NHS
Counter Fraud Authority

Email Service – Incorporating Microsoft Exchange / Outlook and Barracuda Total Email Protection

Data Protection Impact Assessment

September 2023

V1.0 Published

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

Executive Summary

This document contains information related to Microsoft Exchange Online (EOL) and Barracuda Total Email Protection (TEP).

TEP is a cloud hosted suite that provides a number of services for Office 365 customers, these include Email Security, Advanced Threat Protection, Cloud to Cloud Backup, Email Archiving, Forensic Investigation and Incident Response, Sentinel (phishing detection) and PhishLine (phishing educational campaigns). TEP processes and currently stores data in Barracuda's own UK datacentre. This is due to be changed within the next 12-18 months with a planned migration into Microsoft Azure's UK datacentres.

TEP Email Security processes and logs all inbound and outbound external emails. It uses an active Advanced Threat Protection system and Anti-Phishing database maintained by Barracuda to detect live phishing, ransomware and malware attacks, viruses and trending spam emails and blocks them outright or quarantines them. Emails and attachments are scanned in a sandboxed environment to ensure any risks or threats are not transmitted onwards into EOL.

To clarify the mail flow, the Email Security service provides an added layer of security in front of EOL. Inbound emails are processed by TEP and if deemed to be safe are then passed on to EOL. Outbound emails sent from Outlook reach EOL first and are then passed on to TEP for onward transmission. Emails sent internally within the organisation stay within EOL.

TEP Cloud to Cloud Backup service is used to backup all Office 365 related data and store it in the Barracuda's Cloud in the UK datacentre. This covers all email, Teams documents and chats, SharePoint, OneDrive and Groups data. The storage capacity and retention period is unlimited.

TEP Archiving service stores a copy of every sent and received email, contact, task, public folder and calendar item for preservation. They will be retained for six years in line with the Data Retention Schedule.

TEP Forensic Investigation and Incident Response is a service that will be used by CFA staff to report suspicious emails received in Outlook to the Information Security Team. Once reviewed if an email is deemed to be a risk it can be removed from every mailbox that is has entered.

TEP Sentinel is an AI based email protection service that's used to detect and prevent spear phishing attacks, account takeovers and email fraud.

TEP PhishLine service is a proactive tool that's used to bring to the attention of staff the different types of phishing attacks and what they should look out for. The campaigns can be highly customised to use current affairs, news items or organisational information that real life attackers would use to look for across different platforms such as email, text and voicemail. Address books in PhishLine are populated with CFA staff specific details such as email address and mobile number so that targeted or more generic campaigns can be implemented.

Exchange Online (EOL) is a cloud hosted service that's used for the management and delivery of emails. It's used to store all user and shared mailboxes, global address book and for email delivery internally and outbound. Policies covering email retention and archival are set and applied in EOL.

To ensure emails received by users are as safe and clean as possible rules are configured in EOL in addition to TEP to block emails from malicious or suspicious senders should anything unsolicited get through. EOL is also configured to add specific words in the email header depending upon the classification that has been selected.

A Message Records Management (MRM) policy has been applied to all user and shared mailboxes that retains emails for a two year period from the date of receipt, this is the Microsoft default. On expiry the emails are moved into the associated online archive mailbox where they are retained for a period of six years. Items that have been deleted and reside in the Deleted Items folder are purged after 30 days.

Any information viewed/obtained within this document should be treated in the appropriate manner as advised and set out in the Government Security Classifications (June 2023).

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

Government Security Classifications Policy June 2023.docx (publishing.service.gov.uk)

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'**

The document is subject to CROWN COPYRIGHT. It is provided in confidence under existing laws, regulations and agreements relating to the protection of data and shall be so protected. The information contained herein is proprietary and shall only be used for the purposes intended at release. It shall not be reproduced, adapted or used in, whole or in part, for any other purpose without the prior written consent of the Secretary of State for DEPT in the Government of the United Kingdom.

