WILTSHIRE POLICE

XXXXXXXX
By email

Force Disclosure Unit
Police Headquarters
London Road
DEVIZES
Wiltshire
SN10 2DN

Date 10th July 2025 **Our Ref** FOI 2025-604

Dear XXXXX,

I write in connection with your request for information dated 23rd June 2025, concerning M365 DPIAs.

I am required by the Freedom of Information Act 2000 to handle all requests in a manner that is blind as to the identity and motives of the requestor. Any information released as a response to a request is regarded as being published and therefore in the public domain without caveat.

Following receipt of your request, research was conducted by the Data Protection Officer at Wiltshire Police.

Your request for information has now been considered and I am able to respond as follows.

You wrote:

Please could I put in an FOI request for a copy of the m365 DPIAs to include the main overarching one that was done years ago and the smaller ones for the products/tools.

Our response:

Please note, our Data Protection Officer believes the main overarching M365 DPIA requested refers to the National Police Digital - Service National Enabling Programmes (NEP) DPIA. The NEP DPIA is a national one and Wiltshire Police do not hold a finalised version of this. As such, we would advise you contact the national owner to request a copy of this - we believe this is the Police Digital Service (https://pds.police.uk/).

Please find the below DPIAs attached at the end of this response letter.

- DPIA Report for Microsoft O365 SharePoint
- DPIA Report for Microsoft Teams
- DPIA Screening (Stage 1) for MS Whiteboard

Some of the information relevant to this request is exempt by virtue of Section 31(1)(a)(b) - Law Enforcement and Section 40(2) - Personal Data.

- Section 31 is a qualified prejudice-based exemption and therefore requires Wiltshire Police to establish the harm in disclosure, along with the public interest favouring and against disclosure.

- Section 40 is an absolute exemption and therefore there is no requirement to articulate the harm or conduct a Public Interest test.

Section 31

Harm test

Disclosing information into the public domain - specifically details relating data storage locations, permissions, privacy / security settings and risk assessments - would undermine the core principles of policing; namely to prevent and detect crime. Disclosing this information would cause substantial harm to the Force should those with criminal intent use this to access information combined to find a way to access our internal systems; thus, prejudicing our ability to prevent and detect crime, and to apprehend or prosecute offences, ultimately effecting the Force's ability to protect the community.

Factors favouring disclosure

It is in the public interest that Wiltshire Police are open and transparent, allowing us to be held accountable for our actions. Disclosing details relating to data storage locations, permissions, privacy / security settings and risk assessments would demonstrate to the public how the Force are taking actions to maintain our computer systems and the integrity of the information held.

Factors against disclosure

Disclosing specifics on data storage locations, permissions, privacy / security settings and risk assessments would allow those with criminal intent to identify any weaknesses within the security of these systems, allowing them to gain access to any sensitive and operational information stored there. Investigations would be compromised, as these individuals would be able to access valuable information to assist them in evading capture. By evading capture, the public will be put at a greater risk, resulting in trust in the Force diminishing and increase of crime being seen. This would also have a severe impact on the Force's resources, which in turn also assists those individuals to evade capture.

Balance test

Whilst there is a public interest in transparency and openness between the Force and the public, in addition to the public seeing how the Force are engaging with the threat from criminals, there is a stronger interest in ensuring the public are protected from the threat of criminals, and that the enforcement of the law and the prevention and detection of crime is upheld. To disclose information which is likely to assist offenders would seriously undermine the effective delivery of operational law enforcement and is therefore exempt from disclosure.

Section 40

Information which constitutes personal data is exempt under Section 40(2) of the FOIA if it relates to a third party, and the disclosure to the public would contravene the data protection principles set out in Section 34 of the Data Protection Act 2018 and Article 5 of the GDPR.

Section 17 of the Freedom of Information Act 2000 requires the Constabulary, when refusing to provide information (because the information is exempt) to provide you the applicant with a notice which: (a) states that fact, (b) specifies the exemption in question and (c) states (if that would not otherwise be apparent) why the exemption applies.

In accordance with the Freedom of Information Act 2000 this letter acts as a Refusal Notice for those aspects of your request.

Exemptions applied:

Section 31(1)(a)(b) - Law Enforcement

Section 40(2) - Personal Data

I am satisfied that all the relevant information has been passed to me and been considered in the light of your request within the time constraints applicable under the legislation.

Wiltshire Police would like to thank you for the interest that you have shown in the Force.

Yours sincerely,

Force Disclosure Decision Maker

Wiltshire Police offers a re-examination of your case under its review procedure.

Freedom of Information Request Appeals Procedure

1. Who Can Ask for a Review

Any person who has requested information from Wiltshire Police, which has been dealt with under the Freedom of Information Act, is entitled to complain and request an internal review, if they are dissatisfied with the response they received.

2. How to Request a Review

Requests for review of a Freedom of Information request must be made in writing to the:
Force Disclosure Unit
Wiltshire Police Headquarters,
London Road, Devizes,
Wiltshire,
SN10 2DN

Email at disclosure@wiltshire.police.uk.

The reference number, date of the request and details of why the review is being requested must be included. Requests for review should be brought to the attention of the Force Disclosure Unit within 20 working days of the Force's response to the original FoI request.

3. Review Procedure

Receipt of a request for review will be acknowledged in writing to include confirmation of the reasons for the review. The review will be conducted by another Decision Maker, who is independent from the original Decision Maker. The Force Disclosure Unit will set a target date for a response. The response will be made as soon as is practicable with the intention to complete the review within twenty working days. In more complex cases the review may take up to 40 working days.

The Independent Decision Maker will conduct a review of the handling of the request for information and of decisions taken, including decisions taken about where the public interest lies in respect of exempt information where applicable. The review enables a re-evaluation of the case, taking into account the matters raised by the complaint.

4. Conclusion of the Appeal

On completion of the review the Independent Decision Maker will reply to the complainant with the result of the review. If the complainant is still dissatisfied following the review they should contact the Information Commissioner to make an appeal. The Information Commissioner can be contacted via the following details:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Tel: 01625 545 700
Fax: 01625 524 510
Email: mail@ico.gsi.gov.uk

Please note that the ICO's offices will be closed for the foreseeable future and are therefore unable to receive correspondence via post.

If you should wish to contact them, please visit https://ico.org.uk/global/contact-us/

DPIA 2 Form

Data Protection Impact Assessment Report

Project Information	
Project Name (and or number)	Microsoft O365 - Sharepoint
Business Area/s Affected	All
Information Asset Owner	All IAOs – each responsible for their own data
Senior Responsible Officer	REDACTED
Project Manager	REDACTED
Data Protection Officer	REDACTED

Document Ownership	
Author(s)	REDACTED
Document Owner	REDACTED

Document Review Information			
Document Location			
Quality Reviewers	**Name**	**Role**	**Sections Reviewed**
	REDACTED	NEP Business Analyst	Whole document
	REDACTED	NEP MS0O365 SME	Whole document
	REDACTED	RM	Whole document
	REDACTED	RM DM	Whole document
	REDACTED	ISO	Whole document
	REDACTED	DPO	Whole document
Version History	**Version Date**	**Requestor of Change**	**Summary of Change(s)**
0.1			Initial Draft
1.0	13/07/2021		Approved Draft
2.0	13/10/2021		Updated with REDACTED additions - Approved

Distribution List		
Name	**Department/Organisation**	**Project Role**

Introduction

The **Data Protection Impact Assessment (DPIA)** process is a legal requirement (as explained in Appendix B) and an important mechanism for identifying and managing data protection and other project (involving the processing of personal data) risks.

The DPIA process is applicable to initiatives involving the use of personal data and is particularly important when a new business process or technology is being used to process personal data; e.g. to record, share, collect, or retain personal data.

The DPIA enables privacy and data protection considerations to be made in the early stages of a project where any identified risks can be more readily resolved, rather than late or retrospective considerations where solutions can often prove to be more costly or delay implementation. A DPIA, should also recommend whether the project should be continued when balanced with the rights and interests of persons affected.

The DPIA process will consider privacy in the way Wiltshire Police use personal data. This can involve privacy about the individual, their personal information, their personal behaviour and their personal communications.

When carried out early the DPIA process will provide the following benefits:

- meet legal requirements
- avoid loss of trust and reputation
- identity management and privacy principles
- avoid disproportionate or unnecessary use of personal data
- avoid unnecessary costs
- avoid inadequate solutions
- support a communications strategy
- identify and manage risk

Who is responsible for carrying out a DPIA?

The responsibility for conducting a Data Protection Impact Assessment (DPIA) lies with the Project Senior Responsible Owner (SRO) and or Information Asset Owner (IAO) for a business change project and is produced as part of the project proposal. However, this activity can be delegated to an appropriate person such as the Project Manager. When a new project/initiative involving the processing of personal data is being considered, the SRO / IAO or Project Manager will contact the DPO to discuss the proposal and outline requirements. At this stage, it may be identified that it is necessary to undertake an information security assessment.

The DPIA will require authorisation by:

- Information Asset Owner
- Senior Responsible Owner
- Information Security Officer
- Records Manager
- Data Protection Officer

- Head of Information Management & Assurance (D/SIRO) – where the DPIA has identified 'high' residual risks and referral to the Information Commissioner is required (unless the H IM & A is a SRO when the SIRO (DCC) will provide the required authorisation).

Data Protection Impact Assessment Report –

1. Outline of the project, objectives and benefits

SharePoint Online is the strategic choice, backed up by the National Police Technology Council's National Enabling Programmes (NEP), as the platform to migrate appropriate electronic document records for Wiltshire Police and OPCC previously held in FirstPoint.

REDACTED additions 16/09/21

REDACTED is the O365 equivalent of SharePoint 2010's MySite – a personal area built on SharePoint architecture which allows users to save personal files synced from their laptop to the cloud within the Wiltshire Police tenancy.

This project will operate in parallel to Force obligations to sever links with the Wiltshire Council ICT support and bring back into Force.

The objectives of the project are:

- Ensure that all data migrated complies with MOPI, data protection legislation and stakeholder entity data retention policies.
- Migrate all approved files to a safe, secure and resilient SharePoint Online environment. All files that are held in FirstPoint are in scope for migration
- Ensure taxonomy, file plan and data retention are developed for Management of Police Information (MoPI) and UK General Data Protection Regulations (GDPR) classifications.
- Define and apply the non-technical aspects of SharePoint (including taxonomy, retention, security rules and instructions to users to be designed)
- Decommission unsupported systems - Firstpoint
- Design and deliver general user training (including establishment of Sharepoint Champions)

Ensure clear and regular communication to end users

REDACTED additions 16/09/21

- Inform users of the process for migrating personal files from their MySite to REDACTED.
- Ensure end users are aware of how to use REDACTED and fully understand their responsibilities set out in the Acceptable Use Procedure and not storing operational information in this area

Benefits of the Project:

- Improved compliance with MoPI/data protection legislation for documents migrated to SharePoint through better governance, permissions, access controls and document / site retention.

