NHS
Counter Fraud Authority

New Intranet

Data Protection Impact Assessment

July 2022

Version 3.0 Published

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

Document Control					
PM	**Ref**	**Document owner**	**Version No**	**Issue Date**	**Amendments**
Senior Corporate Programme Development Officer	DPIA Staff Intranet	DPO	V0:1	10/07/2018	Initial template provided
Senior Corporate Programme Development Officer	DPIA Staff Intranet	DPO	V0:2	29/03/2019	Comments from Information Governance
Senior Corporate Programme Development Officer	DPIA Staff Intranet	DPO	V0:3	29/03/2019	Updates from previous versions
Senior Corporate Programme Development Officer	DPIA Staff Intranet	DPO	V1:0	10/05/2019	Final updates for authorisation
Senior Corporate Programme Development Officer	DPIA Staff Intranet	DPO	V2:0	13/05/2019	Authorised and prepared for publication
Senior Staff Learning and Development Officer	DPIA Staff Intranet	DPO	V2.1	08/07/2022	Additional content added to pages 4,7,8,9,11 & 20 in relation to PDP/OPD records
Communication Platform Management Officer	DPIA Staff Intranet	DPO	V3.0	18/05/2022	Slight Redaction. Previous date retained as no change to process.

Prefix	
Reference:	DPIA/New Intranet
Date:	July 2022
Author:	Senior Corporate Programme Development Officer
Data Owner:	Organisation Development Manager
Version:	3.0
Supersedes	2.1

Table of contents

Executive summary

This document contains information in relation to the NHSCFA's new staff intranet.

The system will be a new intranet service for the NHSCFA.

It will provide access to information and updates to NHSCFA 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.

It will also be used to facilitate the PDP and OPD process which can include third party opinions/reference to an individual's performance/capability/current disciplinary matters etc.

The new intranet is being delivered through a cloud-based solution provided by our current intranet supplier Orchid Software. The name of the solution is Oak.

The intranet 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, organisational calendar).

NHSCFA staff are added as users to the system when they join the organisation, as part of the new starter process (existing Go2 users have been migrated over to the new system). Access is revoked as part of the leavers process when a user leaves the organisation.

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 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.

Name of database/system general description

10. The system will be a new intranet service for the NHSCFA. It will provide access to information and updates to NHSCFA 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. It will also be used to facilitate the PDP and OPD process which can include third party opinions/reference to an individual's performance/capability/current disciplinary matters etc.

11. The new intranet will be delivered through a cloud-based solution provided by current supplier Orchid Software (please see below for more information about how data is shared with them). The name of the solution is Oak and a test version (beta) of this solution was made available to NHSCFA staff in December 2018. The intranet 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, timesheet, organisational calendar).

12. 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 as part of the leavers process when a user leaves the organisation.

13. For security and confidentiality purposes, the intranet is only accessed by staff from the NHSCFA. 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 on the database and 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 intranet, 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 Database/System 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 intranet 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, news articles, organisational calendar).

This is a new system, however our current intranet runs on an older platform (called Orchidnet) from the same supplier, which we have been using for over 6 years. This product was customised for use by NHS Protect (and later the NHSCFA), this would also be the case for the new system.

The processing will involve collecting the following data for all users:

- name and work contact details
- information on job role and current responsibilities
- PDP and OPD information
- information on system usage

The following personal data may in future be collected for all users, depending on which applications are activated on the new intranet:

- working patterns
- absences and leave
- calendar entries (e.g. meetings, appointments)

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.

Because the intranet 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 and responsibilities will be collected by NHSCFA staff responsible for intranet content as part of the migration to the new system.

Other personal data will typically be entered directly by the data subject (or in some cases by their line manager) as part of their regular use of the system.

What is the source of the data
Personal data is collected typically from the data subject themselves as part of their regular use of the system. In some cases it may be collected from their line manager (e.g. if they have to authorise/confirm an absence) or from a designated team representative (e.g. if information is collected from team reps about current work activities).

Personal data is collected for the following purposes:
- internal communications on general matters of interest to staff (e.g. current work, individual competencies and skills, corporate policies and procedures, charity initiatives etc)
- to facilitate the PDP/OPD process
- monitoring system usage and improving the service

In future, personal data may also be collected for management and reporting purposes (e.g. absences, working patterns), depending on which applications are activated on the system.

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

In future, the system will enable the analysis of personal data for management and reporting purposes, for example on absences and working patterns.

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

Personal data may be accessible to Orchid Software staff for service support and maintenance purposes, although this will be regulated by Orchid's privacy policy and data can only be accessed with our express permission. No other external organisation will have access to the data. Any access from Orchid Software staff to data on our intranet will be direct, as the intranet will be cloud-based.