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

Table of contents

Document Control					
PM	**Ref**	**Document owner**	**Version No**	**Issue Date**	**Amendments**
Security and Operational Support Analyst	DPIA Microsoft Exchange-Outlook	Trevor Duplessis	V0.1	October 2020	Initial creation
Security and Operational Support Analyst	DPIA Microsoft Exchange-Outlook	Trevor Duplessis	V.02	January 2021	Response to Comments/Review
Security and Operational Support Analyst	DPIA Microsoft Exchange-Outlook	Trevor Duplessis	V.03	March 2021	Final Comments/Queries
Security and Operational Support Specialist	DPIA Email Services	Trevor Duplessis	V.04	June 2021	Amended to widen the scope to Email Services incorporating Barracuda TEP and to update and clarify retention and archiving policies
Security and Operational Support Specialist	DPIA Email Services	Trevor Duplessis	V1.0	September 2023	Finalised following confirmation of retention periods

Prefix	
Reference:	**DPIA Email Service**
Date:	**September 2023**
Author:	**Security and Operational Support Specialist**
Data Owner:	**All Corporate Information Asset Owners**
Version:	**1.0**
Supersedes	**0.4**

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	June 2023	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 it 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 affect 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. A separate risk assessment is conducted to outline the threats, risks and security countermeasures involved in the solution.

Microsoft Exchange Online (EOL)

10. The purpose of Exchange Online (EOL) is to provide an email delivery service as well as protect against the receipt of malicious emails. EOL functions as an email server for the sending, receiving and storing of emails as well as for managing personal and shared email accounts and their subsequent permissions.

11. EOL processes emails that are sent and received by users and from shared mailboxes within the organisation. Emails sent are stored within the Outlook client locally and is synchronised with the Exchange mailbox, a copy is sent to the recipient. If the recipient's mailbox no longer exists, is full or the email sent was rejected by the recipient's IT Security Policy the sender might receive a notification to that effect. The MRM retention and archive policy stated previously in the Executive Summary is managed in the Exchange admin centre. Emails are stored in the mailboxes for a period of two years before being moved into the associated online archive mailbox.

EOL checks all emails that it processes against Microsoft's phishing/malicious emails database to determine if they are suspicious, junk or spam. It also checks them against rules set by Exchange Administrators within the NHSCFA.

The EOL admin centre enables Administrators to search the email logs for specific items using the Message Trace function. The search results do not contain the actual content of the email, only the Sender, Recipient, Time/Date, Subject and Status information is available.

12. It is the email sender's responsibility to ensure that the appropriate security marking has been applied.

13. EOL is administered using role based permissions and this has been restricted to a limited number of staff in the ISA Systems and Security teams. Users by default can only access their own mailbox. Access to shared mailboxes is applied using Active Directory linked security groups that have a prefix of EG_.

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

15. The System, 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.

Barracuda Total Email Protection (TEP)

16. The main purpose of Barracuda Total Email Protection (TEP) is to provide an added layer of security to the organisation's email system. It also provides the functionality to back up critical data that's stored in the various Office 365 applications so it can be restored in the event of accidental deletion, in a Disaster Recovery scenario or to recover from a ransomware attack for example. TEP also enables the Information Security team to conduct proactive phishing campaigns to help staff to identify the tell-tale signs of phishing emails. The other functions of TEP have been described previously.

17. The TEP Email Security service processes emails as they are received and it carries out a number of critical actions to determine whether they are acceptable for onward delivery. The sender is checked to see if they are genuine, to make sure the sending account is not being impersonated. It checks to make sure the sender is authorised to send emails from the specified domain and that the sending IP address is registered to that domain. The email content is also checked for integrity to ensure it hasn't been tampered with and finally the content is given a SPAM score. If the score is higher than 5.0 the email is blocked, if it's higher than 3.0 it's quarantined and lower than 3.0 it is delivered.

18. Emails and attachments are scanned for viruses and malicious code in a sandbox environment which prevents the TEP solution from being compromised or infected. It also connects to a vendor maintained database to see if the sender, recipient(s), subject or body contain keywords or content that has been flagged as suspicious.