- For documents migrated to SharePoint and REDACTED, improved search to find documents and information quickly and easily
- Use of a strategic SharePoint platform and cloud-based storage means that documents and information migrated to SharePoint and REDACTED will be available ubiquitously on all approved and corporately owned end user devices
- Improved security and data management by reducing the email traffic and sending email attachments by sharing links
- Simplified and consistent privilege and access control
- Simplified business processes and improved productivity as SharePoint Online supports workflows with the other MS Productivity Tools such as Teams, Power Automate and Forms
- Proven Business Continuity / Disaster Recovery for documents stored on SharePoint and REDACTED
- Legacy environment de-commissioned

2. Describe the intended use of personal data:

a) Describe the nature of the processing:

Wiltshire Police / OPCC has a requirement for the Microsoft O365 collaborative tool Sharepoint to facilitate record/document storage and knowledge sharing in order to meet organisational obligations and ensure effective digital and mobile working.

Data collected will be added to SharePoint by individuals or teams once the bulk migration of existing legacy data from Firstpoint takes place. This is anticipated to take place by the end of March 2021.

The data will be stored in different SharePoint sites as defined by the Force / OPCC Command structure at SLT Hub level. Each site will be managed by a minimum of two site owners and site members. REDACTED.

The data will be used for corporate and operational decision making by the team(s) that have the appropriate access level and it is likely that some of the personal data will be shared with trusted partners.

The way the taxonomy will be designed means that only the people that have appropriate permissions for a particular site, or sites, will be able to read, edit or dispose of the data in that site. SharePoint Permissions and Access is currently managed by the SharePoint Owners. It will be possible to grant individuals permissions to access certain sites on an ad hoc basis as and when required.

As an aside, if an individual does not have access to a site and therefore the documents contained within it, data that they do not have permissions to view **will not** even appear on a generic search.

REDACTED additions 16/09/21

REDACTED files will be available to each individual user in an unshared format initially, this means access is locked down to the end user. Users will be able to share files from REDACTED

with other members of the force as required. However, the primary use of REDACTED will be for non-operational file storage.

Where information should be accessible to all, it will be made available via the associated Communications site.

Data will be shared amongst employees of WP / OPCC (based on the above principles regarding permissions).

Sharing of data with external parties will be permitted via an approval process which will be facilitated by ICT.

In the context of SharePoint, the Chief Constable or the PCC will be the Data Controller for each of their respective areas of business. All police officers, staff (temporary and permanent), contracted / other third parties and volunteers who have access to the data will be under auspices of one of the Data Controllers.

REDACTED.

MoPI, NPCC National and Local Retention and Disposal Schedule and generic Data Protection rules will guide data retention in SharePoint. The system has the capability for automated deletion and therefore there will be some automated rules put in place in due course. It is intended that for information that follows MoPI and NPCC / Local Retention Schedule rules, there will be a mechanism in place to add a label to ensure that when the relevant retention period is reached, records are reviewed and if no longer required, then deleted.

Need to Know principles will be derived from the specific permissions granted to SharePoint sites and libraries and the established approval process with regard to shared access with external parties. Security will also come from the above retention policies being applied

SharePoint is a replacement for Firstpoint and whilst it will be a new way of working for WP / OPCC it is not considered to be a new technology.

REDACTED additions 16/09/21
REDACTED is a replacement for MySites, which was a module within Firstpoint and also not considered to be a new technology.

While REDACTED access will not be shared by default, it is possible for a user's OneDrive to be accessed by an O365 administrator with SharePoint Administrator or Global Administrator permissions. This is to ensure that access to files is not locked solely to individuals who may leave the force with immediate effect. All access to users' REDACTED accounts is audited.

b) Describe the scope of the processing

The personal data will be classified as no higher than Official Sensitive (Government Security Classification Scheme) and would be personal and special category information (Data Protection Act 2018) as well as data processed for Law Enforcement / policing purpose.

Prior to the migration of data from the previous storage location (Firstpoint) to Sharepoint Online, a significant workstream was undertaken to identify data owners and ensure that a weeding / archive exercise took place. This ensured that no out of date, inaccurate or unlawfully held data would be migrated. This work was completed by the 31st of March 2021 and the old Firstpoint storage area was de-commissioned. Current data (including that within its retention period) has

been migrated and the remaining data archived in a new Sharepoint Online archive area where it will remain the responsibility of the Information Asset Owner and managed in line with the Force Records Retention Schedule.

There will be a number of different processing frequencies for each SharePoint site (depending on what that site is set up for), As an enterprise-wide system, it is envisaged that processing (any activity performed on the data) will take place every hour of every day.

REDACTED additions 16/09/21
This also applies to REDACTED (which constantly syncs between the user's laptop and REDACTED).

c) Describe the context of the processing:

New data will be added to SharePoint by site / content owners who have delegated authority from Information Asset Owners or Data Guardians. Each unit will have its own processes (outside of this system) to verify source and data quality.

The type of data subjects whose data will be stored in SharePoint will include, but is not limited to:

- Staff and Officers
- Victims
- Offenders / suspects
- Witnesses
- Members of the Public
- Volunteers

The type of data held will be everything from Corporate to Police Operational records. A reasonable person would expect the type of processing for each type of record held as stated in the Force / OPCC Privacy Notices.

Data stored within Sharepoint Online will relate to the types of data subjects as stated above. As such, it will undoubtedly contain records relating to children and vulnerable people. However, WP and OPCC has demonstrable experience of dealing with these types of records and have existing processes for the storage of such information.

This data will be reviewed and retained in line with MoPI / APP IM, NPCC National and Local Retention Schedules, Data Protection Act 2018 and UK GDPR as appropriate.

REDACTED additions 16/09/21
Data stored within REDACTED will primarily be personal data for employee reference, such as pay slips, holiday forms, etc. However, since files are synced from the user's laptop to REDACTED, any files saved on the laptop will also be saved within REDACTED. If these fall under the classification of operational documents, it will be the responsibility of the user to move them to the correct SharePoint team site as necessary.

Meeting recordings and 121 chat file attachments will automatically save directly into REDACTED and therefore need to be moved to the correct SharePoint team site as and when required.

d) Describe the purposes of the processing:

SharePoint and REDACTED will be used to process personal data in exactly the same way that FirstPoint and MySites were previously utilised. They are intended to provide the Force and OPCC with an improved repository for documents to be managed from creation to deletion, whilst maintaining compliance with current privacy legislation and National / Local policy and best practice.

3. Consultation:

a) The following consultation approach and stakeholder groups were incorporated into the consultation process:

REDACTED – SRO and Head of Information Management and Assurance
REDACTED – Data Protection Officer
REDACTED – Records Manager
REDACTED – Information Security Officer
REDACTED – MS O365 SP SME (NEP)
REDACTED – Digital Services Manager (Shared Hub)
REDACTED – Policy Officer
REDACTED – Records Management Decision Maker
REDACTED – Business Analyst (NEP)
REDACTED – Project Support Officer (NEP)
All Information Asset Owners for individual site data

b) A summary of the stakeholder views are as follows:

The named stakeholders are all part of the project board and have found that there are no current issues with the move from Firstpoint to SharePoint. They consider that SharePoint will be more compliant with legislation and that there will be improved support for the system.

Consultation with Data Subjects was not undertaken as the processing of data remains unchanged as Sharepoint provides a contemporary mechanism for document storage and will enhance rather than restrict data subject rights via improved search and retention management capabilities.

4. Data protection compliance – assessment of necessity and proportionality of personal data processing.

Principle 1: Use of personal data is fair, lawful, and transparent:

a) Lawful basis for the processing of personal data is stated as follows:

In the context of legacy data moving from FirstPoint and new data being added to SharePoint, the lawful bases for processing data:

UK GDPR Regime – personal data

- Article 6 (b) necessary for the performance of a contract
- Article 6 (c) necessary for compliance with a legal obligation
- Article 6 (e) necessary for the performance of a public task carried out in the public interest

UK GDPR Regime – special category data

- Article 9 (b) necessary for carrying out employment and social security obligations placed on an employer. Data Protection Act 2018, Schedule 1, Part 1 (1) – necessary for performing obligations or rights conferred by law on the data controller in connection with employment.
- Article 9 (g) necessary for reasons of substantial public interest, authorised by law. Data Protection Act 2018, Schedule 2, Part (6) – necessary for statutory and government purposes in the substantial public interest and where exercising a function conferred on a person by an enactment or rule of law.

UK GDPR Regime – criminal data

- Article 10 – the processing of criminal records and offences will be under the control of the police as an Official Authority.

Law Enforcement Regime (Data Protection Act 2018, Part 3) - personal data

- Section 31: processing for the purpose of prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties, including the safeguarding against and prevention of threats to national security.

Law Enforcement Regime (Data Protection Act 2018, Part 3) – special category data

- Schedule 8 (1) - necessary for reasons of substantial public interest and is necessary for the exercise of a function conferred on a person by enactment or rule of law.

b) Explain how individuals will be made aware of the processing:

The reasons for the organisations to process these types of data are as stated in the Force and OPCC privacy notices which are easily accessible from both the home page of the WP Force website and OPCC website.

For some specific data that will be stored on SharePoint, an exemption will be applicable from the transparency obligations.

Principle 2: Use of personal data is for a specified, explicit and legitimate purpose and not re-used for a purpose that is in-compatible with the original purpose:

The original reason that the legacy data in FirstPoint was collected will remain the same when it is migrated to SharePoint. Each area, site or library will be owned by an Information Asset Owner (IAO), Data Guardian or a Data Content Owner (with delegated authority) and each will rely on a different lawful basis for processing the data.

New data collected will still be collected for the same purpose and kept in the same taxonomy as the legacy data and so will inherit the same lawful basis for processing.

SharePoint and REDACTED are document storage systems and therefore when information is collected it will be done so lawfully and is not to be re-used for any other purpose that is incompatible with the original purpose, with only those individuals will the correct permissions having access to it.

Principle 3: Use of personal data is adequate, relevant and no more than necessary:

The data stored will be kept for corporate or operational requirements. The new taxonomy will have retention / disposal principles at its core. The system itself cannot ensure that 'no more than necessary' is collected, this will be up to each individual and site owner / administrator to manage. All officers and staff within WP and the OPCC are required to complete mandatory Data Protection (NCALT Managing Information) training taking them through the principles and explaining their responsibilities.

SharePoint file repository should be used to store all operational information and have retention labels in place; whereas REDACTED should be used to store personal and non-operational documents and these will be stored for the length of service plus 30 days.

Principle 4: Personal data must be accurate and kept up to date:

Each area that collects data will adhere to the Records Management Policy around data quality on record creation. SharePoint will enable those with the correct permissions to edit incorrect data or even delete data that is no longer necessary to retain.

The personal data that is processed for a law enforcement purpose that is stored on SharePoint, also needs to meet the additional requirements for categorisation of data subjects, so far as possible, as well as establishing fact from opinion. Although SharePoint has no mechanism of its own in enabling accurate recording of this, individuals will cover this in the documents they create. In many cases in will be inherently obvious from the document's context, whether the data is based on fact or opinion.

