPIA / Proxy Gateway
Date:	May 2021
Author:	Security & Operational Support Analyst
Data Owner:	Information System and Analytics Manager
Version:	4.0
Supersedes	3.0

Links & Dependencies

Document	Title	Reference	Date	POC
DPA	Data Protection Act	All	2018	HMG
EU GDPR	EU General Data Protection Regulation	All	2016	GDPR
FOI	Freedom of Information Act	All	2000	HMG
Government Security Classifications	Government Security Classifications	All	May 2018	Cabinet Office
HRA	Human Rights Act	All	1998	HMG
ISO/IEC 27000	Information security management systems Standards	ISO/IEC 27001:2013	Oct 2010	ISO
IS1P1 & P2	HM Government Infosec Standard No. 1, Part 1 – Risk Assessment and Treatment	P1 - Issue 3.5 P2 – Issue 3.5	October 2009 October 2009	CESG
IS2	InfoSec Standard 2	Issue 3.2	January 2010	CESG
PECR	The Privacy and Electronic Communications Regulations	All	2003	HMG

1. Data Protection Impact Assessment Requirement & Process

Introduction

1. The General Data Protection Regulation (GDPR) 2016 introduces a new obligation to undertake Data Protection Impact Assessments (DPIAs), before carrying out types of processing **'likely to result in high risk(s) to individuals' interests'**. DPIAs are now mandatory for certain types of processing and there are specific legal requirements for content and process. Where a DPIA identifies a 'high risk' that cannot be mitigated, the Information Commissioner's Office (ICO) must be consulted.

2. DPIAs provide a way to systematically and comprehensively analyse the intended processing and help to identify and minimise data protection risks. In addition to considering compliance risks, they should also consider broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm to individuals or to society at large, whether it is physical, material or non-material.

3. To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals. It does not have to eradicate the risks altogether, but should help to minimise them and assess whether or not remaining risks are justified. A DPIA may cover a single processing operation or a group of similar processing operations. For new technologies you may be able to use a DPIA done by the product developer to inform your own DPIA on your implementation plans.

4. A DPIA must consider 'risks to the rights and freedoms of natural persons'. While this includes risks to privacy and data protection rights, it can also effect other fundamental rights and interests:

"The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from data processing which could lead **to physical, material or non-material damage**, in particular: where the processing **may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy**, **unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage**; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data[1]…"

5. Under GDPR you must carry out a DPIA where for example you plan to:

- process special category or criminal offence data on a large scale.

6. The ICO also requires a DPIA to be undertaken for example, where you plan to:

- use new technologies;
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');

7. DPIAs are an essential part of the organisation's accountability obligations under GDPR and an integral part of the 'data protection by default and design approach'. An effective DPIA helps to identify and fix problems at an early stage, demonstrate compliance with data protection obligations, meet individuals' expectations of privacy and help avoid reputational damage which might otherwise occur.

[1] GDPR - Recital 75

8. Conducting a DPIA is a legal requirement for any type of processing. Failure to carry out a DPIA in required cases may leave the organisation open to enforcement action, including a **fine of up to €10 million**.

9. This DPIA is related to the NHSCFA RMADS, which outline the threats, risks and security countermeasures in detail. The RMADS was developed in accordance with the requirements of NHSCFA and CESG HMG Infosec Standards 1 and 2.

Proxy Gateway General Description

10. The purpose of the Proxy Gateway is to manage the internet request of users and provide various functionality including blocking, inspecting and allowing traffic. The Proxy provides a more secure way of browsing the internet by acting as a “proxy” for users. This involves receiving user requests and sending them onto the website and receiving the response before returning it to the user. By doing this it allows for rules and policies to be in place as the user request is run through the rules and policies before it is sent on, if the website category is blocked then so is the request.

The proxy gateway contains a summary of requests that are sent through the proxy as well as a note detailing if any rules were triggered. The proxy also contains information regarding user searches on the likes of Google.