19. Rules can be applied to allow or block emails from specific domains, email addresses, countries or languages. Attachments can be blocked based on the file extensions and rules can be applied to pick out keywords in different fields.

20. A message log is kept of all emails that have been sent and received through TEP. The message log and quarantined emails are retained for 30 days and then deleted.

21. The TEP services are managed in a Cloud Control administration console and access is restricted currently to members of the Information Security team using administrative permissions. Administrators are able to view the full email content, header information, view attachments and download the email as a file. They can also re-deliver an email if it wasn't received. Administrators also have the ability to create and amend policies and create and amend allow/block rules. The policies and block/allow rulesets are applied in TEP and EOL to ensure mail flow is secure and protected

22. This is the only DPIA to have been completed for Barracuda TEP.

Data Protection Impact Assessment

16. To ensure the 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.

Microsoft EOL and Barracuda TEP are both cloud hosted services that process email data and store it in Microsoft's and Barracuda's UK datacentres. The underpinning infrastructure is maintained by Microsoft and Barracuda respectively. The services are used to:

- Provide a robust, secure and resilient email delivery system
- Permit the sending and receiving of emails internally and externally
- Actively prevent and detect malicious emails and remove them from mailboxes if found
- Provide a system for archiving emails
- Enable storage capacity management and email retention using policies
- Provide a solution for backing up and restoring data
- Provide a proactive and reactive Phishing

The NHSCFA migrated email services from IBM Notes to EOL in 2020 and this was followed by a migration of email security functionality from Barracuda's on-premise Email Security Gateway to TEP in February 2021. Due to the nature of email systems and gateways they process a large quantity of data which covers many data types and potentially Official-Sensitive communications. A DPIA was deemed necessary to identify the processes and justify why they exist.

The type of data that can be processed by TEP and EOL includes personal and sensitive information as well as information of more mundane nature. The information processed depends entirely upon the information sent by users within and outside of the organisation, as such we have put measures in place to ensure that what is sent and received is safe and secure. The majority of data processing is automated as TEP and EOL will check against the vendor managed databases and frameworks, policies and rulesets and apply automated delivery actions to safe emails as well as blocking or quarantining malicious emails.

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?

A record of every email, sent or received externally, is stored in TEP for 30 days and a copy of emails sent internally and externally through EOL for the period set out in the Microsoft MRM policy (currently two years in a mailbox and then archived for six years in line with the Data Retention Schedule.

The data is received when an email is sent or received by staff. As such the data is sourced from both inside and outside of the organisation.

The emails stored within EOL are only accessible to users within the organisation. The email contents themselves are only accessible to the sender or recipient of the email as well as anyone who has permissions to view that mailbox.

It is highly likely that emails will contain Personal Identifiable Information (PII) or financial details relating to investigations or HR related matters for example. Due to the processing of data being predominantly automated there is limited room for human error. As previously mentioned, access to email content is not available in the EOL admin centre Message Trace function only limited header information is visible but TEP does allow Administrators full access to emails that have been processed. One risk associated with email processing is user error on entering a recipient address into the To field.

Details of processing are detailed in the 'Scope of Processing' below

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?

The data processed and stored in TEP and EOL consists of emails sent and received by users within the organisation. As these emails have no form of input validation they can contain any type of information as well as information of any sensitivity. As such, this information can contain special category data and, due to the nature of the work the NHSCFA conducts, there is a potential that this will include Criminal Offence Data.

The email services provided by TEP and EOL by design will collect all information related to an email. This includes the sender, recipient, subject, send time, status, attachments and message body. This is required for the successful completion of the service. As previously described, controls are in place to limit who can access this data.

The data is collected and processed constantly to provide a constant mail processing service.

Users no longer have the option in Outlook to set retention policies on individual emails. This has been removed to prevent any conflict or non-compliance. The default Microsoft MRM retention and archiving policy of two years then for six years is applied to every user and shared mailbox and it cannot be overridden.

