NHS
Counter Fraud Authority

Oak Extranet Platform

Data Protection Impact Assessment

October 2021

Version 1.1 Published

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

Document Control					
PM	**Ref**	**Document owner**	**Version No**	**Issue Date**	**Amendments**
Corporate Communications Officer	Oak Extranet Platform	DPO	V0.1	Sep 2020	Initial template completed
Corporate Communications Officer	Oak Extranet Platform	DPO	V0.2	Oct 2020	Amendments
Corporate Communications Officer	Oak Extranet Platform	DPO	V0.3	Jan 2021	Updates to DPO comments
Corporate Communications Officer	Oak Extranet Platform	DPO	V0.4	Oct 2021	Further updates to DPO comments
Corporate Communications Officer	Oak Extranet Platform	DPO	V1.0	Oct 2021	Final
Communication Platform Management Officer	Oak Extranet Platform	DPO	V1.1	May 2023	Slight Redaction. Previous date retained as no change to process.

Prefix	
Reference:	**DPIA Oak Extranet Platform**
Date:	**October 2021**
Author:	**Corporate Communications Officer**
Data Owner:	**Organisation Development Officer**
Version:	**1.1**
Supersedes	**1.0**

Table of contents

Executive summary

This document contains information in relation to the NHSCFA's new extranet platform.

The platform will be an upgrade and move of the existing extranet for the NHS counter fraud community (Directors of Finance/Chief Finance Officers, Audit Committee Chairs, Fraud Champions and Local Counter Fraud Specialists.

It will provide access to information and updates to NHSCFA people and stakeholders on topics to do with the organisation and its work, as well as useful information about organisational updates, guidance and manuals, forms and templates and issues of interest to staff for their day-to-day work.

The extranet is being delivered through a cloud-based solution is hosted using the Microsoft Azure Cloud Services in Dublin, Ireland. A secondary backup region is in the Netherlands for disaster recovery purposes. This is provided by our current intranet supplier Oak Engage Ltd. The name of the solution is Oak.

The extranet will be a web-based service with similar design and functionality to a website, with a variety of applications to perform specific tasks (e.g. online forms and surveys, calendar).

NHSCFA stakeholders and staff are added as users to the system when they are active in their roles as tracked by our stakeholder database. Access is revoked as part of the leavers process when a user leaves their role.

This document is deemed OFFICAL 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'**.

Nothing contained herein should be construed as endorsing any particular Technical Solution to any United Kingdom Government Invitation to Tender.

Links and 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 Privacy 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 Risk Assessments which outline the threats and risks. The Risk Assessment document was developed in accordance with the requirements of NHSCFA and CESG HMG Infosec Standards 1 and 2.

Oak Extranet Platform general description

10. The platform will be a new Extranet service for the NHSCFA stakeholders. It will provide access to information and updates to NHSCFA people and stakeholders on topics to do with the organisation and its work, guidance, forms and templates as well as useful information about organisational policies and procedures and issues of interest to our stakeholders for their day-to-day work.

11. The new extranet will be delivered through a cloud-based solution provided by Oak Engage Ltd (please see below for more information about how data is shared with them). The name of the solution is Oak. This platform is already being used to provide the NHSCFA's staff intranet since December 2018. The Extranet will be a web-based service with similar design and functionality to a website, with a variety of applications to perform specific tasks (e.g. online forms and surveys, discussion forums, document repository).

12. Stakeholders will be added to the system as they're added to CPOD (NHSCFA's counter fraud nomination management system) in an active role. As CPOD is updated the user records will be updated accordingly. NHSCFA staff will be added as users to the system when they join the organisation, as part of the new starter process. Existing users of the current staff intranet have been migrated over to the new system. Access is revoked when a user leaves their role or organisation.

13. For security and confidentiality purposes, the intranet is only accessed by users we enable access for. Some Orchid Software staff may also access the system from time to time for maintenance purposes.