11. The processes used by the proxy server involve the processing of internet requests through a set of rules and policies which decide whether or not a site will be blocked. This is done through a number of methods such as website categorisation which involves checking what a website is categorised as if it is a known website, to blacklisting/whitelisting which will deny/allow access to a website, regardless of whether the website would be allowed/blocked due to other policies or rules. Another way data is processed is through the use of packet inspection. This involves unpacking the packet and analysing the contents. Depending on the contents it will either be blocked or allowed through. This is a more thorough inspection method primarily used to try and detect malware hidden within packets.

12. As the communications that are monitored are internet communications they could contain any kind of information.

13. For security and confidentiality purposes, the database is only accessed by approximately 5 members of staff from NHSCFA, which includes the database administrators.

14. This is the only DPIA to be completed on the Proxy Gateway and it has been carried out by the Information and Records Management Officer, in consultation with the Security and Operational Support Analyst and the Information Governance and Risk Management Lead.

15. The Proxy Gateway, in addition to GDPR is also required to comply with other relevant HMG legislation including where applicable the Data Protection Act 2018, Human Rights Act 1998 and Freedom of Information Act 2000.

Data Protection Impact Assessment

16. To ensure the Proxy Gateway meets all legal requirements and the risks to personal data are identified and understood it is necessary to undertake a DPIA. This DPIA is based on the ICO's recommended template[2] comprised of seven steps:

Step 1 - Identify the need for a DPIA

Step 2 - Describe the processing

Step 3 - Consultation process

Step 4 - Assess necessity and proportionality

Step 5 - Identify and assess risks

Step 6 - Identify measures to reduce risk

Step 7 - Sign off and record outcomes

[2] Version 0.3 (20180209)

STEP 1: Identify the need for a DPIA

Explain broadly what the system/project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

The Proxy Gateway is made up two clustered servers. These servers work together to perform several tasks:

- The masking of a user's computer; meaning the outside cannot tell how many computers are on the network or target any computer in particular.
- Provide content filtering to block inappropriate websites.
- To detect and block malicious packets from being delivered to a user's computer.

This proxy server was installed in September and replaced the Bluecoat proxy servers. It was decided this was an opportune time for DPIA to be conducted to assess the ways the data is processed and determine the justifications behind it.

The type of data that is hosted on the service is limited to website addresses, usernames and searches.

STEP 2: Describe the processing

Describe the nature of the processing:

1. How will you collect, use, store and delete data?

2. What is the source of the data?

3. Will you be sharing data with anyone (consider using a flow diagram or other way of describing data flow)?

4. Why types of processing identified as 'likely high risk' are involved?

Data is collected through the proxy server. This is done when a user makes a request, the request is forwarded from the proxy server after checking against the rules, blacklist and whitelist. This request is stored. The response from the website is then received and the next step depends on the policies enabled. If the website is under a category that allows for packet inspection then the packet is unpacked, checked and if it is fine then it is repackaged and sent on the user. If packet inspection is not enabled then the packet header is checked. This involves the website address and destination. This is then sent onto the user if everything is correct.

The sources of the data are the user's computer and the website that the user was requesting. This means that it can vary massively between requests from users using google in one site Bing in another.

The data will not be shared and only system administrators will have access to it.

No processing is identified as high risk.

Describe the scope of the processing:

1. What is the nature of the data and does it include special category or criminal offence data?

2. How much data will you be collecting and using?

3. How often?

4. How long will you keep it?

5. How many individuals are affected?

6. What geographical area does it cover?

Given that the information collected will largely be from internet sites most of the information is part of the public domain and it is unlikely that any special category or criminal offence data will be processed or stored. This information would likely go through the email or intranet services.

Any requests to access the internet will go through the proxy server. This information will be collected and run through the rules and policies to clarify the sites category and whether the user is allowed access the website.

The information will be requested on a per request basis.

The data will be stored until space starts to become limited whereupon the oldest records will be deleted. There was no estimated time provided for this.

All NHSCFA users will go through the proxy server.