Principle 5: Personal data must be kept in an identifiable format for no longer than necessary:

SharePoint Online does have automated deletion capability, which will be configured to the needs of WP and OPCC. Sites will be set up to be retained for as long as they are required, but individual pieces of data and records collected will have individual retention set to them. It is intended that for some records, bespoke retention labels will be created which determines the record's retention period in accordance with the Force Records Retention Schedule. These labels will be added by the individual picking the correct classification from a series of easy to follow drop down boxes.

Relevant individuals will be notified when retention periods are reached and asked to review the content. If further retention is required there will be the capability to extend the retention period and if this does not take place, automated deletion will take place. It is intended that guidance

and support will be provided to individuals at the appropriate time setting out easily accessible criteria to aid them with the decision making, regarding deletion or further retention.

The system also has the functionality for ad-hoc deletion and delegated individuals with the correct permissions will be trained and then be able to delete documents.

REDACTED does not have automatic retention labels applied, due to the nature of the documents being stored in this area being of a personal nature, therefore it is the end users responsibility, in line with the acceptable use procedure to manage and weed these documents.

When new sites are created, the business area will be asked to stipulate how long the site is required for and when this time period has been reached, they will receive a notification. The relevant site owners will then be asked to review whether the site is still required or whether it can be deleted at that point and they will also be expected to confirm relevancy of permissions to the site.

Data that has been transferred from Firstpoint has been placed in SharePoint folders where retention periods have not yet been defined or applied. Therefore, interim arrangements will need to be established to ensure that this information is only retained in line with existing policies (e.g. manual methods). These records will be managed in SharePoint by the relevant owners and potentially retained unlawfully until work to set in place automated weeding takes place.

Principle 6: Personal data must be protected against unauthorised / unlawful use, accidental loss, damage or destruction:

Site owners and administrators will be responsible for ensuring that only the correct individuals have access to individual sites and the documents contained within it, they will also ensure that those individuals are set up with the correct permissions e.g. read only. The IAO will be required to review and authorise permissions ensuring that those users who no longer require that access are removed.

REDACTED.

SharePoint and REDACTED have an audit facility which stamps documents when they have been created or amended, deterring improper use.

Site owners / administrators will receive training on system use and capability and given details of best practice, which will then be cascaded down to the entire team.

Documents may be used for a law enforcement purpose or if not now, they may do sometime in the future and therefore in order to comply, the system meets the logging requirement in the following way:

- Create – stamped with time, date and user ID
- Amend - stamped with time, date and user ID
- View – stamped with time, date and user ID. In order to be able to view a document, an individual must have the correct permissions. Though searching and reason for search are not logged. However, an individual would not be able to search on anything that they do not have access to and if they view a document returned in their search results then this would be logged.

- Merge –it is not possible to merge documents without manually creating a new document

- Download - stamped with time, date and user ID. It is possible to prevent the individual downloading of documents on an ad hoc basis, if required.

- Disclose – although other 3rd party organisations will not be able to access our Sharepoint directly, links to documents can be shared with authenticated partners and they would receive read only access to the document on Sharepoint via the link. The individual sharing the link has the capability to set a timeframe in which the link can be utilised. A log of anyone that accesses that document using the link will then be created. Although the norm in the organisation currently is to share actual documents, through training and guidance there will be a shift in best practice to share links to documents rather than the documents themselves.
  Where individuals want to share documents with partners that are not authenticated, they should be logging the disclosure elsewhere e.g. PNB, though a process for authenticating partners is being looked at and therefore the non-compliance risk will be small.

- Delete – documents can only be deleted by authorised individuals or via the automated deletion process and once deleted by the business area it can only be retrieved by an authorised member of staff however after 93 days the document will disappear completely along with any audit information.

7. Personal data will be processed in accordance with the individual's data protection rights:

Freedom of Information requests, and requests from data subjects exercising their data rights (e.g. Subject Access requests) will be managed through the existing IM & A department under existing policy and processes.

For each category of data subject, it will be able to apply the appropriate rights to the data held and SharePoint will enable those rights (right of access, right to erasure etc) to be applied on a case by case basis. The system will make it easier to find the data through powerful search tools, which may make the process more efficient for locating relevant data to assist with an individual's data for 'Subject Access Requests'.

8. Personal data will not be transferred outside the European Economic Area (EEA) without guaranteed adequate privacy protections:

REDACTED and there will be no data processing outside of the EEA.

9. The force must be able to demonstrate how they are complying with the Data Protection Act 2018 & UK GDPR:

The record will be in this Data Protection Impact Assessment (DPIA) document and project documents. Within the scope of this project, SharePoint will not be enabled to allow the sharing

of documents with trusted partners. This will be functionality introduced by Office 365 project which has completed its own DPIA and ensure the appropriate agreements / MoUs are in place.

There is a contract already in place containing the relevant mandatory UK GDPR clauses for Microsoft to act as Data Processor for storing the force information REDACTED.

This DPIA provides an account of how the use of Sharepoint will comply with the Data Protection Act 2018 and UK GDPR.

5. Identifying and assessing risks.

The main focus of the risk assessment within the DPIA is to consider the risks to the interests of the individuals whose data will be processed. Risks may also be intangible (significant social or economic disadvantage) such as the risk of losing public trust. The identified risks are listed below and scored using a standardised risk assessment matrix.

The listed 'agreed actions' have been identified as a way to either **reduce or eliminate** risks identified as **medium or high**. Agreed measures will be factored into implementation plans and will be the responsibility of either the Project Manager or Information Asset Owner to ensure they are completed.

	Describe the source of the risk, the problem it creates and the potential impact on individuals. Focus on data protection compliance risks. Mention corporate risks only as necessary.	**Likelihood of harm** Remote, possible or probable.	**Severity of harm** Minimal, significant or severe.	**Risk score** Low, medium or high.	**Agreed action** Detail to action that will reduce the risk	**Action Owner & due date** Name & date	**Residual Risk score** Low, medium or high.
1	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED
2	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED
3	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED
4	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED
5	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED

***If you have accepted any of the above risks you must provide a rationale for doing so in the 'Agreed Actions' column.**

6. Authorisation of DPIA:

DPIA copies will be retained by the DPO, Information Asset Owner and within the relevant Project Management records.

a) Approval signatories

Item	Name / role / date / comments	Notes
Risk Reducing Measures approved by **Information Asset Owner:**		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by **Senior Responsible Officer**:	REDACTED 13 July 21 REDACTED, 14 Oct 21 (REDACTED)	Acceptance of mitigating actions.
Residual risks approved by **XXXXXX** (in consultation with IAO):	N/A	If accepting any residual high risk, consult the ICO before going ahead
Information Security Officer approval of DPIA	REDACTED, Information Security Officer, 24th June 2021	ISO should consider any risks concerning the information security provisions for the processing and whether processing can proceed
Records Manager approval of DPIA	REDACTED, Records Manager, 8th July 2021	RM should consider any risks concerning the record management provisions for the processing and whether processing can proceed
Data Protection Officer approval of DPIA:	REDACTED, Data Protection Officer, 8th July 2021 REDACTED, Data Protection Officer, 13th October 2021 (REDACTED)	DPO should consider any medium / high residual risks and whether processing can proceed
Summary of DPO advice: Having reviewed the content of this DPIA I am satisfied that this processing activity does not present any high (or medium) risks to the rights and freedoms of the data subjects affected by this processing activity. Significantly, the use of SharePoint does not fundamentally change the way in which personal data was previously processed by FirstPoint, however it does, via new technology (e.g. permission management, application of retention labels) have a number of features, which when fully enabled, are		

likely to support the Force and OPCC achieving and maintaining compliance with prevailing privacy legislation.

It should be noted that there are still some processes that are yet to be fully implemented or defined (e.g. creation and application of bespoke retention labels, processes / procedures in relation to guest access to SharePoint, etc) and therefore my recommendation is that this DPIA should be reviewed in 6 months' time.
Update 13th October 2021: REDACTED additions

I am satisfied that the use of REDACTED does not present any high / medium risks to the rights and freedoms of the data subjects affected by this processing activity. I note the new risk and the mitigating action that has been identified.

Still recommend that this DPIA is reviewed in 6 months' time (April 2022).

b) Residual high risks (complete <u>only</u> if there are any 'high' <u>residual</u> risks):

Item	**Name / role / date**	**Notes**
DPO advice accepted or overruled by **Senior Information Risk Owner (SIRO):**	N/A	If overruling the DPO's advice you should record your rationale below
SIRO Comments:		
Date and name of person referring DPIA to ICO:		As required by law if any high residual risks remain.
Summary of ICO advice:		

c) Accountability – update of 'records of processing':

Information Management Name / role	**Information Asset Register**	**Special Category Data Policy Document**	**Notes**
N/A			Add dates the records were updated.

d) Review of DPIA:

Item	Information Management Name / role / date	Frequency	Notes
DPIA will be kept under review by:	REDACTED (NEP Business Analyst) and REDACTED (DPO)	Initial 6 months (April 2022) and annually thereafter	How often dependant on the nature of processing & residual risk level

DPIA 2 Form

Data Protection Impact Assessment Report

Project Information	
Project Name (and or number)	Microsoft Teams
Business Area/s Affected	Force-wide
Information Asset Owner	All IAOs across the force
Senior Responsible Officer	REDACTED
Project Manager	REDACTED
Data Protection Officer	REDACTED

Document Ownership	
Author(s)	REDACTED
Document Owner	REDACTED

Document Review Information			
Document Location			
Quality Reviewers	**Name**	**Role**	**Sections Reviewed**
	REDACTED	Data Protection Officer	
	REDACTED	Records Manager	
	REDACTED	Records Management Decision Maker	
	REDACTED	Review Officer	
Version History	REDACTED	Information Security Officer	**Summary of Change(s)**
0.1			Initial Draft
1.0			

Distribution List		
Name	**Department/Organisation**	**Project Role**

Introduction

The **Data Protection Impact Assessment (DPIA)** process is a legal requirement (as explained in Appendix B) and an important mechanism for identifying and managing data protection and other project (involving the processing of personal data) risks.

The DPIA process is applicable to initiatives involving the use of personal data and is particularly important when a new business process or technology is being used to process personal data; e.g. to record, share, collect, or retain personal data.

The DPIA enables privacy and data protection considerations to be made in the early stages of a project where any identified risks can be more readily resolved, rather than late or retrospective considerations where solutions can often prove to be more costly or delay implementation. A DPIA, should also recommend whether the project should be continued when balanced with the rights and interests of persons affected.

The DPIA process will consider privacy in the way Wiltshire Police use personal data. This can involve privacy about: the individual, their personal information, their personal behaviour and their personal communications.