All users who have access to the email solution are affected. Emails sent into the organisation will be retained according to the above policy processed as previously described.

In theory emails can be sent from anywhere in the world however they are more likely to be sent from within the United Kingdom as the NHSCFA is a national body so there is limited requirement for communications outside of the country.

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)?

As these are public facing systems there are users who will have their information processed that we will not know. The relationship with internal users is they are members of staff.

External users have no ability to manage retention or how the email is managed once inside the Exchange service. Internal users can manage their emails retention policy.

When an individual sends an email to an organisation there is the expectation that it will be processed and checked for malicious code/viruses before being stored on the email solution for a period of time.

Children or vulnerable groups are able to send emails to the organisation and as such their information could potentially be processed. Unless the individual identified themselves as such there would be limited ways of identifying this information.

This type of processing for email services is considered standard. Access is restricted and auditable.

The email services provided are not novel, they are industry standard.

Despite migrating to cloud hosting for email services the actual technology being used has not changed significantly. Email delivery is more secure and robust than it has ever been but the actual process and data requirements of sending an email are largely the same as they were 5 years ago.

There are no issues of public concern that need to be factored in. Emailing an organisation comes with the expectation that the email will be processed against a rule set and stored as per the organisation's retention policy.

No.ISO27001 compliance ensures that data is managed and processed securely by the CFA. Risks are identified and logged and measures are put in place to resolve or mitigate them.

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 processing of email information is required to provide an effective email management service. The emails need to be compared against rules set by the NHSCFA, Barracuda and Microsoft to reduce the number of spam and malicious emails that enter the estate. It is also required to provide a mitigation against data loss and provide correct data classification and protections.

The effect on individuals should be limited. Suspected spam and malicious emails should be blocked while valid emails should be allowed through.

The benefits of this mainly come from a more secure environment and an improvement in email quality received by users.

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?

As the data processing in this situation is not excessive then individual views are not required. The processing carried out in this situation is what is expected and considered standard as part of an email management solution. The emails are processed against rules set by Barracuda, Microsoft and the NHSCFA. Access to the content of the emails is restricted to those with access to either the sender or recipient mailbox and designated Administrators in the Information Security team.

The policies regarding the retention are covered in the organisations Data Handling and Retention policy. As such users should be aware of the retention policy that the organisation will follow.

No.

Advice on the setup has been sought online and through other security professionals to advise on how to setup a secure environment to process emails.

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 email information by the services covered in this document is required for the running of a secure email system as such the data collection is not excessive and required therefore it has a basis in law. It follows points e in article 6 of the GDPR:

(e) 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.

Yes. The processing of the information is required to provide the email management service itself.

Not a feasible way. The To and From is required to identify a sender and recipient, data and time is required for chronological ordering and auditing, the subject is required for further identification purposes, the status is required for troubleshooting and the content is required to make the communication useful.

New features or functions will be assessed and tested before being deployed into production.

As we do not edit the information, only process it we have no real control over the quality of information as this is up to the user. Other than the To and From address, there's no input validation on a user's email. As such the confirmation contained therein can be of varying quality. The input validation on the To and From fields is limited to that of a valid email address, it can still be an incorrect one.

Users are made aware that their emails will be processed as part of the email management system to the degree that is required to maintain the solution and protect the network.

The actual contents of emails cannot be accessed by anyone who does not have access to a sender or recipient mailbox involved in the communication.

Administrators are limited in their ability to modify the processing rules and any changes made will be fully auditable.

No change is made to processing based on location. Be the sender national or international.