This covers all sites

Describe the context of the processing:

1. What is the nature of your relationship with the individuals?

2. How much control will they have?

3. Would they expect you to use their data in this way

4. Do they include children or other vulnerable groups?

5. Are there any prior concerns over this type of processing or security flaws?

6. Is it novel in any way?

7. What is the current state to technology in this area?

8. Are they any current issues of public concern that you should factor in?

9. Are you signed up to any approved code of conduct or certification scheme (once any are approved)?

The information that is monitored is related to queries sent by users at the NHS CFA. The relationship is that they are our colleagues.

All information goes through the proxy server, there is no control over whether it gets sent however the users have control over what gets sent as they look for the websites.

It is advertised on the IT Policy which all users agree to by logging into and using the computer systems.

No data relating to vulnerable groups should be analysed.

No concerns have been raised to my knowledge regarding this type of processing. I have no knowledge of any flaws.

This service is not new, this data was processed by a preceding system known as Bluecoat.

The system in place is new but was tested for a few months prior to implementation. Proxy servers are still a standard system to be used in a network infrastructure.

Describe the purposes of the processing:

1. What do you intend to achieve?

2. What is the intended effect on individuals?

3. What are the benefits of the processing, for you and more broadly?

The intent behind processing the data is to ensure that content we would not like to be displayed is not displayed. One example of this is gambling. If a user requests access to a known gambling website, then the content will be blocked as we do not allow access to gambling on the corporate network. Another purpose is to attempt to block malware and other malicious packets from reaching an end user. For instance, packet inspection will look at the actual contents of a packet and attempt to identify what is in the packet. This could identify malware or malicious code within the packets. This website or packet would then be blocked.

A user will be unable to access any website that has its content characterised as something that is blocked, for example gambling.

The benefits of this include the blocking of access to unwanted websites as well as the protection of the network from malware setup on websites.

STEP 3: Consultation process

Consider how to consult with relevant stakeholders:

1. Describe when and how you will seek individuals' views or justify why it's not appropriate to do so?

2. Who else do you need to involve within your organisation?

3. Do you need to ask your processors to assist?

4. Do you plan to consult information security experts or any other experts?

The overall service itself has barely changed; the system that provides it has. Due to this the stakeholders were not required to be made aware of the entirety of the change and were instead informed of the noticeable changes to the service, for example the fact that the implementation of the new system might take some time to get to the level of the previous system.

The people involved are the IT Administrators and the Information Security Team.

For this same reason consultation with information security experts is not required at this time as the service has not undergone a drastic change.

STEP 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular:

1. What is your lawful basis for processing?

2. Does the processing actually achieve your purpose?

3. Is there another way to achieve the same outcome?

4. How will you prevent function creep?

5. How will you ensure data quality and data minimisation?

6. What information will you give individuals?

7. How will you help to support their rights?

8. What measures do you take to ensure processors comply?

9. How do you safeguard any international transfers?

The processing of the data is lawful as the proxy gateway is designed and used to prevent access to malicious or potentially damaging web content from being accessed.

The defined lawful basis for the processing as identified in Article 6(1) of GDPR would be:
Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

The processing provides a safeguard and is a reliable solution for meeting the organisation's security objectives.

A firewall could potentially provide some of the proxy functionality. However, it would mean becoming reliant on the firewall for more tasks as well as no longer having an additional layer of defence for web browsing.

The proxy gateway is managed by a small group and performs a specific task. There is unlikely to be any function creep.

Data integrity, confidentiality and quality is maintained due to a limited number of users having access to the data. By limiting the number of users and having auditing in place we are able to monitor who has access to the data effectively and ensure that the data is stored safely.

Staff automatically accept the IT Security Policy and Acceptable Use Policy upon signing into the NHSCFA Computer Systems. All staff are advised to read these documents upon their induction to the CFA and therefore should be aware of email communications being monitored.

Access to the data kept on the proxy servers is limited to specific individuals. This reduces the chances of data loss or leakage as well as reducing the likelihood of a successful compromise of the accounts. This also limits the effectiveness of the insider threat by reducing the number of users who could do any potential damage.

The logs are not transferred outside of the UK.