When carried out early the DPIA process will provide the following benefits:

- meet legal requirements
- avoid loss of trust and reputation
- identity management and privacy principles
- avoid disproportionate or unnecessary use of personal data
- avoid unnecessary costs
- avoid inadequate solutions
- support a communications strategy
- identify and manage risk

Who is responsible for carrying out a DPIA?

The responsibility for conducting a Data Protection Impact Assessment (DPIA) lies with the Project Senior Responsible Owner (SRO) and or Information Asset Owner (IAO) for a business change project and is produced as part of the project proposal. However, this activity can be delegated to an appropriate person such as the Project Manager. When a new project/initiative involving the processing of personal data is being considered the SRO / IAO or Project Manager will contact the DPO to arrange a meeting with relevant parties to discuss the proposal. At this stage it may be identified that it is necessary to undertake an information security assessment.

The DPIA will require authorisation by:

- Information Asset Owner
- Senior Responsible Owner
- Information Security Officer and / or Records Manager
- Data Protection Officer

- Head of Information Management & Assurance (D/SIRO) – where the DPIA has identified 'high' residual risks and referral to the Information Commissioner is required (unless the H IM & A is a SRO when the SIRO (DCC) will provide the required authorisation).

Data Protection Impact Assessment Report

1. Outline of the project, objectives and benefits
Microsoft Teams is a communication tool that combines workplace chat, calls, video, meetings and file storage (including collaboration on files). It encourages chat in place of email which reduces the number of emails across the organisation. It will allow individuals to chat and share documents through Microsoft Teams using the associated SharePoint Teams site, one to one chat, group chat or channel posts (replacing Skype). Objectives:- 1. The O365 Information Governance project has been established to upskill the force in the use of Microsoft Teams (and other O365 applications) by developing policy/procedure and providing regular and up-to-date training materials, information and support when needed 2. Records management is key to identifying, classifying, storing, securing, retrieving, auditing and the lawful and timely destruction of records we hold within force. The project needs to communicate this to end users and ensure the appropriate information and records management governance is in place to keep our data secure and ensure that staff are aware of their collective responsibilities in terms of the acceptable use of Microsoft Teams and the ongoing management of their data in line with Force policy and procedure. 3. Initially all new processes that require a Microsoft Team as part of a use case will be supported by the NEP Project Team, so that end users understand their responsibilities in line with current data protection legislation (DPA 2018 and UK GDPR) and the Authorised Professional Practice (APP) on the Management of Police Information (MoPI). 4. Moving forward into BAU, an approval process to request a new Microsoft Team now sits within ICT where the necessary considerations will be taken into account before a new Microsoft Team is created. This will necessitate the upskilling of the ICT Team in the use of Microsoft Teams and when a new Team would be appropriate, checking for duplicates, monitoring and managing the demand and understanding the IM&A risks, raising them with IM&A and the requestor where necessary. 5. Upskilling the ICT Team in the understanding the process, technical requirements and governance for setting up guest access and putting in place the necessary approvals, policies and procedures to support any new requests. 6. When Wiltshire Police migrated to Sharepoint Online, in most cases business areas will have an associated Microsoft Teams site enabled from their SharePoint Team Site. · 7. Microsoft Teams is a key productivity tool in many of the candidate use cases we are trialling across the force, including the use of guest access and providing external partners secure access when sharing information. The project team need to understand

the tool and put in place the necessary activities to ensure the use cases are set-up in the correct way, with a minimum of 2 owners etc.

The benefits of Microsoft Teams are the following.

1. Productivity gains and enriched, targeted communication
2. Better focus on your work
3. Increased transparency
4. Seamless move to a digital workplace, which considering covid has been invaluable to us as a force
5. New team members can more quickly get up to speed
6. Reducing email traffic
7. Greater structure around file management
8. Everything in one place, saving the end user time coming in and out of different applications
9. Interacts with many of the Microsoft Productivity Tools
10. Microsoft Teams is that it can be accessed anywhere, anytime, on any device
11. Increased security and control of the data we share with external partners, with multi-factor authentication and linked to the identity & access management solution
12. Real-time collaboration on document

2. Describe the intended use of personal data:

Wiltshire Police/OPCC has a requirement for the Force to use the Microsoft Teams collaborative tool with the associated SharePoint Teams Sites to facilitate record/document storage, collaborate effectively and knowledge sharing to meet organisational obligations and maximising the use of the Microsoft Productivity Tools to ensure effective digital and mobile working.

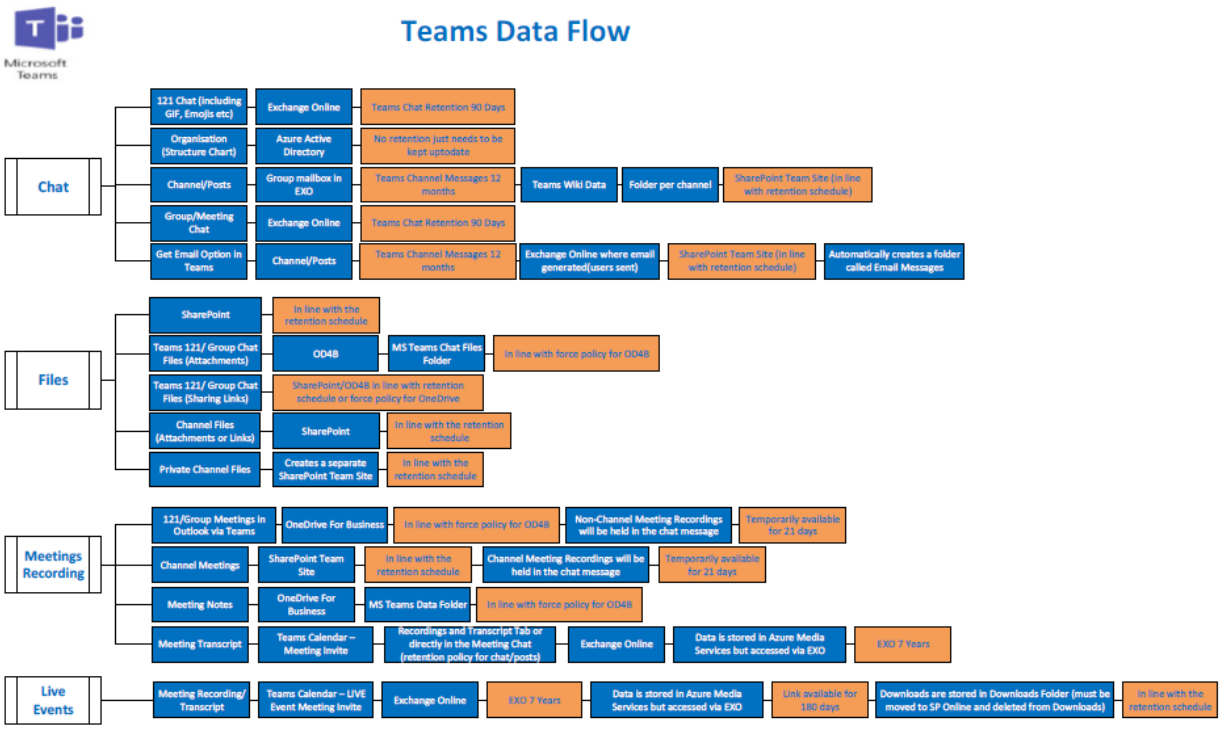
Creation

Microsoft Teams request process/approval process

We have implemented a request and approval process for the creation of any new Microsoft Teams, with an associated SharePoint Team Site. There is a form that end users submit within the self-service area of the homepage, and it is also accessible in the Halo ICT Ticket System. Currently the Service Delivery Operations Managers have agreed to approve all new requests as they can ask the necessary questions to determine if it can be approved or rejected, each request is automatically recorded in a SharePoint approved or rejected list, thus ensuring there is a register of all sites. This mutually agreed approval process ensures that no duplicate sites are created, and alternatives are explored, if appropriate. Permissions are managed by the person requesting the Microsoft Team, they must ensure there is a minimum of 2 owners and that they remove the Service Account as an owner, this is covered in a training video within the body of the email notification once their Microsoft Team has been approved.

The specific functionality that will be available within a Microsoft Team is the ability to create a 121/Group Chat, work, share and collaborate on files, arrange and record meetings, hold live events REDACTED please see the Microsoft Teams Data Flow below for more detail.

Microsoft Teams Data Flow.



a) Describe the nature of the processing:

Are there other versions of the tool?

There is a desktop application which has been installed on all laptops, the web application is available by selecting https://teams.microsoft.com/ or going to the Wiltshire Police homepage, clicking on the App Launcher and selecting Teams and Microsoft Teams is available on all mobile devices; you will be asked to verify your credentials when using each version for the first time.

Upload/export & duplication of files

You can upload files, documents, images and videos into Microsoft Teams from REDACTED, your computer i.e. your desktop and SharePoint Online.

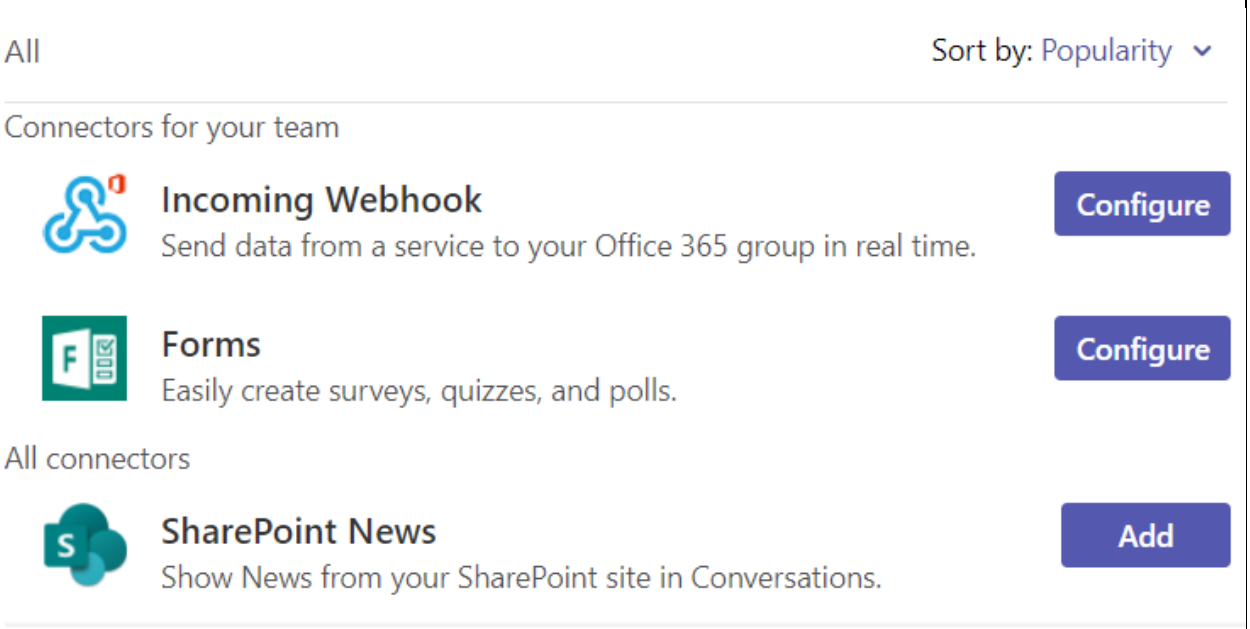
If you attach a document/image etc within Microsoft Teams channel posts, one to one or group chat, it will save a duplicate copy within the files section of the area it has been uploaded to. This means that if that document is deleted from the place it is uploaded from, i.e. Documents, it will still need to be deleted from the one to one/group message (if deleted directly from the MS Teams Chat Files it will no longer be accessible via the chat attachment). If it was attached to the channel posts, it will appear in the files section within the channel and will need to be deleted from there.