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 Administrator – An administrator in TEP and or EOL, through accident or malicious intent, uses the service in a way that causes damage for the organisation. Administrators can provide themselves with access to mailboxes. This could be done to delete emails, send emails on behalf of others and so forth. This action would be fully auditable, and all members of the CFA undergo security checks prior to and throughout employment.	Remote	Severe	Medium
Physical Intruder – Someone could access a Barracuda or Microsoft Data Centre and remove or damage hardware used to provide the email services to the CFA. Data Centre locations are not revealed and there are many on site security measures as well as back-ups of services and data across multiple sites.	Remote	Severe	Medium
External Attacker – Through a breach in the CFA network or Microsoft's network an attacker could potentially delete information, send emails or modify permissions leading to harm to the CFA's reputation and ability to perform its role. This doesn't apply to TEP as it cannot send emails directly, it processes and delivers emails into and out of EOL. Microsoft and the CFA have multiple security measures in place to mitigate against such attacks.	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 by SMT Owner** Yes/No
Microsoft Data Centres meet various standards (https://docs.microsoft.com/en-gb/microsoft-365/compliance/offering-home?view=o365-worldwide) and numerous physical security measures in place to reduces the likelihood of a successful break in. Staff are also vetted to reduce the likelihood of a member of their staff causing these issues.	Reduced	Medium	Yes
Barracuda currently leases space in private and public data centres. https://www.barracuda.com/company/legal/trust-center/security-compliance Migration of all data into Azure regional datacentres is an ongoing project which is due to complete with 12-18 months. Barracuda and Microsoft have numerous security measures in place (See links above) to mitigate against physical and logical attacks. We also make use of Multi-Factor Authentication on administrator accounts to further reduce the likelihood of a successful compromise.	Reduced	Medium	Yes

STEP 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	Ann Sturgess	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Ann Sturgess	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:		If overruled, you must explain your reasons
Comments: Having reviewed the DPIA I am satisfied that a comprehensive assessment of the Microsoft Exchange Online (EOL) and Barracuda Total Email Protection (TEP) platform has been carried out. TEP is a cloud hosted suite that provides a number of services for Office 365 customers, these include Email Security, Advanced Threat Protection, Cloud to Cloud Backup, Email Archiving, Forensic Investigation and Incident Response, Sentinel (phishing detection) and PhishLine (phishing educational campaigns). TEP processes and currently stores data in Barracuda's own UK datacentre. EOL is administered using role-based permissions and this has been restricted to a limited number of staff in the ISA and Security teams. The TEP services are managed in a Cloud Control administration console and access is restricted currently to members of the Information Security team using administrative permissions. Administrators are able to view the full email content, header information, view attachments and download the email as a file. They can also re-deliver an email if it wasn't received. Administrators also have the ability to create and amend policies and create and amend allow/block rules. The policies and block/allow rulesets are applied in TEP and EOL to ensure mail flow is secure and protected. All of which is fully auditable. All data processed is 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 organisational security measures employed.		
Consultation responses reviewed by:	Trevor Duplessis - 8th September 2023	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 Exchange Online roles and responsibilities:

Table 1 - Roles and Responsibilities

Role	Responsibility
Information Asset Owner (IAO)	All Corporate Information Asset Owners
Senior Information Risk Owner (SIRO)	Head of Intelligence and Fraud Prevention
Application/Database Owner	Information Systems and Security Team
Data Protection Officer	Trevor Duplessis Information Governance and Risk Management Lead

2. DPIA Report

Section 1: Overview of Data Collection and Maintenance

1. Exchange Online is a replacement for the previous IBM Notes solution. It is being used to provide an email management service. This involves providing a front end for receiving emails.
Barracuda TEP is a replacement for the on-premise Barracuda Email Security Gateway. It provides the same security controls to inbound and outbound emails and also has additional functionality such as Office 365 backups, email archiving and phishing campaigns.

2. The data will include information contained within emails.

3. The impact level of Microsoft Exchange (EOL) was assessed as OFFICIAL and it can only be accessed internally. TEP can only be accessed internally and currently is restricted to the Information Security team.

4. The following measures briefly describe what controls have been implemented to protect the EOL and TEP systems and the personal data recorded:

   a. EOL is accessible to all staff however administration is limited to specific users within the Information Systems and Security teams.

   b. TEP is not accessible to staff. It can only be managed by the Information Security team.

   c. The EOL System does have direct interconnections with other NHSCFA systems and applications. These applications are Teams and Azure AD.

