National Records of Scotland

M365 Guidance

from the

Keeper of the Records of Scotland's PRSA Assessment Team

Introduction

With many of Scotland's public authorities considering the adoption of Microsoft in the Cloud (M365) as their principal records and information management solution, the Keeper of the Records of Scotland's (the Keeper) Assessment Team has developed this guidance to help authorities understand some of the issues associated with implementing M365. It is hoped that by having regard to this guidance authorities can develop solutions to these issues and, in so doing, ensure they remain compliant with expectations under the Public Records (Scotland) Act 2011 (the Act).

The guidance does not seek to offer answers to all the issues highlighted. Rather, it suggests questions that an authority (the public authority named in the Act) implementing M365 might ask, and maps these to the relevant elements in the Keeper's Model Records Management Plan: Model Records Management Plan | National Records of Scotland (nrscotland.gov.uk) (the Model Plan). It uses the Model Plan layout to pose these questions, and under each of the 15 elements, it lists what is required as it appears under the Model Plan. It begins each individual guidance text with a brief explanation, drawn from the Model Plan, of what the Keeper's expectations are for the purposes of compliance. The Model Plan was written in collaboration with stakeholders and represents what the Keeper considers are the core record management facets that must be considered by public sector records managers.

This guidance document is specifically for those considering a M365 roll-out. For guidance around the Keeper's records management expectations generally, and examples of best practice, please see Introduction to Guidance for Model Plan | National Records of Scotland (nrscotland.gov.uk)

It should be noted that this guidance leans on the work of a Microsoft Customer Advisory Board (CAB) where records management is discussed directly with the M365 development team by representatives from the international information governance and records management sector. The CAB was itself developed from a roundtable facilitated by the Information and Records Management Society in July 2020. The Roundtable is available to watch again online at https://www.youtube.com/watch?v=BeEKhLAF9rE.

When considering the records management implications of a M365 roll-out in public authorities, records managers should probably start with Microsoft itself, Records Management in Microsoft 365 - Microsoft 365 Compliance | Microsoft Docs, bearing in mind that M365 is a complex product designed as a business communication and collaboration tool rather than an electronic document and records management system (eDRMs). Although it is a single product, M365 contains a whole suite of different applications that can be used for creating and storing information and records.

Microsoft 365 and the Keeper of the Records of Scotland's Model Records Management Plan: Issues for consideration under each Element

Element 1 - Senior management responsibility

An individual senior staff member is identified as holding corporate responsibility for records management.

"Section 1(2)(a)(i) of the Act specifically requires a RMP to identify the individual responsible for the management of the authority's public records. An authority's RMP must name and provide the job title of the senior manager who accepts overall responsibility for the RMP that has been submitted."

1.1 Roles

There is no suggestion that the adoption of M365 should change the identification of the individual with overall responsibility for records management in an authority.

Element 2 - Records manager responsibility

An individual staff member is identified as holding operational responsibility for records management and has appropriate corporate responsibility, access to resources and skills.

"Section 1(2)(a)(ii) of the Act specifically requires a RMP to identify the individual responsible for ensuring the authority complies with its plan. An authority's RMP must name and provide the job title of the person responsible for the day-to-day operation of activities described in the elements in the authority's RMP. This person should be the Keeper's initial point of contact for records management issues."

2.1 Roles

Within its various control centres, the M365-package comes with a variety of 'roles' that must be allocated to individuals within the authority. These will generally fall, in the first instance, to IT professionals within the organisation. It is important that some of these roles, particularly within the Security and Compliance Centre, are then delegated to the individual responsible for the day-to-day management of the authority's records (hereafter referred to as 'records managers' regardless of the actual job title allocated to the role in an organisation – for example, the compliance administration and disposition management roles). Within the control centres, there are also a number of available reports which can support records managers to manage information and records. The individual identified at Element 2 should ensure that the relevant reports are provided directly to them rather than via IT professionals. An appropriate role structure that suits the organisation's business will have to be agreed internally.