However, to avoid multiple versions of the same file being created, there is a copy link function available so that you can send a link to the document you are collaborating on, ensuring users are working from a single source of truth; this is the recommended approach documented in the Acceptable Use Procedure, the details can be read in full, using this link Microsoft Office 365 Acceptable Use Procedure. You can manage access and give direct access to a file using the "manage access" option when clicking on the 'Open in SharePoint' option within Microsoft Teams, which enables you to share the link or give direct access to the document, this has additional options available which means you can give users edit access or view only.

3rd Party applications

Microsoft Teams has 3 ways of integrating 3rd Party Applications, they are connectors, bots and tabs.

We are currently not using Bots or Connectors, both would need development, 3rd Party Connectors are disabled, the only connectors available in Microsoft Teams are the following (none of these have been tested yet within Teams);



Tabs maintain persistent information and provide a dedicated window to a third-party app within the canvas of a Teams channel, however there are no 3rd Party Applications available via Microsoft Teams at present. Users can easily view a tab while still chatting with the members of their channel. This allows for smoother collaboration and multi-tasking.

Tabs have been used when adding other Microsoft applications such as, TasksByPlanner & Whiteboard.

Auto generation

When you create a Microsoft Team, it creates an associated SharePoint Team Site, it will automatically create a 'General' folder which is where we recommend you create your folder

structure and save your files, this is the associated SharePoint Team Site, for DPIA considerations please review the SharePoint and REDACTED DPIA using this link SharePoint and REDACTED DPIA.

If you create additional channels within a Microsoft Team, it will automatically create a folder for each channel, the folder will automatically be named the same as the channel name. If you delete the channel because it is no longer needed, the folder will remain within the SharePoint Team Site for the overarching Microsoft Team, you will need to remove the folder and associated documents saved from SharePoint as well. If you delete the Microsoft Team, will it automatically delete the associated SharePoint Team Site, user guidance is documented in the Acceptable Use Procedure in relation to this and the Team Owners responsibilities in relation to data held here, please refer to Microsoft Office 365 Acceptable Use Procedure and SharePoint and REDACTED DPIA.

When you create a Teams 121 Chat/Group chat and attach a file it automatically saves it in a folder in your REDACTED called MS Teams Chat Files.

Co-authoring/ownership
Microsoft Teams does allow you to co-author on all documents and other Microsoft applications it is one of the main benefits of the tool. The ownership is dependent on the productivity tool being used, please refer to each tool specific DPIA for more information.

Privacy
REDACTED

Sharing
The data will be used for corporate and operational decision making by the team(s) that have the appropriate access level and it is feasible that the personal data will be shared internally and with trusted partners. Sharing of data with external parties via Microsoft Teams, namely B2B Guest Access; will be permitted via an approval process which will be facilitated by IM&A and ICT. This process is currently being defined and tested through the Candidate Use Cases and NEP Project Team, using the MAPPA referral process.

To-date we have created an IAO/Requestor question-set, which should be accessible via Halo with the addition of a Microsoft 365 Guest User Access Pre Approval Security Questionnaire (based on NCSC 14 Cloud Security Principles) created by the Information Security Officer.

Sharing with guest users can be via Microsoft Teams by adding the guest user as a member to the Microsoft Team, that member can then access the chat, channel posts and files within Microsoft Teams.

Federation is another form of sharing and collaboration; Federation provides your organisation with the ability to communicate with other organisations to share IM and presence. In Teams federation is on by default. However, tenant admins have the ability to control federation through the Microsoft 365 admin centre.

Access

An end user will request a new Microsoft Team via the request process, which is approved by ICT, when the request is approved the automated creation of a Microsoft Team will add the requestor as one of the owners and the ICT Service Account will be the second owner (this will show as REDACTED), there is a training video asking the requestor to remove the Service Account and add in a second owner and the specific members. It is the responsibility of the Information Asset Owner and the 2 Owners to maintain the access to this site and also when they leave or move to another role, to ensure the MS Team is handed over to a new owner.

Guest Users will have access in some cases and again this is the responsibility of the Information Asset Owner to manage and maintain.

Teams Meetings
People who are invited to the meeting or forwarded the meeting invitation after it is scheduled have access to the chat before, during, and after the meeting (up to the 1000-person limit). People who are added to a meeting after it starts using the Invite someone field on the Participants pane (or are provided the meeting join coordinates in another way) will have access to the chat from the time they join to the time the meeting ends. They will not be able to see chat that takes place after the meeting ends.

Meeting invites can be shared by someone other than the organiser, unless you untick the option when organising the meeting that allows forwarding. There is more information documented in the Acceptable Use Procedure in relation to meeting recordings and sharing meeting invites, here is a link MS Teams Meeting Recordings Acceptable Use Procedure.

Meeting organisers should check there are no unauthorised participants before a meeting begins. If someone is being invited to a single meeting in a series of reoccurring meetings, the organiser should make sure they are only sent the invite for the single occurrence. Participants will be able to see any chats from the single meeting they are in, but not any previous/subsequent meetings.

If a user is asked to join part of a meeting they will be able to see and contribute to the chat posts for the remainder of the meeting, even after they have left and the meeting is still continuing. The content of any subsequent posts may not be appropriate for all users, therefore it would be advisable to remove that attendee from the chat after they have left.

Local settings / deviation
Teams has been set-up in line with the NEP Blueprint and LLDs, there have been no deviations.

Retention/ Deletion
Please see the data flow for full details of each function of MS Teams and the associated retention.

121/Group Chat – there is a change request in with ICT to set a retention for 90 Days. Channel Posts – there is a change request in with ICT to set a retention for 12 months.

Audit

Full details of what's available in terms of the security and compliance centre is available here Overview of security and compliance - Microsoft Teams | Microsoft Docs

Disclosure
The content of Microsoft Teams may be disclosable, for example under FOI Legislation or in accordance with a Right of Access request, subject to applicable exemptions.

b) Describe the scope of the processing

The personal data processed by Microsoft Teams will be classified as no higher than Official and Official Sensitive (Government Security Classification Policy) and will include personal and special category information (UK GDPR / Part 2 DPA, 2018) as well as data processed for a Law Enforcement/policing purpose (Part 3, DPA 2018). Please refer to the Acceptable Use Procedure in terms of uploading evidential material in Microsoft Teams, this is outlined as not appropriate within this tool.

There will be a myriad of processing frequencies for each Microsoft Team and the associated SharePoint site (depending on what that site is set up for). As an enterprise-wide system, it is envisaged that processing (any activity performed on the data) will take place every hour of every day.

When the user requests a Microsoft Team they are asked what the Microsoft Team is going to be used for and how long the Microsoft Team will be needed for, i.e. a project MS Team may be needed for 12 – 18 months.

c) Describe the context of the processing:
New data will be added to the Microsoft Team by the site owners and members who have delegated authority from Information Asset Owners or Data Guardians. Each unit will have their own processes (outside of this system) to verify source and data quality.

The type of data subjects whose data will be stored in Microsoft Teams are, but is not limited to:

- Staff and Officers
- Victims
- Offenders / suspects
- Witnesses
- Members of the Public
- Volunteers
- Contractors
- Partner agency personnel

The type of data held will be everything from Corporate to Police Operational records (up to Official Sensitive). A reasonable person would expect the type of processing for each type of record held as stated in the Force / OPCC Privacy Notices.

Data stored will relate to the types of data subjects as stated above, as such it will undoubtedly contain records relating to children and vulnerable people, however WP and OPCC has a vast amount of experience of dealing with these types of records and have existing processes for the storage of such information.

This data will be reviewed and retained in line with APP IM/MoPI, NPCC National and Local Retention Schedules, Data Protection Act 2018, UK GDPR which will include chat, calls, online meetings, recordings and transcripts.

d) Describe the purposes of the processing:
Microsoft Teams will be used to process personal data in exactly the same way that Wiltshire Police and the OPCC was previously doing so in tools such as Exchange Online, Skype, Word, Excel, PowerPoint, Mitel Phone System.

The expectation is that the functionality in Microsoft Teams will reduce the number of emails sent out where data and information is shared internally and externally. Microsoft Teams is a more secure way of sharing and collaborating on documents in that it is managed by Site Owners by providing permissions to the information users who need to see it for policing purposes. It is possible to lock down documents in respect of editing, viewing and downloading and any guest access requests for external partners will be authenticated through our Identity and Access Management Solution.

3. Consultation:

The following consultation approach and stakeholder groups were incorporated into the consultation process:

REDACTED – SRO and Head of Information Management and Assurance
REDACTED – Data Protection Officer
REDACTED – Records Manager
REDACTED – Information Security Officer
REDACTED – ICT Security Officer
REDACTED – MS O365 SP SME (NEP)
REDACTED – Digital Services Manager (Shared Hub)
REDACTED – Policy Officer
REDACTED – Records Management Decision Maker
REDACTED – Records Management Decision Maker
ICT Colleagues invited to our weekly project meetings and the NEP Governance Board
REDACTED – Business Analyst (NEP)
REDACTED – Project Support Officer (NEP)
All Information Asset Owners for individual site data and Use Case Owners when setting up any new Teams.

The above stakeholder views were taken into consideration and measures to support them have been included in the planned data processing activities.

The following stakeholders views whilst being considered were not reflected in the planned processing activities:

The above-named stakeholders are all part of the MS 365 & Information Governance Project Board or attendees at the NEP Governance Board and have found that there are no current issues with enabling Microsoft Teams. They feel that the suite of MS Productivity Tools will be more compliant with legislation and that there will be improved support for the system.

For each productivity tool it will be considered whether there is a requirement to produce a DPIA, Information Sharing Agreement, to update the Acceptable Use Procedure or put in place the relevant privacy notices where required.

4. Data protection compliance – assessment of necessity and proportionality of personal data processing.

Principle 1: Use of personal data is fair, lawful, and transparent:

The lawful basis for processing data in Microsoft Teams and / associated SharePoint sites will differ dependant on the purpose that each Team is established for, however they are likely to be one of the following:

UK GDPR Regime – personal data

- Article 6 (b) necessary for the performance of a contract
- Article 6 (c) necessary for compliance with a legal obligation
- Article 6 (e) necessary for the performance of a public task carried out in the public interest

UK GDPR Regime – special category data

- Article 9 (b) necessary for carrying out employment and social security obligations placed on an employer. Data Protection Act 2018, Schedule 1, Part 1 (1) – necessary for performing obligations or rights conferred by law on the data controller in connection with employment.
- Article 9 (g) necessary for reasons of substantial public interest, authorised by law. Data Protection Act 2018, Schedule 2, Part (6) – necessary for statutory and government purposes in the substantial public interest and where exercising a function conferred on a person by an enactment or rule of law.