STEP 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary	**Likelihood of harm** Remote, Possible or Probable	**Severity of harm** Minimal, Significant, or Severe	**Overall risk** Low, Medium or High
NHSCFA Proxy User (Admin) – Through accident or intent an administrator uses the service in a way that can cause damage to the organisation. The admin can view user's search history but cannot directly influence it. Due to this the potential damage is somewhat limited. They could remove rules that are in place to protect users or perform a DoS which	Remote	Severe	Medium
External Internet Based Attacker – Gaining access to the proxy. This can reduce the defences on our network by disabling rules or other features. The attacker would not be able to gain a significant information from the records on the server.	Possible	Significant	Medium
Physical Intruder - In the event of a physical intruder who attempts to steal or destroy hardware a denial of service could take place. The data on the server is not substantial as such from a data loss perspective the impact is relatively low.	Remote	Severe	Medium

STEP 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5.	Effect on risk Eliminated, Reduced, Accepted	Residual risk Low, Medium, High	Measure approved Yes/No
Continual assessment of opportunities to improve network security.	Reduced	Medium	
Continual monitoring of access rights given to staff and removal of access where it is no longer required.	Reduced	Medium	
Integration of the Proxy Internet Gateway logs into the current SIEM (Security Incident and Event Management) solution for use with pattern recognition and alerts.	Reduced	Medium	

STEP 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before proceeding.
DPO advice provided		DPO should advise on compliance, step 6 measures and whether processing can proceed.
Summary of DPO advice:		
DPO advice accepted or overruled by:	Trevor Duplessis 19 November 2018	If overruled, you must explain your reasons
Comments: Having reviewed the DPIA I am satisfied that a comprehensive assessment of the system has been undertaken. Access to the software system is restricted to the IT Administrators and the Information Security Team; with individual access accounts this can be fully audited. The data will be stored until space starts to become limited whereupon the oldest records will be deleted. There was no estimated time provided for this but the system is to be kept under continuous review to monitor this. Given that the information collected will largely be from internet sites most of the information is part of the public domain and it is unlikely that any personal, special category or criminal offence data will be processed or stored by the system.		
Consultation responses reviewed by:		If your decision departs from individuals' view, you must explain your reasons
Comments:		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA

Ownership

16. The following table describes the Proxy Gateway roles and responsibilities:

Table 1 - Roles and Responsibilities

Role	Responsibility
Information Asset Owner (IAO)	Information System and Analytics Manager
Senior Responsible Officer (SRO) Information Risk Owner (IRO)	Head of Intelligence and Fraud Prevention
Application/Database Owner	Information Security Lead
Data Protection Officer	Trevor Duplessis Information Governance and Risk Management Lead

2. DPIA Report

Section 1: Overview of Data Collection and Maintenance

1. The aim of the Proxy Gateway is to block access to unwanted and malicious websites and to detect and block malicious packets.
2. The data should not include personal or sensitive data, only usernames and websites accessed.
3. The impact level of the Proxy Gateway System was assessed as CONFIDENTIAL and it can only be accessed internally.
4. The following measures briefly describe what controls have been implemented to protect the Proxy Gateway System and the personal data recorded:
    a. All off site back-ups are secure as they can only be opened via the encryption key.
    b. The System is only accessed by approximately 5 members of staff from NHSCFA, which includes the database administrators
    c. The Proxy Gateway System does have any direct interconnections with other NHSCFA systems and applications
    d. The Data Custodian must comply with the data protection requirements Examples include: regularly reviewing the business requirement to record the personal data; ensuring that the data is not excessive; it is being used for the purpose intended; that there is a deletion and disposal policy; that the application is registered on the NHSCFA register and the NHSCFA DPO is aware of its existence.
5. It is assessed that there are no residual privacy risks to the personal data used by the Proxy Gateway System.
6. This DPIA must be reviewed if any changes are made to the personal information if used by the database or any other changes are made that affect the privacy of an individual.

Section 2: Uses of the Application and the Data

7. Describe the purpose of the System.

The aim of the Proxy Gateway is to block access to unwanted and malicious websites and to detect and block malicious packets.