14. This is the only DPIA to be completed for the extranet platform, though an additional one has been completed for the intranet, which runs on the same platform. It has been carried out by the Information and Records Management Officer, in consultation with Senior Corporate Programme Development Officer and the Information Governance and Risk Management Lead.

15. The new Extranet, 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 Extranet 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

[2] Version 0.3 (20180209)

Step 6 - Identify measures to reduce risk

Step 7 - Sign off and record outcomes

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 Extranet will be a secure web-based service with similar design and functionality to a website, with a variety of applications to perform specific tasks (e.g. online forms and surveys, discussion forums, document repository). It will only be accessible by authorised users. While this is a new platform for the Extranet. The Oak platform has been used internally by the NHSCFA since 2018. And prior to that the same supplier provided the organisation's previous intranet platform (Orchidnet), which we have been using for over 6 years.. **The processing will involve collecting the following data for all users:** • name and work contact details • job role • information on system usage Other types of personal data may be provided directly by users themselves (for example by posting on a discussion board or updating their user profile including photograph) or collected with their consent. Because the Extranet is a completely new system to replace the existing one, it is a new technology and therefore a DPIA is required to identify the data it will process.

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?

How will you collect, use, store and delete data?
Contact details and basic information on job role will be collected on CPOD as part of the NHSCFA nomination process. This information will be migrated over into individual user accounts. As a user's role changes or ends on CPOD, this will in turn be updated on the Extranet.

Other personal data such place of work could be entered directly by the data subject as part of their regular use of the system.

What is the source of the data
Personal data can be collected, typically from the data subject themselves as part of their regular use of the system.

Personal data is collected for the following purposes:
- communications on general matters of interest to users (e.g. current work, individual competencies and skills, corporate policies and procedures etc)
- monitoring system usage including user location and device used via Google Analytics to help improve the service

The system will provide the facility to analyse personal data for the following purposes:
- monitoring system usage and improving the service – for example the system may enable us to identify who has not read a certain piece of information for the purposes of sending a reminder. Users will be made aware of this during launch by reference to NHSCFA's Privacy policy on the CFA website.

Will you be sharing data with anyone
Most personal data will only be visible to the data subject and to registered users of the Extranet. Further data (e.g. relating to system usage) will be visible to designated NHSCFA staff with responsibility for maintaining the system.

Personal data may be accessible to Oak Engage staff for service support and maintenance purposes, although this will be regulated by Oak Engage's privacy policy and data can only be accessed for specific purposes as detailed in the service agreement. No other external organisation will have access to the data. Any access from Oak Engage staff to data on our Extranet will be direct, as the intranet will be cloud-based.

Permissions to users will be granted from within the system by NHSCFA people with responsibility for administration and maintenance of the system (admin users). Permissions to Oak Engage staff are granted by Oak Engage in compliance with its own internal policies.

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

None of the processing has been identified as high risk, however as the extranet will be hosted on the Microsoft Azure cloud platform, a range of security measures will be in place to protect the system

and data from unauthorised access. Orchid Software have confirmed that the NHSCFA's extranet platform and all data processed on it will be hosted in data centres within the UK.

Due to the interactive nature of the platform, the users of the platform have the ability to share content. We will have usage guidelines in place to manage risks around the sharing of personal information. Any content identified as breaching the guidelines will be removed and the incident reported as a data breach and remedial action will be taken.

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?

Personal data collected and processed on the extranet will include users' name and work contact details, information about their work and information about their use of the extranet. In addition to this, users may generate personal data through their use of the platform. We expect this will mainly relate to their work but users may occasionally share personal information (e.g. on a charity initiative they are participating in). Users' sharing of information on the Extranet will be regulated by the platform's terms and conditions of use. We do not expect the information will include any special category or criminal offence data, this will also be regulated by the platform's term and conditions of use.

Data about each user will first be collected and processed when the user is given access to the Extranet platform. Data will then be processed on a daily basis, mainly as part of users posting and sharing information on the intranet and as part of monitoring system usage.