For more about roles look at: Search Results for "M365 roles" – Records about the world (wordpress.com) and Permissions - Security & Compliance Center - Office 365 | Microsoft Docs.

Questions:

- Are the M365 roles properly allocated?
- Does the individual named under Element 2 have access to relevant control centre reports?
- Is the individual at Element 2 able to undertake or delegate responsibility within their team of the disposition review role?

2.2 Knowledge / Understanding

M365 is a complex system compared with the shared network drives or eDRM systems that most public authorities operate. In fact, it is several applications rolled into one platform. It is important that the named individual at Element 2 understands the mechanics behind M365 rather than just the practical 'how-to-save' instructions that all staff need. Furthermore, the package is continually evolving as Microsoft develops new functionality. It is crucial that the individual identified at Element 2 is kept informed of these changes to enable them to consider the implications for the authority. On some occasions, a decision may be required as to whether or not the change should be applied within the authority. If this decision affects records management, the individual identified under Element 2 should be involved in that discussion. For more about the changing nature of M365 see Microsoft 365 Roadmap - See What's Coming | Microsoft 365.

Questions:

- What resource is being provided to train relevant staff, particularly the individual identified at Element 2, in the details of how M365 works?
- How is the person at Element 2 updated in regard to the latest developments in M365? Do they have appropriate input in any decision as to whether optional changes are applied?

2.3 Involvement in Project

It is probable that the implementation of M365 will be led by IT departments. It is imperative that the person identified at Element 2 is fully involved in the project by having an understanding of the implementation plans as well as providing expert opinion, both on the controls which should be applied and the content of user guidance and training. Furthermore, their involvement must continue as the product develops over time. While it is not necessary for the person identified at Element 2 to be an expert in the technology which drives the process of why things happen (that's for IT Professionals) they will need to have a clear understanding of what happens to a specific record. This includes what can happen to a record dependant on the settings applied, particularly in relation to SharePoint, Exchange, and OneDrive, and where a record stored in those systems can be accessed and monitored.

Questions:

- What formal relationship between IT and RM is set up within the organisation and how do these teams engage with one another. Is there, for example, a joint RM/IG/IT project group?
- Is the records manager involved in decisions on what settings should be applied when those affect the management of information and records?

2.4 Provision of User Training

The individual identified at Element 2 is likely to have some responsibility for providing advice and training to other staff.

Questions:

- How will the individual identified at Element 2 meet this responsibility?
- Are / will they be involved in the creation and delivery of training packages?
- How can they be satisfied that they have access to the appropriate professional development to learn and transfer M365 skills and knowledge?
- Will Microsoft help records managers directly, or will they only engage with the IT Team?
- Can the authority be satisfied that there is there enough/appropriate M365 guidance online and, if so, can the records manager easily point colleagues to that guidance?

Element 3 - Records management policy statement

The authority has an appropriate policy statement on records management.

"The Keeper expects each authority's plan to include a records management policy statement. The policy statement should describe how the authority creates and manages authentic, reliable and useable records, capable of supporting business functions and activities for as long as they are required. The policy statement should be made available to all staff, at all levels in the authority."

3.1 Application of Policy

The effect of introducing M365 on this Element will vary from authority to authority, and depend on whether the Records Management Policy describes the situation in general terms, or whether it takes a more in-depth IG Strategy approach. Either way, the authority will need to be confident that all of the aspirations in the Policy are achievable after the M365 roll-out.