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

The intranet will be linked to the email system (for the sole purpose of sending users email notifications from the system). In future it may also be linked to the active directory (for the purposes of user identification/login), although initially this may not be possible as Oak is a cloud-based product

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

None of the processing has been identified as high risk, however 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. Orchid Software have confirmed that the NHSCFA's intranet platform and all data processed on it will be hosted in data centres within the EEA.

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 intranet will include users' name and work contact details, information about their work and information about their use of the intranet. 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 intranet will be regulated by the platform's terms and conditions of use.

The intranet will also be used to facilitate the PDP and OPD process which can include third party opinions/reference to an individual's performance/capability/current disciplinary matters etc. PDP information however, will be locked down to ensure that it is only visible to the authoring individual, their line manager and one internal administrator. Similarly, OPD information is only visible to the authoring individual, their line manager and the HR Lead' We do not expect the information will include any special category or criminal offence data.

Data about each user will first be collected and processed when the user is given access to the intranet 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 the 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 one year after the user has left the organisation.

About 170-180 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)?

Users will be NHSCFA employees or contractors working within NHSCFA teams on a temporary basis. Users will also include members of NHS Counter Fraud Service Wales, who are employed by the NHS in Wales but are accountable to the NHSCFA for operational matters.

Users will have control over the personal details provided in relation to them on the intranet, as well as on 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, in fact this is already largely the type of data processing carried out on the current intranet (the main areas of change relate to the ability for users to post and share information on the intranet itself).

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 internal NHSCFA communications, the information posted on the intranet 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 organisation has an ISO ISO27001:2013 certification on information security which covers the provision of a staff intranet.

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 staff – and supports them in their day-to-day work. Another important aim is to improve staff engagement by providing better tools for staff to communicate and share information.

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

Higher levels of staff engagement can lead to greater motivation and ultimately to the organisation being better able to meet its strategic aims and objectives.

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 surveys and by engaging with all teams through intranet champions. Senior management have been involved through our project sponsor (first John Manuel, then Nicola Burton), and the information governance and information security teams have also been consulted.

We have engaged regularly with suppliers 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 reviewed a draft risk assessment they have completed of the new intranet.

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, legitimate interests seems to be the most appropriate lawful basis for processing.

The organisation has a legitimate interest in processing personal data relating to 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 intranet has increased during the last year, even though there is demand for a new and updated platform.

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 new applications are activated (e.g. timesheet). If we do look into activating new applications we will update this assessment to reflect this.

Data quality will be ensured by regular checks carried out by the Communications team and by intranet champions – 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 suppliers of their continued compliance with applicable data protection rules, and we will work with the information security and information governance team 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

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 by SMT Owner** 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 • investigate options around 2-factor authentication Please see the Information Security team's risk assessment document for more details.	Reduced	Medium	To be agreed and initialled by SMT Lead Noted A Sturgess Head of Business Support 12.1.23

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 13 May 2019	If overruled, you must explain your reasons
Comments: I am satisfied having reviewed the DPIA that a comprehensive assessment has been undertaken of the system. Access to the software system is restricted to limited numbers of NHSCFA staff with occasionally access by Orchid Software staff for maintenance purposes only, thereby enabling system access to be fully auditable and removed when no longer required. Personal information collected and processed by the system will not include special category or criminal offence data and will be subject to periodic review to ensure that it is not kept longer than is necessary in the accordance with the organisation's data retention policy.		
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 New Intranet roles and responsibilities:

Table 1 - Roles and Responsibilities

Role	Responsibility
Information Asset Owner (IAO)	Organisation Development Manager
Senior Responsible Officer (SRO)	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 intranet service for the NHSCFA.
2. It will provide access to information and updates to NHSCFA 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 Intranet was assessed as CONFIDENTIAL.
4. The following measures briefly describe what controls have been implemented to protect the Intranet 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 Intranet is only accessed by internal staff from NHSCFA, and occasionally by Orchid Software staff for maintenance purposes.
    d. The intranet will be linked to the email system (for the sole purpose of sending users email notifications from the system). In future it may also be linked to the active directory (for the purposes of user identification/login), although initially this may not be possible as Oak is a cloud-based product.

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 staff intranet.
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 Intranet 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, PDP/OPD information 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 database.

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 intranet 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 170 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 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, NHSCFA staff 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 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 Database/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 Intranet, 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	New Intranet

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 system will be a new intranet service for the NHSCFA. It will provide access to information and updates to NHSCFA 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.

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 system will be a new intranet service for the NHSCFA.

It will provide access to information and updates to NHSCFA 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.

Access is restricted to staff within NHSCFA. Some Orchid Software staff may also access the database occasionally for maintenance purposes.

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 database

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

7th Floor
10 South Colonnade
Canary Wharf
London
E14 4PU

Newcastle

1st Floor
Citygate
Gallowgate
Newcastle upon Tyne
NE1 4WH