Data relating to users' work activities will be kept for as long as the information is relevant to the organisation. Users' personal details will be removed from the system once the user leaves their role or organisation, and the same will happen with data relating to system usage. If usage data relating to a user is required for reporting purposes, it will be kept for no longer than **2 years** after the user has left the organisation.

Due to the nature of the platform, users will also be able to make contributions via the comments function on articles/content. As this data usually will relate to the work of the users and not be personally identifiable data this data will be retained indefinitely.

About 1500 users in England and Wales will be affected by data collection and processing.

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 users of the system will be our stakeholders (Directors of Finance/Chief Finance Officers, Audit Committee Chairs, Fraud Champions and Local Counter Fraud Specialists) at the various trusts and CCGs working in the NHS. Along with members of NHSCFA.

Users can request changes to the personal details provided in relation to them on the extranet, and they will have control over any data they share on the platform. They will be able to view usage data relating to them on request and challenge it if needed by contacting the communications team.

Users will expect their data to be used in the manner proposed.

It is not expected that users will include children or people belonging to vulnerable groups, although if any users are identified as vulnerable measures will be put in place to ensure they are supported in their use of the intranet and their personal data is handled appropriately.

There are no prior concerns nor known security flaws regarding this type of processing, which is not novel for the organisation. Technology in this area has evolved, with greater use being made of cloud-based solutions. As the intranet will be hosted on the Microsoft Azure cloud platform, a range of security measures will be in place to protect the system and data from unauthorised access. More details are available on the entry for Oak on the government's Digital Marketplace at https://www.digitalmarketplace.service.gov.uk/g-cloud/services/127821877641824 (Oak has been approved as a service public sector bodies can procure under a framework agreement).

No issues of public concern should be highlighted. As with all NHSCFA communications, the information posted on the Extranet will be handled in accordance with the terms and conditions of use as well as policies regarding acceptable use, standards of business conduct and policies and procedures relating to information sharing.

The NHSCFA has an ISO ISO27001:2013 certification on information security which covers information processed within the NHSCFA network.

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 main purpose of the data processing is to provide information that meets the needs of our users – NHSCFA stakeholders and staff – and supports them in their day-to-day work. Another important aim is to improve engagement with the NHS counter fraud community by providing better tools for stakeholders to communicate and share information.

The intended effect is for individual users to be more engaged, better informed about the work of the organisation and better able to collaborate on shared goals.

Higher levels of engagement can lead to improved knowledge, greater motivation and ultimately be beneficial to the NHS counter fraud community.

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?

We have sought the views of users through a survey with our intended users and by engaging with a volunteer group of stakeholders.

A project team is in place with representation from across the organisation. Senior management have been involved through our project sponsor (Nicola Burton), and the information governance and information security teams have also been consulted.

We have engaged regularly with the supplier who provide assistance on development and rollout of the system, and sought assurance from them on various aspects of data processing (e.g. location of data centres).

As stated above we have already consulted the information security team, and a risk assessment has been completed for the new extranet.

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?

On the basis of what is set out above, public task seems to be the most appropriate lawful basis for processing.

The organisation as an official authority relies on public task for the processing personal data relating to stakeholders and members of staff for the purposes of providing them with information that is useful and relevant to their work, and enabling them to communicate effectively with each other. The processing set out above is necessary to achieve this purpose. While in theory other channels could be used to achieve the same outcome (e.g. email), a secure intranet platform is the most effective way to do so.

The proposed processing does actually achieve our purpose, as demonstrated by the current NHSCFA intranet, which involves very similar processing – feedback from staff has indicated that satisfaction with the extranet has increased during the last year. Surveys from external users have indicated the additional features the platform provides would be beneficial to their work.

We will prevent function creep by keeping our processing under periodic review – we do not expect the purpose of processing to change following release of the system, unless the platform is used to process sensitive data. If we do introduce new processes, we will update this assessment to reflect this.