It is important to remember that, under the Act, the Keeper considers any information that is generated by a public authority in delivering its functions, stored on any system, is a public record. To reiterate, the Keeper does not differentiate between documents that are somehow elevated or 'declared' 'public records' and other, apparently less formal, documents. Like other Information legislation in the UK, such as the Freedom of Information Act, the Public Records (Scotland) Act "is not limited to official documents and it covers, for example, drafts, emails, notes, recordings of telephone conversations and CCTV recordings." However, there are various M365 applications that seem to indicate alternative records management processes depending on the formality of the document, i.e., where action must be taken to 'declare' a record as such. It is important to remember that M365 applications have varied levels of functionality depending on the licences purchased and are not designed for Scottish public authorities in particular. Incorporating tools to maintain adherence to country-specific and public sector-specific legislation is not within Microsoft's, but the public authority's, remit. For more about Microsoft's stance on this, see Declare records by using retention labels - Microsoft 365 Compliance | Microsoft Docs.

Questions:

- Is the authority confident that their Records Management Policy can be applied comprehensively across all information being created and managed on the M365 platform?
- How will the authority address the M365 option to 'declare a record' and ensure this aligns with the Keeper's expectations and in compliance with Section 3, 'Meaning of public records, of the Public Records (Scotland) Act 2011 (Public Records (Scotland) Act 2011 (legislation.gov.uk))?

3.2 Licences

There are various licencing tiers available in M365. If the organisation is a small public authority, they may be able to operate with a licencing structure that does not extend beyond an E3 (limited rights) licence. However, for any complex authority, one that has a large

number of record creators, or one that is subject to various and varying legislation, they may need to consider access to broader functionality. E5 licences, or a Premium Service with enhanced automation to gain greater administrative rights, may be essential in satisfying the Keeper that all records are being satisfactorily managed. Some authorities have chosen to manage this situation by operating under E3 licences, but with a third party bolt-on (a function or compliance extender) to make up for a perceived records management deficit under M365.

The authority will need to consider which members of staff require a particular licence. For example, is it possible for the authority to operate with most of the record creators on a basic tier licence (E3), and the information governance admin officers records managers on something more substantial (possibly an E5 licence)? This will remain a business decision for an authority, and should be discussed with Microsoft at the outset. It is important that information governance compliance records management, and the need for the authority to have systems that allow it to meet its regulatory obligations, is considered in these discussions.

To inform decision-making around licences, Microsoft provide a general comparison between the different licensing tiers:
Microsoft Modern Work Plan Comparison - Enterprise US ERP.pdf.
They also provide a specific 'compliance' comparison here:
Download Detailed Microsoft 365 Compliance Licensing Comparison XLS (April 2021) from Official Microsoft Download Center.

For an independent take on this subject:
What licences or roles are needed to manage records in Microsoft 365 – Records about the world (wordpress.com).

Questions:

- Has the records manager been sufficiently consulted regarding the licencing?
- Will the licenses provided to users allow for the appropriate control of records?
- Will all record creators in the organisation need to be on the same licence tier?
- If only the records managers have an advanced licence, will they require additional resource to carry out all the activities needed (perhaps there will be responsibilities that now fall to them that were previously undertaken by record creators)?

3.3 Third-party bolt-on

As noted above, some Scottish public authorities have chosen to adopt a third-party add-on to the M365 platform. Authorities may take this step for any one of several reasons. For example, they may judge that a bolt-on will allow them to manage and record the disposition of records in a smoother fashion than Microsoft's native functionality.

However, careful consideration requires to be given as to whether the third party will have access to the records, and how they will keep up to date with the ever evolving nature of M365.

Questions:

- Due to the developing nature of the M365-package, how can the organisation ensure that the bolt-on will continuously evolve or “keep up”? The third-party may only be responsible for providing the technical functions in the original contract which may result in difficulties if/when these are overtaken by developments in M365.

- If an authority is engaging with a third-party service provider to enhance the M365 platform, are they satisfied that they have implemented appropriate privacy/security agreements in place to protect their information?

Element 4 - Business classification

Records are known and are identified within a structure, ideally founded on function.

"The Keeper expects an authority to have properly considered business classification mechanisms and its RMP should therefore reflect the functions of the authority by means of a business classification scheme, information asset register or similar. This should record, at a given point in time, the information assets the business creates and maintains, and in which function or service area they are held. As authorities change, the structure should be regularly reviewed and updated. A classification structure allows an authority to map its functions and provides a system for operating a disposal schedule effectively."