UK GDPR Regime – criminal data

- Article 10 – the processing of criminal records and offences will be under the control of the police as an Official Authority.

Law Enforcement Regime (Data Protection Act 2018, Part 3) - personal data

- Section 31: processing for the purpose of prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties, including the safeguarding against and prevention of threats to national security.

Law Enforcement Regime (Data Protection Act 2018, Part 3) – special category data

- Schedule 8 (1) - necessary for reasons of substantial public interest and is necessary for the exercise of a function conferred on a person by enactment or rule of law.

b. Explain how individuals will be made aware of the processing:

The reasons for the organisations to process these types of data are as stated in the Force and OPCC privacy notices which are easily accessible from both the home page of the WP Force website and OPCC website.

For some specific data that will be stored on SharePoint, an exemption will be applicable from the transparency obligations

Principle 2: Use of personal data is for a specified, explicit and legitimate purpose and not re-used for a purpose that is in-compatible with the original purpose:

Microsoft Teams has an associated SharePoint site for storing documents, each area, site or library will be owned by an Information Asset Owner (IAO), Data Guardian or a Data Content Owner (with delegated authority) and each will rely on a different lawful basis for processing the data, this is covered in the SharePoint DPIA.

New data collected will still be collected for the policing purposes in relation to each specific business areas needs.

Microsoft Teams will be used for data collection, when information is collected it will be done so lawfully and is not to be re-used for any other purpose that is incompatible with the original purpose, with only those individuals will the correct permissions having access to it.

Microsoft Teams has the chat function, posts section in a channel and you can make calls from Teams. Its main purpose is to collaborate and communicate with one another and is seen as an alternative/replacement for emails and Skype but with additional functionality making collaboration and communication more effective for the end user and is seen as a more secure platform because it is permission based.

The chat functionality and sharing of information and documents will be used in the same way that Exchange Online and Skype was used. The way in which this data is used, or its intended use is outlined in the MS O365 Acceptable Use Procedure.

Principle 3: Use of personal data is adequate, relevant and no more than necessary:

The data stored will be kept for corporate or operational requirements. The new processes in place will have retention / disposal principles at its core. The system itself cannot ensure that 'no more than necessary' is collected, this will be up to each individual and site owner / administrator to manage. All officers and staff within WP and the OPCC are required to complete mandatory Data Protection (NCALT Managing Information) training taking them through the principles and explaining their responsibilities.

Principle 4: Personal data must be accurate and kept up to date:

Each area that collects data will adhere to the APP IM and local Force Records Management Policy around data quality on record creation. Microsoft Teams will enable those with the correct permissions and membership to the MS Team to edit incorrect data or even delete data that is no longer necessary to retain.

The personal data that is processed for a law enforcement purpose that is stored in MS Teams needs to meet the additional requirements for categorisation of data subjects, as far as possible, as well as establishing fact from opinion. Although Teams has no mechanism of its own in enabling accurate recording of this, individuals will cover this in the documents they create, posts they comment on and meeting recordings they take part in. In many cases it will be inherently obvious from the specific tool's context, whether the data is based on fact or opinion.

Principle 5: Personal data must be kept in an identifiable format for no longer than necessary:
Microsoft Teams will be retained for as long as they are in use. Microsoft Teams and its associated SharePoint site content will be retained and managed in line with the Force Records Retention Schedule. If a Microsoft Team is deleted, it will automatically delete the associated SharePoint Team Site.

Inactive O365 Groups/Sharepoint/Teams: In addition to automated and manual weeding, notifications of inactive groups (which includes Microsoft Teams activity) have been implemented.

This process will ensure that O365 Groups (Exchange Online, MS Teams and SharePoint sites) that have been inactive for 180 days, are not deleted without review by the Owners or, if no Owner can be located, the Records Management Team in conjunction with the Information Asset Owner and any data that needs to be retained is moved to an appropriate site within SharePoint Online

The system also has the functionality for ad-hoc deletion and delegated individuals with the correct permissions will be trained and then be able to delete documents.

Principle 6: Personal data must be protected against unauthorised / unlawful use, accidental loss, damage or destruction:

Microsoft Teams owners (minimum of 2) will be responsible for ensuring that only the correct individuals have access to individual sites and the documents contained within it, they will also ensure that those individuals are set up with the correct permissions. The IAO will be required to review and authorise permissions ensuring that those users who no longer require that access are removed.

REDACTED.

The files are visible in the Microsoft Team; however it is a window into the associated SharePoint Site and SharePoint has an audit facility which stamps documents when they have been created or amended, deterring improper use.

Site owners will receive training on system use and capability and given details of best practice, which will then be cascaded down to the entire team.

Documents may be used for a law enforcement purpose or if not now, they may do sometime in the future and therefore in order to comply, the system meets the logging requirement in the following way:

- Create a post to share a document – stamped with time, date and user ID
- Amend a post - stamped with time, date and user ID
- Disclose – links to documents can be shared via a Microsoft Team with authenticated partners and they would receive read only access to the document on Sharepoint via the link. The individual sharing the link has the capability to set a timeframe in which the link can be utilised. A log of anyone that accesses that document using the link will then be created. Although historically within the organisation we would share actual documents, through training and guidance there will be a shift in best practice to share links to documents rather than the documents themselves.
- Delete – channel posts and chat can only be deleted by authorised individuals that are a member or owner of the Microsoft Team, or deleted via the automated deletion process and once deleted by the business area it can only be retrieved by an authorised member of staff however after 93 days the document will disappear completely along with any audit information.

7. Personal data will be processed in accordance with the individual's data protection rights:

Freedom of Information requests, and requests from data subjects exercising their data rights (e.g., Subject Access requests) will be managed through the existing IM & A department in accordance with the current policy and processes.

8. Personal data will not be transferred outside the European Economic Area (EEA) without guaranteed adequate privacy protections:

REDACTED and there will be no data processing outside of the EEA.

9. The force must be able to demonstrate how they are complying with the Data Protection Act 2018 & GDPR:

There is a contract already in place containing the relevant mandatory UK GDPR clauses for Microsoft to act as Data Processor for storing the force information REDACTED.

This DPIA provides an account of how the use of Microsoft Teams will comply with the Data Protection Act 2018 and UK GDPR.

5. Identifying and assessing risks

The main focus of the risk assessment within the DPIA is to consider the risks to the interests of the individuals whose data will be processed. Risks may also be intangible (significant social or economic disadvantage) such as the risk of losing public trust. The identified risks are listed below and scored using a standardised risk assessment matrix.

The listed 'agreed actions' have been identified as a way to either **reduce or eliminate** risks identified as **medium or high**. Agreed measures will be factored into implementation plans and will be the responsibility of either the Project Manager or Information Asset Owner to ensure they are completed.

	Describe the source of the risk, the problem it creates and the potential impact on individuals. Focus on data protection compliance risks. Mention corporate risks only as necessary.	**Likelihood of harm** Remote, possible or probable.	**Severity of harm** Minimal, significant or severe.	**Risk score** Low, medium or high.	**Agreed action** Detail to action that will reduce the risk	**Action Owner & due date** Name & date	**Residual Risk score** Low, medium or high.
1	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED
2	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED
3	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED
	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED	REDACTED

***If you have accepted any of the above risks you must provide a rationale for doing so in the 'Agreed Actions' column.**

6. Authorisation of DPIA:

DPIA copies will be retained by the DPO, Information Asset Owner and within the relevant Project Management records.

a) Approval signatories

Item	Name / role / date / comments	Notes
Risk Reducing Measures approved by **Information Asset Owner:**	REDACTED, H IM & A / DSIRO / NEP SRO, 4th April 2022	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by **Senior Responsible Officer**:		Acceptance of mitigating actions.
Residual risks approved by **XXXXXX** (in consultation with IAO):		If accepting any residual high risk, consult the ICO before going ahead
Information Security Officer approval of DPIA	REDACTED, ISO, 09/03/2022	ISO should consider any risks concerning the information security provisions for the processing and whether processing can proceed
Records Manager approval of DPIA	Approved REDACTED Records Manager 17/03/22	RM should consider any risks concerning the record management provisions for the processing and whether processing can proceed
Data Protection Officer approval of DPIA:	REDACTED, DPO, 21st March 2022	DPO should consider any medium / high residual risks and whether processing can proceed

Summary of DPO advice:

I note the outstanding action regarding the retention periods to be applied to 121 and Team Channel posts, and I understand that this is in the process of being implemented, therefore am content to approve this DPIA on that basis. The retention being set to indefinite currently is disproportionate and does present a risk regarding what data could be in scope for disclosure; e.g. in accordance with a DSAR.

Having reviewed the DPIA in full I am content that the use of Microsoft Teams by Wiltshire Police does not present any significant or high risks or negatively impact on the rights and freedoms of the data subjects affected by this processing activity.

b) Residual high risks (complete only if there are any 'high' residual risks):

Item	Name / role / date	Notes
DPO advice accepted or overruled by **Senior Information Risk Owner (SIRO):**		If overruling the DPO's advice you should record your rationale below
SIRO Comments:		
Date and name of person referring DPIA to ICO:		As required by law if any high residual risks remain.
Summary of ICO advice:		

c) Accountability – update of 'records of processing':

Information Management Name / role	Information Asset Register	Special Category Data Policy Document	Notes
			Add dates the records were updated.

d) Review of DPIA:

Item	Information Management Name / role / date	Frequency	Notes
DPIA will be kept under review by:			How often dependant on the nature of processing & residual risk level

DPIA Screening (Stage 1)

Criteria to determine when a Data Protection Impact Assessment is needed.

What is a DPIA?

Data protection legislation requires organisations to conduct a Data Protection Impact Assessment (DPIA) when they plan to use data in a way that is likely to result in a risk to the rights and freedoms of individuals.

The purpose of a DPIA is to assess a proposal to ensure that, before processing starts:

- the processing is necessary and proportionate
- data protection and privacy risks are identified and mitigated
- any risks to an individual's rights and freedoms are identified and mitigated
- decisions about the use of personal data are recorded.

The WP DPIA Process?

The DPIA process is made up of two stages:

- **Stage 1: DPIA Screening** - screening assesses whether a project or proposal is likely to result in a risk to individuals and whether a DPIA will therefore be required. DPIA screening must be completed at the earliest possible stage in the Project lifecycle so that a DPIA can be conducted where necessary, ensuring that recommendations and solutions are incorporated into the proposed design.
  Stage 2: Data Protection Impact Assessment - a mandatory legal requirement where risks to individuals are likely to be high. A DPIA requires a full assessment of the risks to individuals. This is an iterative and inherent process throughout (planning, development and operation phases)

The DPIA process applies to all WP activity where personal data is used and encompasses activities such as the introduction of new or changes to existing Applications, Systems, Processes, Tools / Functions, Techniques, Services or Contracts.