Data quality will be ensured by regular checks carried out by the Communications team and the nominations team – there will be, as a minimum, monthly checks of contact information and quarterly checks of information relating to teams and their work. These checks will also identify information relating to staff who have left the organisation, or out of date information, so that relevant personal data can be removed.

Individuals will be informed about personal data held on the platform and about processing through communications sent in advance of live release – this information will be available on the intranet at all times, and contact information will be provided for any queries or support required.

We will periodically seek assurance from the supplier of their continued compliance with applicable data protection rules, and we will work with the information security and information governance teams to flag up and address any concerns. No transfers of data are expected outside the EEA.

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
Use of a cloud-based platform results in compromise or loss of personal data.	Possible	Significant	Medium
Data being shared with third parties by the processor	Remote	Significant	Low
Account compromised	Possible	Severe	High

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
A range of security measures are already in place, and the following measures will be taken to reduce the risk: • monitor Microsoft Azure accreditations to ensure it is still compliant with the required standards • consider activating 2-factor authentication Please see the Information Security team's risk assessment document for more details. Potential users may share confidential information. This can be reduced/prevented by providing terms of use for users to follow and to regularly monitor content shared on the platform.	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: Having reviewed the DPIA I am satisfied that a comprehensive assessment and review of user access, storage and retention of person identifiable data has been undertaken. Personal data is either provided with consent or via direct user input. No sensitive data is collected/held in the system and this is reinforced through the platform's terms and conditions, which users must abide by helping to ensure against the collation and sharing of such data. Access to the system is restricted to nominated users, with access permissions assigned by NHSCFA staff responsible for the administration and maintenance of the system (admin users). Access is also granted to limited platform provider (Oak Engage) staff in accordance with their internal compliance policies, as a consequence all access is fully auditable. All data will be held and governed in accordance with current legislative requirements and handled in accordance with organisational best practice and its data retention policy. I am therefore satisfied with the with the organisational security measures employed.		
DPO advice accepted or overruled by:	Trevor Duplessis - 2nd November 2021	If overruled, you must explain your reasons
Comments		
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 roles and responsibilities:

Table 1 - Roles and Responsibilities

Role	Responsibility
Information Asset Owner (IAO)	Organisation Development Officer
Senior Information Risk Officer (SIRO)	Head of Intelligence and Fraud Prevention
Application/Database Owner	Senior Corporate Programme Development Officer
Data Protection Officer	Trevor Duplessis Information Governance and Risk Management Lead

2. DPIA Report

Section 1: Overview of Data Collection and Maintenance

1. The system will be a new extranet service for the NHSCFA.
2. It will provide access to information and updates to NHSCFA stakeholders and staff on topics to do with the organisation and its work, as well as useful information about organisational policies and procedures and issues of interest to staff for their day-to-day work.
3. The impact level of the Extranet was assessed as CONFIDENTIAL.
4. The following measures briefly describe what controls have been implemented to protect the Extranet and the personal data recorded:
    a. Oak is a 'software as a service' (SaaS) solution, hosted in an external data centre and as such the NHSCFA has no control over security measures in place. However, the credentials, certifications and assertions of both the hosting data centre (Microsoft Azure) and of the software supplier (Orchidsoft) can be checked.
    b. The Microsoft Azure datacentres are certified to a wide range of standards and frameworks including ISO27001, Cyber Essentials Plus and numerous others. The supplier, Orchidsoft, is working towards ISO27001 compliance, and annual penetration tests are performed on Oak. The entire NHSCFA network is in scope of the NHSCFA ISO27001:2013 certification and controls, including local User Access Management. For more details on security controls, please see the Information Security team's risk management document on the Oak Intranet service.
    c. The Extranet is only accessed by internal staff from NHSCFA and nominated counter fraud professionals in the NHS (LCFSs, ACCs, DOF/CFOs), and occasionally by Orchid Software staff for maintenance purposes.

d. The extranet will be linked to the email system (for the sole purpose of sending users email notifications from the system).

e. 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 new extranet.
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 Database/System.