4.1 File Plan

An authority with an agreed Records Management Plan should have a business classification scheme (BCS), a file plan, or an information asset register (IAR), or have been in the process of developing one. The Keeper will expect an authority to be able to demonstrate how it has imposed that scheme in the structure of their M365 roll-out.

Questions:

- How is the organisation's file plan to be represented on the M365 structure?
- How are records transferred from the current system into M365?
- A BCS/file plan/information asset register is a 'living document'. What are the practical steps needed to make regular changes to the scheme on M365?
- How will the organisation ensure documents are 'classified' as per the BCS?

4.2 Applications

M365 provides a large package of applications, some of these are for analytical and technical purposes, but many can be used for the creation/storage of information and records. A snapshot of the M365 platform can be found here: https://pro.jumpto365.com/@/hexatown.com/PTO365.

To be compliant with the Act, an authority must be aware of where its public records are being managed. The Keeper requires that an authority's Records Management Plan considers records held in

a) Digital format on the main records management system (such as shared drives or an eDRM),
b) On 'line of business systems' such as a case management system, or
c) In hard-copy format; for example paper files in a filing cabinet.

The authority must satisfy the Keeper that the systems used are being properly managed. M365, however, has expanded the range of places that an authority's information and records might be created and managed to include associated Microsoft applications, such as Sway, Forms, Lists, To Do, Yammer, Loop or Planner.

Records managers are used to e-mail records being created in Outlook, and will have an email policy that governs how these are deleted or moved to the main records management system. Microsoft proposes that users do not move records, for example, from Exchange to SharePoint. The default position of M365 is that records will be managed within the application in which they were created, and will be located using the powerful in-built search functionality. This has implications for how public authorities manage their records if they are stored in applications rather than in departmental folders.

Questions:

- Has the records manager been sufficiently consulted regarding what new applications staff will be permitted to use? This is likely to be an ongoing requirement as new functionality in M365 is developed.

- Is the records manager absolutely clear which applications are actively being used to create records? If not, how can they be provided with reports/alerts that will give them this information?

- How will an authority control 'data sprawl' (where record around a specific topic or project are scattered across multiple applications)? Could this lead to incomplete record collections in the future where, for example, they wish to refer to past activities, but only the records moved to SharePoint are still locatable?

- Do public records stay where they are created or are they moved into a SharePoint folder structure? If the latter, who does this? The record-creator? RM/IG staff? Do they have the relevant permissions to do this?

- Are all the applications in which records can be created and stored necessary for the business? Do an organisation's activities allow limits to be applied to staff usage of certain products on the platform? In short, does everything have to be switched on?

- Is the authority satisfied that all record creators know what is expected of them when they have created a record on an M365 application (and, of course, that they recognise what a 'record' is)? For example, if a business areas is using Sway, how will the record-creator know what to do with the records they have created? Remember that if it is necessary for record creators to move records out of the application in which they were created (into a SharePoint folder, for example), M365 will not prompt them to do this.

- Can the authority be assured that they have taken every step to avoid duplication? Does the Record Manager's administration privileges allow them to identify where the same record is being held (or worse, edited) separately on more than one application? The issues around the dangers of duplication is nothing new to records managers. However, they should be convinced that the processes in place to limit this – previously explained in the authority's Records Management Plan – are still applicable under the new M365 system.

- How will records managers have sight over the volume of records/information being stored, in terms of data storage size and file numbers?

- How will records managers be aware of all the 'containers' which have been created, such as Teams or SharePoint sites?

Whether staff are permitted to use all the applications provided in the M365-package should remain a business decision for the authority, but the questions above should be considered for each. However, if M365 is adopted, the organisation will certainly be using SharePoint and Outlook, and it is likely that they will also use Teams.