   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 Exchange Online 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. The purpose of EOL and TEP is to provide secure email functionality as well as protections against malicious threats and attacks. EOL functions as an email server for sending, receiving and storing emails as well as for managing personal and shared email accounts and their subsequent permissions. TEP provides a secure layer between EOL and the wider internet.

8. The Information Security Team is responsible for administration and support of TEP and EOL is administered between the Information Security and Systems teams.

9. Emails processed in TEP and EOL are likely to contain sensitive information such as PII or financial details relating to investigations. Whilst the email system has limited input validation the CFA does have a solution called Stealthbits that scans emails and mailboxes for sensitive data and flags it up. It can then be reviewed and managed accordingly to ensure users are following the organisation's acceptable use policy for example.

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

a. All users have access to their own email mailboxes and shared mailboxes if they have been given specific access in EOL. Administration access is limited to some members of the Information Security and the Information System teams.

b. Users do not have access to TEP. Administration access is currently restricted to the Information Security team.

c. EOL does have a direct interconnection with other NHSCFA systems such as Teams and Azure AD.

d. 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

11. Emails stored in EOL are retained in the user and shared mailboxes for a period of two years before they’re moved to an associated online archive mailbox. Office 365 suite data including email that has been backed up and archived by TEP are retained for six years.

12. 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

13. All users have access to Exchange Online however administration access is limited to 6 members of the Information Security and the Information System teams.

Section 5: External Sharing and Disclosure of Data

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

Section 6: Notice/Signage

15. 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.

16. 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

17. 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.

18. It is unlikely that many access requests will be received as the personal data recorded is all in relation to communications sent by individuals as such there is an assumed acknowledgement that the information will be stored and processed before being sent onto the intended recipient.

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

20. 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

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

Barracuda and Microsoft host the environment and meet numerous standards:

https://docs.microsoft.com/en-gb/microsoft-365/compliance/offering-home?view=o365-worldwide

https://www.barracuda.com/company/legal/trust-center/security-compliance

22. Access to the TEP Cloud Control administration console is restricted to Information Security internal staff only and access to the EOL admin centre is restricted to a limited number of Information Systems and Security staff.

23. The technical controls to protect the database include:

a. Anti-virus protection;

b. Permission based access controls to the service.

c. Logging, audit and monitoring controls.

d. Vulnerability Patching Policy for the underlying infrastructure.

Section 9: Technology

24. The System holds personal information taken both by telephone and electronically and is located in a Barracuda and Microsoft Azure UK Data Centre.

3. Compliance Checks

DPA 2018 Compliance Check

1. The DPO must ensure that the Email Service (incorporating Barracuda TEP, Exchange and Outook), 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 processes sensitive personal data so a Data Protection Compliance Check Sheet has been completed describing how the requirements of GDPR and the Data Protection Act 2018 have been complied with, see Annex B

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 Security
Project	IBM Notes to Exchange and Mail Gateway Migration

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	Corporate Affairs, 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.

Exchange Online is a replacement for the previous IBM Notes solution. It is being used to provide an email management service. This involves providing a front end for receiving emails, a mechanism to process the emails against rulesets set by both ourselves and Microsoft. It is also used to provide a storage area for emails and email attachments as well as a hub for setting data retention based policies.

Barracuda TEP is a replacement for the on-premise Barracuda Email Security Gateway. It provides the same security controls to inbound and outbound emails and also has additional functionality such as Office 365 backups, email archiving and phishing campaigns.

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 provide a secure and robust email management and delivery solution to send and receive emails, process them against threat databases, rules and store them.

EOL access is available to all members of staff however administration is restricted to members of the Information Security and Information Systems teams. TEP cannot be accessed by anyone outside of the Information Security team.

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 TEP and EOL systems have 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

9th Floor
Earlsdon Park
55 Butts Road
Coventry
West Midlands
CV1 3BH

London

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

Newcastle

1st Floor
One Citygate
Gallowgate
Newcastle upon Tyne
NE1 4WH