Data protection and privacy must be at the forefront of the design of any new systems or proposals.

Responsibility for completing a DPIA Screening?

The Senior Responsible Owner for the proposal is responsible for ensuring the screening takes place and appointing an individual who must ensure that

the DPIA process is followed and that the DPIA Screening is completed appropriately. The WP Data Protection Officer (DPO) will assess the completed submission (form) and will advise whether or not a full DPIA is required.

Completing the DPIA Screening?

Provide comprehensive detail about the nature, scope, context and purpose. Avoid using technical jargon and acronyms, explain the proposal in a way that someone with no prior knowledge of it could easily understand. Completed forms must be submitted to the DPO inbox (dataprotectionofficer@wiltshire.police.uk). Failure to provide sufficient information will delay the assessment and response.

The DPO is responsible for reviewing DPIA Screenings to ensure that the process has been correctly followed and the risks identified. The DPO will provide:

- an initial assessment;
- advice where the project need to do further work to adequately complete the document and deliver data protection by design and default;
- a final assessment to any revised initial screening as to whether a DPIA will be required.

Factors likely to indicate that a DPIA is required?

A DPIA will be required when the processing is likely to result in a medium / high risk to the rights and freedoms of individuals. When considering what is meant by an individual's rights and freedoms, whilst the primary concern relates to the right to privacy, it may also involve other fundamental rights such as freedom of speech, freedom of thought or prohibition of discrimination.

Risks to the rights and freedoms of individuals may result from processing which could lead to physical, material or non-material damage, for example:

- where the processing may give rise to discrimination, identity theft or fraud, financial loss or reputational damage;
- where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their data;
- where special categories of data are processed;
- where personal aspects are evaluated, in particular analysing data concerning performance at work, health, personal preferences or interests, reliability or behaviour, location or movements, in order to profile individuals;
- where personal data of vulnerable natural persons, in particular of children, are processed; or
- where processing involves a large amount of personal data and affects a large number of data subjects.

The Information Commissioner's Office has published a number of factors that present a 'high risk' when processing personal data and these factors are outlined in Sections 2 and 3. Saying yes to one or more of these factors is likely to mean that a DPIA is required.

If there is any doubt as to whether a DPIA Screening or DPIA are required, then one should be carried out.

List of questions / points to be addressed in the MS O365 Productivity tool DPIA screening document:

- High level overview of MS productivity tool.
- Technical consideration/recommendations to include:
    - **Creation** - who can create, is there any requirement for an approvals process to grant licenses or permissions?
    - **Are there other versions of the tool?** i.e desktop/web app. Can end users access all?
    - **Upload/export** - Can other files types/ documents/ images/ video/audio be uploaded into the tool, if so, where from? Is it possible to export copies? For example; Whiteboards.
    - **3rd Party applications** - Does the tool have the capability to interact with any 3rd party applications?
    - **Auto generation -** Does the tool automatically create any documents or folders in specific storage locations? (For example; Forms autogenerates spreadsheets, and Teams generates folders in REDACTED)
    - **Duplication** – Does the tool store any copies of attachments separately within the application?
    - **Co-authoring/ownership** - where applicable is this required? if so, how will the process work?
    - **Privacy** – Is there any password protection capability? Or any other privacy controls which may need disabling or enabling?
    - **Sharing** - Internal & external considerations and can we disable if required
    - **Access** - who will have access to the tool – if specific users, how will that be managed? If force wide what access do they have, will those with guest user access be included?
    - **Local settings / deviation** – due to NEP or force policy
    - **Retention/ Deletion** -– Does the tool support retention policies? If not, what is the default retention period assigned by MS/NEP? Will deletion be automated or a manual function? If so, who will this responsibility fall to?
    - **Audit** - Is the tool supported by the Security & Compliance Centre?
    - **Disclosure** – DP/FOI considerations

- Data flow / storage location (both geographically and within MS) & Specified retention policy
- Additional information security / assurance considerations

Record of whether a Data Protection Impact Assessment is required.

DPIA Screening	
Section 1 - Governance	
Project Proposal Name:	MS Whiteboard
Information Asset Owner (IAO):	This will be dependent on the data stored / processed via the Whiteboard
Senior Responsible Officer (SRO):	REDACTED – NEP Business Change SRO
DPIA Author:	REDACTED
Date on which processing will commence:	Use of Whiteboard piloted from 24/09/2021 (Improvement & Change Department)
Date submitted to DPO	17th January 2022
Note: The DPO will give an **initial response** within 10 working days of receiving the completed form.	
Section 2 - Purpose, Scope and Context	
Please provide as much detail as possible, avoiding technical language and acronyms, explaining the proposal in a way that someone with no prior knowledge could easily understand.	
2.1 Overview Please provide the following information: • What is the overall aim and purpose of the proposal? • How and why do you intend to use personal data? • Why is the processing necessary and proportionate?	

Microsoft Description of Whiteboard;

Microsoft Whiteboard is a free-form, digital canvas where people, content, and ideas come together. Whiteboard integration in Microsoft Teams meetings is powered by the Whiteboard web app, which lets Teams meeting participants draw, sketch, and write together on a shared digital canvas.

A virtual whiteboard is a digital application that functions like a traditional whiteboard but is hosted virtually. Digital whiteboards can integrate with other video conferencing and screen sharing platforms to allow for collaboration even when you are not physically in the same room. A virtual whiteboard has multiple colours, shapes, and templates to choose from and allows whiteboards to be saved in shareable files for easy access in the future.

Users can share a whiteboard to make it available to all participants in a Teams meeting. That same whiteboard is simultaneously available in all the Whiteboard applications on Windows 10, iOS, and the web app.

Creation, access, storage, retention, and deletion:

Whiteboard is currently open to the whole force to use in Teams as an app.

Whiteboard can be used for data up to official-sensitive, and the application is accessible by users within the organisation, including those with approved Guest user access.

Whiteboards are accessible from a user's account in the Windows 11 app, iOS app, Microsoft Teams, in REDACTED or on the web.

It is possible to create a Whiteboard within the Teams Chat (1-2-1 or Group) areas, within the Teams Channel area, within the web application. There is a separate desktop version of the application which offers increased functionality such as:

- the ability to upload certain additional file types and images (including directly from the internet via Bing)
- use of webcam etc
- additional capability to export Whiteboards to MS OneNote.

REDACTED.

The web/Teams version is limited to allowing PDF and PowerPoint document types only (as an image), as well as JPG and PNG image files.

Although not advisable, it will be possible for users to upload personal data, and evidentially relevant content such as copies of custody images, CCTV and Dash Cam stills into a Whiteboard. However, it is then the responsibility of the Whiteboard owner to delete or 'wipe' the board clean once the meeting has concluded.

When you create a Whiteboard for a meeting, it is associated with the meeting and all participants (internal personnel and guest users with appropriate access permissions) will be able to access it during and afterwards. Because a whiteboard is a common resource that everyone connects to, any changes made are seen everywhere in real time.

The person who creates a Whiteboard or organises the Teams meeting is its owner.

Whiteboards created via Teams or within the web are accessible to users via a list within the web application, this list will contain Whiteboards either created by them, shared with them or those created in meetings they have attended. The Whiteboard(s) will be stored REDACTED and will therefore be retained in line with the retention policy for REDACTED (length of service plus 30 days) or until they are manually deleted. REDACTED

As stated above, it is the responsibility of the Whiteboard owner to delete or 'wipe' the board clean once the meeting has concluded. Although it is force policy that no operational or organisational data is stored in users REDACTED, if a Whiteboard is needed for a re-occurring meeting then it can be retained (REDACTED) **but only for as long as is necessary**, after which it must then be wiped clean. If a Whiteboard is moved to Sharepoint it will only show as a file conversion with a list of code.

If a copy of the Whiteboard is required, it will be necessary to export it. This will create a non-editable image of the Whiteboard which is then available to view via the exporter's downloads under their quick access in file explorer. The exporter must ensure this is moved and stored in an appropriate SharePoint site where it can be managed in line with the Force Records Retention Schedule according to the type of data that it is, i.e. project notes will be kept in line with project paperwork.

Only the meeting organiser or Whiteboard owner can delete a Whiteboard. Deletion can be actioned via the web application or via REDACTED. The owner can also delete

the tab from the Teams chat/channel/meeting; however, this will still leave the Whiteboard available for all connected users via the web app.

By default, a Whiteboard tab is added to all organised Teams meetings. This tab cannot be deleted, however, if the Whiteboard is used then the owner can delete it from the web application or REDACTED as required.

REDACTED

Sharing:

Internally it is possible to share a Whiteboard via a link taken directly from the web app or share a link via SharePoint. However, it is not permissible to share Whiteboards with anybody outside of our organisation. Should a link be shared accidentally (e.g., via email) there is no risk of inappropriate access on the basis that only those preapproved have access to our tenancy and therefore will be able to open the link.

As with many other types of documents it is possible for a copy of a Whiteboard to be shared/attached via e-mail. REDACTED.

Auto-generation:

The only auto-generation that occurs within Whiteboard is the creation of a specific "Whiteboard" storage folder within the creators/owners REDACTED.

Co-authoring/co-ownership:

It is possible to share a Whiteboard in order to collaborate; however, it is not possible to Co-own a Whiteboard.

Privacy:

REDACTED

3rd Party Applications:

Whiteboard does not integrate with any 3rd party applications (outside of O365). This is also not permissible in our tenancy.

Local settings / deviation:

See NEP LLD guidance for use of Whiteboard. No deviations from the NEP LLD have taken place.

Audit:

The current position suggests that Whiteboard content is not captured by Microsoft Teams compliance records, nor is the content indexed and available to content searches and eDiscovery cases. This may be subject to change now that the storage location has moved to REDACTED, and as such the text only within a Whiteboard might be searchable. As the functionality/capabilities of Security and Compliance are yet to be explored however, we are not able to say definitively at this time.

Disclosure:

The content of Whiteboards may be disclosable, for example under FOI Legislation or in accordance with a Right of Access request, subject to applicable exemptions.

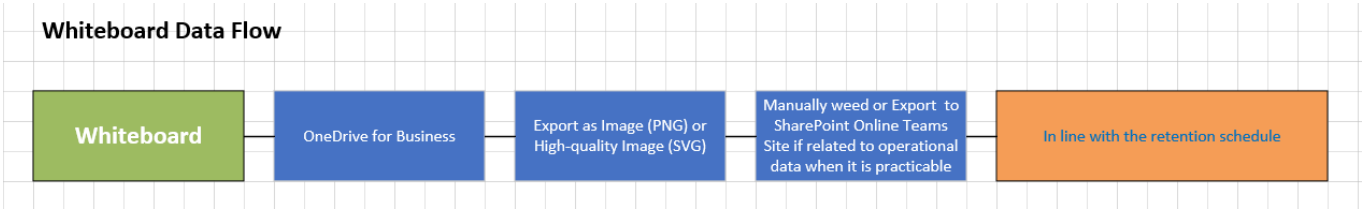
How the Whiteboard will be used in Improvement & Change;

MS Whiteboard is a collaborative virtual whiteboard that is used within Microsoft O365 and would be used during Microsoft Teams meetings in place of a real whiteboard in in-person meetings.