8. The new Extranet will be administered by the NHSCFA's Organisational Development unit and the NHSCFA's Information Systems and Analytics unit.

9. Information in the New Intranet could include: name and work contact details, information on job role and current responsibilities, and information on system usage. Other types of personal data may be provided directly by users themselves (for example by posting on a discussion board) or collected with their consent. An example of this is staff photographs.

10. There is no sensitive data collected in the system. Users will be required to abide to set terms and conditions, which in turn should reduce the chances of sensitive data being shared.

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

a. Access is restricted to internal members of staff within NHSCFA and administrators from Orchid Software.

b. The extranet will be linked to the email system (for the sole purpose of sending users email notifications from the system).

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.

For more details of security measures implemented on the new intranet platform, please see the Information Security team's risk assessment document.

Section 3: Data Retention

12. The new staff intranet Database/System is subject to NHSCFA Data Handling and Storage Policy. There is not currently a specific deletion process for the intranet, but we will delete contact information for users who leave the organisation (although work-related information may remain on the system if still current and relevant for users)

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 1500 members from within NHSCFA including the database administrators and externally amongst our stakeholders (providers of NHS services, NHS commissioners, Trusts, etc.).

Section 5: External Sharing and Disclosure of Data

15. The only information shared with external organisations, would be if it was requested for the administration of justice and with Orchid Software for the purposes of maintenance and support of the system (in accordance with the terms of the contract and support agreement for the delivery of the Oak intranet service).[if shared with other organisations need to state/confirm this is being done in accordance with appropriate Information Sharing Agreement/Memorandum of Understanding]

Section 6: Notice/Signage

16. Is the data subject aware that we hold the data for them? If not, why not?

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 Database/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 any access requests will be received as staff have access to the personal data recorded about them on the New Intranet and as such this is not relevant to the database.

20. In the unlikely event that information is identified as being incorrect, system users will take appropriate steps to correct the record.

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 Database/System is as explained in this DPIA:

The application and the hosting infrastructure was assessed at **Official** and the Microsoft hosting infrastructure is subject to the ISO27001 standard

23. Access is restricted to active stakeholders on NHSCFA's CPOD database and internal staff only.

24. The technical controls to protect the database are as described above in;

Section 1: Overview of Data Collection and Maintenance 4(a)

Section 9: Technology

25. The System holds personal information taken electronically and is located in a Microsoft Azure data centre as explained above.

3. Compliance Checks

DPA 2018 Compliance Check

1. The DPO must ensure that the New extranet, 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.

The Privacy and Electronic Communications Regulations

4. 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

5. 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

6. 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

7. There are no residual privacy risks to the personal data recorded in the Database/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
Project	OAK Extranet Platform

2. Contact position and/or name.
(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

3. Description of the programme / system / technology / legislation (initiative) 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 platform will be an upgrade and move of the existing extranet for the NHS counter fraud community (Directors of Finance/Chief Finance Officers, Audit Committee Chairs, Fraud Champions and Local Counter Fraud Specialists.

It will provide access to information and updates to NHSCFA people and stakeholders on topics to do with the organisation and its work, as well as useful information about organisational updates, guidance and manuals, forms and templates and issues of interest to staff for their day-to-day work.

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

The platform will be an upgrade and move of the existing extranet for the NHS counter fraud community (Directors of Finance/Chief Finance Officers, Audit Committee Chairs, Fraud Champions and Local Counter Fraud Specialists.

It will provide access to information and updates to NHSCFA people and stakeholders on topics to do with the organisation and its work, as well as useful information about organisational updates, guidance and manuals, forms and templates and issues of interest to staff for their day-to-day work.

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 New Intranet 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 platform

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

Cheylesmore House
5 Quinton Road
Coventry
West Midlands
CV1 2WT

London

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

Newcastle

1st Floor
Citygate
Gallowgate
Newcastle upon Tyne
NE1 4WH