4.3 Teams

When a Teams site is created, a separate SharePoint site is automatically created in the background. Any documents created in the Teams site will be saved to the correlating SharePoint site. A report on all SharePoint sites should identify these. However, Teams chat messages and channel conversations are not saved to SharePoint, but to Exchange. Teams chats and channels, for as long as they are retained, are public records. A report into all SharePoint sites will **NOT** identify records held on Exchange. Furthermore, Teams also offers the function to record meetings and offers other collaborative communication tools. These are all public records for as long as they are retained on the platform.

Questions:

- Does the records manager have appropriate access to Teams Admin? Can they be satisfied that they will be able to review where public records created on Teams are held?

- Teams chat, while it is retained, is a public record. Is the authority satisfied that the records manager understand how symbols (such as a 'thumbs up' emoji) or attachments in the chat are captured?

- Has the authority applied a retention policy to mailboxes (see “E-mail” below), and are they satisfied that this will adequately protect any teams chat/channels they might want to keep?

- Does the authority have procedures for managing inactive Teams sites and the public records in them? Who is responsible for this? Is it, for example, the owner of the Exchange mailbox account (or group mailbox) to which the site is connected?

4.4 Legacy, line of business and non-standard format Records

Most public authorities will not be starting from scratch with M365, and will hold legacy records - possibly in paper-format. They may also create public records in non-standard format (such as databases or templates), or use specialist line-of-business systems such as for case management.

Questions:

- How will legacy records be accounted for in the M365 structure? Is it the intention for the organisation to run two systems until the natural disposition of the legacy records?

- What are the limitations on managing hard-copy records, or records in non-typical formats, with M365? These may be listed in the authority’s information asset register, but can they be acknowledged on the M365 platform?

- What line-of-business systems does the authority have? Can these be accounted for?

- Can M365 cope with the templates that are currently being used? For example, can these be transferred to MS Forms?

- What is the authority’s policy for oral recordings, such as meetings or presentations? This is a developing area of long-term, legally defensible recordkeeping.

4.5 E-Mail

M365 is designed to save e-mails in Exchange rather than in SharePoint. Outlook e-mails are not designed technically for saving in any other application than Exchange, and therefore do not drag-and-drop particularly successfully. If e-mails are only saved in individual Exchange folders, this can lead to significant problems with retention, access and archiving.

Question:

- How are e-mails managed? Does the authority keep them in Exchange, or move them to SharePoint? Do staff receive guidance on how to do this? How does the records manager check? How and when are they irretrievably deleted from M365 (Exchange)?

4.6 Tenancy

It is possible for one ‘umbrella’ authority to license an iteration of M365 and then to have a sub-tenant share in this platform. This is not particularly common, but, if this scheme is adopted, the ‘sub-tenant’ needs to understand what permissions they have to make alterations to the main tenancy settings. They also need to understand how they can maintain their role as data owner and have full control on their information and records. They need to be able to differentiate between different sub-tenant records, and have access to reports to allow them to do this.

Questions:

- Can ‘sub-tenant’ authorities develop their policies, for example around retention or sensitivity? If, for example, a particular tenant wants to keep a particular record type longer than everyone else (perhaps for research purposes), is there any way for them to do this?

- Can boundaries be put in place to allow sub tenants to ring-fence their data, and easily identify which records and information belongs to them (as opposed to other sub-tenants)?

- Can sub tenants be given access to admin centres to manage their own data, or will this be done by a centralised team? If so, how does this affect ownership and abilities under Element 2?

Element 5 - Retention schedules

Records are retained and disposed of in accordance with the Retention Schedule.

"Section 1(2)(b)(iii) of the Act specifically requires a RMP to include provision about the archiving and destruction or other disposal of the authority's public records. An authority's RMP must demonstrate the existence of and adherence to corporate records retention procedures. The procedures should incorporate retention schedules and should detail the procedures that the authority follows to ensure records are routinely assigned disposal dates, that they are subsequently destroyed by a secure mechanism at the appropriate time, or preserved permanently by transfer to an appropriate physical repository or digital preservation system."