8. Who has responsibility for the administration of the Database/System

The Information Security Team is responsible for the maintenance and configuration of the proxy server.

9. Information in the System could include;

- User web access
- Usernames
- User searches

10. Also list any sensitive data:

No sensitive data will be hosted.

11. The measures that have been implemented to protect the Personal Data are:

a. Access is restricted to approximately 5 members of staff within NHSCFA including the database administrators

b. Proxy Gateway does not have a direct interconnection with other NHSCFA systems or application

c. The IAO must comply with data protection requirements. Examples include: regularly reviewing the business requirement to use the personal data; ensuring that the data is not excessive, it is being used for the purpose intended; that there is a deleting and disposal policy; that the application is registered and the DPO is aware of its existence.

Section 3: Data Retention

12. The Proxy Gateway System is subject to NHSCFA Data Handling and Storage Policy. Logs are deleted as space fills up, starting with the oldest web access logs.

13. The IAO is required to review the retention period and any requirement to change must be submitted to the Senior Information Risk Owner.

Section 4: Internal Sharing and Disclosure of Data

14. Access is restricted to approximately 5 members of staff within NHSCFA including the database administrators.

Section 5: External Sharing and Disclosure of Data

15. The only information shared with external organisations, would be with the *police* if it was requested for the administration of justice.

Section 6: Notice/Signage

16. NHSCFA's privacy policy on its website hosts separate sections in relation to data collection, retention and storage. This broadly covers all elements of the NHSCFA usage of data, in a nonspecific manner.

17. The use of signage or other notifications to notify the public of the gathering and use of personal data is not relevant to this System and therefore outside the scope of this DPIA.

Section 7: Rights of Individuals to Access, Redress and Correct Data

18. Individuals subject to certain exemptions, have the right to gain access to their own personal data. In the event an access request is directly or indirectly received by NHSCFA, we are required to provide the individual who has made the request with details of the personal data recorded about them.

19. It is unlikely that many access requests will be received as no substantial personal data should be held.

20. In the unlikely event that information is identified as being incorrect, NHSCFA staff will take appropriate steps to correct the record where permissible.

21. All NHS employees and member of the public have the right to access, redress and correct personal data recorded about them.

Section 8: Technical Access and Security

22. The security and technical access architecture of the System is as explained in this DPIA:

The application and the hosting infrastructure was assessed at **Official-Sensitive** and the hosting infrastructure is subject to CESG approved IT Security Health Check.

23. Access is restricted to internal staff only.

24. The technical controls to protect the database include:

a. Permission based access controls to the server.

b. Logging, audit and monitoring controls.

c. Vulnerability Patching Policy for the underlying infrastructure.

Section 9: Technology

25. The Database/System holds no substantial personal information.

3. Compliance Checks

DPA 2018 Compliance Check

1. The DPO must ensure that the Proxy Gateway System, and the personal data that it records, and its business activities, are compliant and maintain compliance with:

   a. The GDPR and the Data Protection Act in general;

   b. The Data Protection Principles;

   c. The interpretations of the Principles.

2. **This is not a recommendation but a requirement of law.**

3. The roles and responsibilities for the protection of personal data are described in the NHSCFA security policy.

4. The system does not process sensitive personal data.

The Privacy and Electronic Communications Regulations

5. The Privacy and Electronic Communications Regulations is not applicable as personal data is not exchanged with external organisations for commercial purposes.

The Human Rights Act

6. The decisions and activities of the organisation are undertaken in compliance with the Human Rights Act, having due regard to appropriateness and proportionality to ensure compatibility with Convention rights.

The Freedom of Information Act

7. As a public authority we are compliant with the provisions of the Freedom of Information Act, in proactively publishing and making available upon request, certain recorded information held by the organisation subject to any relevant exemption(s). However, no personal information would be disclosed under the Freedom of Information Act as this would breach the data protection principles.