This is primarily to: support note taking (for non-written notes); aid in teaching/tutoring concepts that are more visual than oral; run workshops etc.

Data entered onto the Whiteboard will be freely given by attendees of the virtual meetings (e.g., if the meeting initially determines a list of actions, these may have attendees' names against them up until the time that the white board is "converted" into a written document (for actions/minuting purposes). This should be rare and proportional.

Whiteboard Data Flow



**content of orange box should read: Retained in line with the retention schedule.*

The LLDs state the following for Whiteboard:

Whiteboard gives teams a freeform, intelligent canvas for real time ideation, creation, and collaboration. Whiteboard provides an infinite canvas to draw, type, add images and use sticky note. Designed for pen, touch, and keyboard, Whiteboard allows force users to share ideas naturally. Intelligent ink recognizes shapes and makes creating tables a snap.

ID	Decision	Rationale
DR3-AC11	Forces should enable Whiteboard for all force users. Forces are also advised to ensure that the relevant adoption and technical support is available for force users.	Whiteboards provides a useful canvas for users to collaborate in virtual meetings. Whiteboard is included in the MOU licensing and could provide a cost saving against similar third-party services, whilst also keeping data within Microsoft 365.

Table 154 Design Decision - Whiteboard

8.8.2 Architecture

All your whiteboards are automatically and securely saved in the forces Microsoft Azure.

Whiteboards are owned by their creator and can be shared with others.

8.8.3 Clients

Whiteboards can be simultaneously accessed in the Windows 10, iOS, and web app Whiteboard applications.

8.8.4 Access

The Whiteboard configuration is accessed in the Microsoft 365 admin center, on the 'Whiteboard' page under the 'Org settings' header. The NEP recommends the configuration detailed in Table 155.

Feature	Setting	Value
Whiteboard	Turn on Whiteboard for everyone in your org	Yes
	Level of diagnostic data to send to Microsoft	Neither
	Optional Connected Experiences	Yes
	Enable easy sharing of Whiteboard from Surface Hub	Yes

Table 155 Whiteboard configuration

Note: If required, forces administrators can enable and disabled Whiteboard license for an individual user. Refer to 'Enable Microsoft Whiteboard for your organization' [124] for instructions

2.2 Nature and Scale of Processing

2.2.1 Does the processing involve operational and/or administrative data? (Please select below)

☐ Operational Data (Personal data processed for law enforcement purposes)

☐ Administrative Data (Personal data processed for non-law enforcement purposes)

As this is a new technology it is unclear how the force intend to use whiteboards, for the specific use case we have in and other requests from People Development it is not operational data, REDACTED.
Content is more likely to contain administrative data, diagrams, blue sky thinking type scenarios, which may contain personal data.

2.2.2 What categories of data subject are involved? (Please select all applicable

categories below)

☐ Persons suspected of having committed or being about to commit a criminal offence

☐ Persons convicted of a criminal offence

☐ Persons who are or may be victims of a criminal offence

☐ Witnesses or other persons with information about offences

☐ WP Employee (current, former and voluntary)

Yes - Other

If other then please provide further details below:

There is a potential for any of the above categories of data subject to be used; however, we have no way of defining at this time as this will be dependent on the user and purpose for which the Whiteboard is being utilized.

For the specific use case within the Improvement & Change Department, it is not expected that there will be any data subjects.

2.2.3 What categories of personal data will be processed? Provide an overview of the categories of personal data that will be processed, for example: names, DOB's, addresses, vehicle registration plate number, health data, criminal records, or any other unique identifiers such as IP addresses, usernames, e-mail addresses.

For the current known uses of Whiteboard (in People Development and Improvement and Change) personal data is not intended to be processed and therefore no categories of personal data. However; there is no way of knowing how the wider force and OPCC will use Whiteboard yet and it is highly likely that personal data will be processed.

2.2.4 How many data subjects will the processing affect? (Please specify one answer below)

☐ Fewer than 100 data subjects

☐ 100 to 1000 data subjects

☐ 1000 to 5000 data subjects

☐ More than 5000 data subjects

Other: This is difficult to ascertain at this time as we are unsure how the Force and OPCC intend to use Whiteboard

2.2.5 Will it involve the collection of new information about individuals?

☐ Yes

☐ No

Other: This is difficult to ascertain at this time as we are unsure how the Force and OPCC intend to use Whiteboard

2.2.6 Will the processing involve making decisions or taking actions against individuals in ways which can have a significant impact on them?

☐ Yes

X No

Other: This is unlikely, however difficult to ascertain at this time as we are unsure how the Force and OPCC intend to use Whiteboard

2.3 Data Source and Collection

How will the data be collected? Outline how you will obtain the data, for example: directly from data subjects, from another data set already in WP's possession, from a partner agency?

Within Improvement & Change Department, the data recorded on the Whiteboard will only be gathered from individuals attending the meeting.

For use by Force and OPCC it should be noted that data could be drawn from any meeting attendees, WP / OPCC personnel, other databases, or the internet.

2.4 Data Sharing

Does the processing involve:		**Yes or No**
1.	Data being shared with third parties external to WP or recipients that have not previously had routine access to the information?	**No**
2.	Transferring the data outside the UK?	**No**
3.	Storing data using a cloud service provider?	**REDACTED**

2.5 Data Controller and Processor Relationships

Is WP: (Please consult your DPO if you are unsure)

☐ Data Controller (Sole)

2.6 Lawful Basis

To process personal data you must have a lawful basis. Please consult your DPO regarding this

Lawful Basis for Operational Data:

Lawful Basis for Administrative Data:

The lawful basis for this processing activity will vary dependent on the purpose for which the data is being processed and the type of data being processed. However it is likely to be one of the following:

UK GDPR, Article 6 (1):

(c) necessary for compliance with a legal obligation to which the controller is subject;

(e) necessary for the performance of a task carried out in the public interest

UK GDPR, Article 9 (2):

(f) necessary for the establishment, exercise or defense of legal claims or whenever the courts are acting in their judicial capacity

(g) necessary for reasons of substantial public interest

DPA (2018), Part 3, Section 31: The law enforcement purpose

Section 3 – ICO: Additional Factors

The Information Commissioner's Office have published a number of factors that present a 'high risk' when processing personal data and these factors. Saying yes to one or more of the following may indicate that the processing is medium/high risk and a full DPIA is likely to be required.			
Does the processing involve:		**Please check either Yes or No**	**If 'Yes' then please provide further details**
1.	**Systematic, extensive and large scale profiling and automated decision-making about people?** *"Any systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects, or significantly affect the natural person"*	☐ **No**	Click here to enter text.
2.	**Large scale use of sensitive data or criminal offence data?** *"Processing on a large scale of special categories of data, or personal data relating to criminal convictions and offences referred to in Article 10"*	☐ **No**	Click here to enter text.
3.	**Public monitoring?** *"Systematic monitoring of a publicly accessible area on a large scale"*	☐ **No**	Click here to enter text.
4.	**New technologies or techniques?** *"Processing involving the use of new technologies, or the novel application of existing technologies (including Artificial Intelligence)"*	☐ **No**	
5.	**Profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit?** *"Decisions about an individual's access to a product, service, opportunity or benefit which is based to any extent on automated decision-making (including profiling) or involves the processing of special category data"*	☐ **No**	Click here to enter text.
6.	**Biometrics/genetic data?**	☐ **No**	Are Custody counted in the Biometrics data?

	"Any processing of biometric data" ***and/or*** *"any processing of genetic data other than that processed by an individual GP or health professional, for the provision of health care direct to the data subject"*		
7.	**Data matching?** *"Combining, comparing or matching personal data obtained from multiple sources"*	☐ **No**	Click here to enter text.
8.	**Invisible processing?** *"Processing of personal data that has not been obtained direct from the data subject in circumstances where providing a Privacy Notice would prove impossible or involve disproportionate effort"*	☐ **No**	Click here to enter text.
9.	**Tracking?** *"Processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment"*	☐ **No**	Click here to enter text.
10.	**Targeting of children or other vulnerable individuals?** *"The use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children"*	☐ **No**	Click here to enter text.
11.	**Risk of physical harm?** *"Processing is of such a nature that a personal data breach could jeopardise the [physical] health or safety of individuals"*	☐ **No**	Click here to enter text.
12.	**Evaluation or scoring?** *"Aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements"*	☐ **No**	Click here to enter text.

13.	**Data processed on a large scale.** *Considerations include:* • *The number of data subjects concerned* • *Volume of data and/or range of data items* • *Duration, or permanence, of the data processing* • *Geographical extent of data processing*	☐ **No**	Click here to enter text.
14.	**Preventing data subjects from exercising a right or using a service or contract?** *The rights are:* • *The right to be informed* • *The right to access data* • *The right to rectification* • *The right to erasure* • *The right to restrict processing* • *The right to object* • *The right to portability* • *Rights relating to automated processing*	☐ Yes ☐ No	The current position suggests that Whiteboard content is not captured by Microsoft Teams compliance records, nor is the content indexed and available to content searches and eDiscovery cases. This may be subject to change now that the storage location has moved to REDACTED, and as such the text only within a Whiteboard might be searchable. As the functionality/capabilities of Security and Compliance are yet to be explored however, we are not in a position to be able to say definitively at this time.

Section 4 – Risk Assessment

Have you identified any risks that the processing will present for data subjects, and if so have you considered what mitigations you could implement? Please detail below.

Risk Risks to the privacy and rights and freedoms of data subjects	**Severity** Scale: High, Medium, Low	**Likelihood** Scale: Remote, Possible, Probable	**Mitigation** Mitigating solutions proposed or already implemented
REDACTED	REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED	REDACTED
REDACTED	REDACTED	REDACTED	REDACTED

Section 5 – DPO Assessment

*****DPO Use Only*****

A. A DPIA is not required.	☐	
B. A DPIA is not required as long as the remedial action listed is carried out. If the remedial action is not carried out, a DPIA will be required.	X	A full DPIA is not required – this screening document accurately identifies the core (known) information governance considerations, identifies risks and sets out appropriate actions than can and should be taken to mitigate those risks. It must be acknowledged that due to this being a (relatively) new technology that will be made available to the whole force and OPCC, how it is intended to be used and how it will eventually be used are likely to differ. Should there be any fundamental changes (to include those imposed by Microsoft) this DPIA should be updated. REDACTED, DPO, 19th January 2022
C. A DPIA is required.	☐	