5.1 Retention Policies

The management of disposition in M365, either by destruction or transfer to archive, is a major issue to be considered at the earliest possible opportunity when implementing the platform. This is crucial even if, potentially, an authority will not be applying a disposition process for several years. The foundation of this will be the clear allocation of retention decisions at the outset.

Although it is to be expected that an authority will already have a retention schedule in place, M365 now gives it the ability to apply retention to a document by Policy, Tag (where retention is applied to the whole folder), or Label (where retention is applied at document level). E5 licence-holders have the authority to apply all these options to a single record and, unfortunately, the platform is not designed to report on contradictory decisions. It is possible, for example, that a *label* could be applied to a record to destroy it after 7 years, which is then stored in a folder that has a 'permanent' retention tag, which subsequently becomes subject to a *policy* that accords that record type with a 3-year retention. Records managers will need to be alert to this possibility.

There is a useful primer video by Joanne Klein, a M365 consultant, on the IRMS YouTube channel that will help with this: https://www.youtube.com/watch?v=JIGzLztBMM8.

Although an organisation should always try and keep copies to a minimum (see under Element 4 above), sometimes, for business purposes, creating a copy is unavoidable. It will be important to understand how retention decisions are applied to copies under M365.

Retention/destruction labelling for records managed on M365 is a developing issue and there are several sources for latest developments. For example, Rob Bath at Intelogy has a blog records managers may wish to follow: https://www.intelogy.co.uk/blog/sharepoint-retention-labels-align-with-onedrive-to-use-the-preservation-hold-library/.

Questions:

- How is retention to be applied? To a document? To a folder? To a record type using a 'policy'? To an individual account (unusual, but possible in M365). To an application? Are records managers involved in this decision?

- Are records managers confident that retention is mandatory? That records cannot be created with no retention, or created and then have their retention removed? Generally, how much control does the authority have over the retention that is applied to a record at the time of creation? For example, is the records manager clear about the possibility of a user editing a document (which they may want), also editing the retention decision applied to that document (which they may not want).

- Is the authority clear about whether 'retention' or 'destruction' is being applied, and what the difference is?

- Who can change retention decisions on a record and can these changes be shorter as well as longer? Similarly, as a retention schedule is a 'living document' are relevant staff clear about the process for changing the retention decision on an entire record type?

- Is the authority clear about how retention decisions on a record automatically change if it is moved to a new location?

- If there was a sudden need for the retention decision on a record to be changed (for example if they were unexpectedly needed for a public inquiry purposes), how is this done? Can it be done in bulk?

- If a business area normally allocates 'event-based retention' on certain records, can they carry this over to M365?

5.2 Retention in Teams

Teams can, of course, be used to create public records, but it can also be used to share copies of records from other sources and is, therefore, not always the original location of a record stored in the application. Does an authority need Teams channels to be permanently 'archived', for example to record advice given over teams chat? Alternatively, what happens if there is information in a Teams channel that an authority should delete, such as someone's address, where there are other things in the same chat that an authority feels it should retain?

Questions:

- What is the authority's policy for applying retention in Teams going to be, and how will they a) apply it, and b) monitor whether users are following that policy?

- Who is responsible for applying retention in Teams, and how do they get advice about this?

5.3 E-mail

An authority probably has an e-mail policy in place by which they instruct staff to routinely clear up their e-mail accounts. With M365, there is a default expectation that e-mails will be managed in Exchange rather than a SharePoint site. It is important that this is understood, and the authority considers whether its e-mail procedures may have to be adjusted to take account of this?

Questions:

- How is retention applied to e-mail accounts? Is there a danger that too much trivia will be kept or too much of value deleted? Also, see the dangers of keeping personal information beyond business need under Element 9.
- How can the authority be confident that their e-mail policy applies to all mail, regardless of where in the system it is being created and stored?
- How can the authority ensure that emails stored within Exchange are retained for their full retention period if a staff member leaves, and their account and associated information and records (emails) are deleted.