Conclusion

8. There are no residual privacy risks to the personal data recorded in the System. The controls described in this DPIA explain in detail how the data is protected and managed in accordance with the GDPR and Data Protection Act 2018. The DPO is responsible for ensuring that the controls are implemented through the life cycle of the system.

Annex A - Definition of Protected Personal Data

Personal data includes all data falling into Categories A, B or C below:-

A. Information that can be used to identify a living person, including:

Name;
Address;
Date of birth;
Telephone number;
Photograph, etc.

Note: this is not an exhaustive list.

B. Information which, if subject to unauthorised release, could cause harm or distress to an individual, including:

Financial details e.g. bank account or credit card details;
National Insurance number;
Passport number;
Tax, benefit or pension records;
DNA or fingerprints;
Travel details (for example, at immigration control or oyster records);
Place of work;
School attendance/records;
Material related to social services (including child protection) or housing casework.

Note: this is not an exhaustive list.

C. Sensitive personal data relating to an identifiable living individual, consisting of:

Racial or ethnic origin;
Political opinions;
Religious or other beliefs;
Trade union membership;
Physical or mental health or condition;
Sexual life
Commission or alleged commission of offences;
Proceedings relating to an actual or alleged offence.

Any data set containing this information must be processed in accordance with the GDPR and the Data Protection Act 2018 (DPA 2018).

Particular care must be taken with data in Category B and with any large data set. Information on smaller numbers of individuals may justify additional protection because of the nature of the individuals, source of the information, or extent of information.

There are additional, specific constraints within the provisions of GDPR and the DPA (2018) on the processing of data in Category C.

Annex B - Data Protection Compliance Check Sheet

PART 1: BASIC INFORMATION - New or existing Project, System, Technology or Legislation

1. Organisation and project.

Organisation	NHSCFA
Branch / Division	NHSCFA Information Systems and Analytics
Project	Proxy Gateway

2. Contact position and/or name, telephone number and e-mail address.
(This should be the name of the individual most qualified to respond to questions regarding the DPIA)

Name, Title	Trevor Duplessis
Branch / Division	Finance and Corporate Governance, NHSCFA
Phone Number	020 7895 4642
E-Mail	Trevor.Duplessis@nhscfa.gov.uk

3. Description of the system being assessed.
(Please note here if the initiative does not collect, use or disclose personal data*). If this is a change to an existing project, system, technology or legislation, describe the current system or program and the proposed changes.

The Proxy Gateway is the replacement for the Blue Coat Proxy servers. This system is made up of two servers that act alongside one and other to provide a gateway to the internet. When a user makes a request to access the internet it is first sent to one of the gateway servers before the gateway server sends it to the destination.

4. Purpose / objectives of the initiative (if statutory, provide citation).

NHSCFA leads on a wide range of work to protect NHS staff from economic crime.

The purpose of the System is:

- To ensure that end points are protected by hiding the IP Addresses of the end points by using the gateway's own IP address range as the requestor.
- To block unwanted/malicious files and packets from entering the network.

Access is restricted to 5 members of staff within NHSCFA, including the database administrators.

5. What are the potential privacy impacts of this proposal?

Data Protection Impact Assessments (DPIA) have been considered in the light of personal data gathered, and the data in the Proxy Gateway System has been gathered for a specific, justifiable and proportional purpose and found to be mitigated by the steps put in place to minimise the possibility of unauthorised access or use (see Compliance Checks in section 3 of this document)

6. Provide details of any previous DPIA or other form of personal data* assessment done on this initiative (in whole or in part).

This is the first DPIA carried out on the system.

IF THERE IS NO PERSONAL DATA INVOLVED, GO TO PART 3: DPA COMPLIANCE - CONCLUSIONS

*IMPORTANT NOTE: 'Personal data' means data which relate to a living individual who can be identified: (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, And includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Page left intentionally blank.

NHSCFA offices

Coventry

Earlsdon Park
55 Butts Road
Coventry
West Midlands
CV1 3BH

London

4th Floor
Skipton House
80 London Road
London
SE1 6LH

Newcastle

1st Floor
Citygate
Gallowgate
Newcastle upon Tyne
NE1 4WH