Element 6 - Destruction arrangements

Records are destroyed in a timely and appropriate manner and records of their destruction are maintained.

"Section 1(2)(b)(iii) of the Act specifically requires a RMP to include provision about the … destruction, or other disposal, of an authority's public records. An authority's RMP must demonstrate that proper destruction arrangements are in place."

6.1 Destruction of Records

At the time of the Keeper's original agreement for an authority's RMP, it will have explained how it plans to destroy digital records in a controlled, secure and irretrievable way. An authority adopting M365 must review that explanation, and ensure that the procedures in place are still applicable.

Questions:

- What happens when a record gets to the end of its retention period? Is it deleted automatically, or does it get flagged up for deletion? If the latter, to whom is it flagged up?
- Can the organisation apply large-scale destruction commands, such as 'all the receipts from 2015', or does each have to be marked for deletion individually (e.g. a check box)?
- Does the authority need more than one authorisation for deletion - for example, Information Asset Owner, then Archivist, and then the IG Team? If so, can this serial disposition arrangement be operated with the M365 licence arrangement the organisation has?

6.2 Destruction Logs

Best practice, as explained in the Keeper's Model Plan, would suggest that an authority should be able to evidence the records that have been destroyed. This is normally done through the retention of a destruction log or similar. This is not an automatic feature of M365, where the default position is that destruction logs are limited by their own 7-year retention, and do not necessarily cover all records – only those particularly selected for disposition review. There is clearly potential here for records to simply disappear from the system with no record that they ever existed. This is not an acceptable position for any public authority committed to meeting its statutory obligations.

Questions:

- Does the authority require Teams channels to be permanently 'archived', for example to record legal advice given over Teams?

- What happens if there is something in a Teams channel that the authority should not keep (such as someone's address), but where there are other things they must retain? What is the policy for that going to be, and how will the authority a) apply, and b) monitor that policy?

6.3 Teams

Questions:

- Is the authority satisfied that the set-up of M365 will allow them to prove that a record was destroyed at a particular time?

- Does the authority have a work-around for M365's default 7-year retention of destruction logs?

- If the authority chooses to intervene to create a destruction log, are they confident about what metadata needs to be kept in the log?

- What licencing structure will record managers need to access any destruction logs (in the first 7 years)?

6.4 Containers

Question:

- SharePoint sites and libraries, Teams Channels, Exchange accounts and other applications can all hold public records. When destruction is applied to all the records in a 'container', what happens to the container itself? Is it automatically deleted? Does it sit empty?

- Is there a process to allow the records manager to be alerted to 'empty' containers?

Element 7 - Archiving and transfer arrangements

Records that have enduring value are permanently retained and made accessible in accordance with the Keeper's 'Supplementary Guidance on Proper Arrangements for Archiving Public Documents'.

"Section 1(2)(b)(iii) of the Act specifically requires a RMP to make provision about the archiving and destruction, or other disposal, of an authority's public records. An authority's RMP must detail its archiving and transfer arrangements and ensure that records of enduring value are deposited in an appropriate archive repository. The RMP will detail how custody of the records will transfer from the operational side of the authority to either an in-house archive, if that facility exists, or another suitable repository, which must be named."

7.1 Transfer to Archive

The Public Records Act requires each authority to identify a suitable repository for the retention of the small selection of that authority's records that have been selected as appropriate for permanent preservation, and to have a formal transfer agreement with that repository.

As is the case with hard-copy records, the document being transferred must normally be the original, not a copy. This is very important in the case of digital records where a copy may, on face value, appear identical to the original. In M365, a copy is treated as an entirely new 'item', and is not connected to the original. Most importantly, the metadata sitting behind it will be that of the copy, not the original. This obviously raises questions around authenticity. An archive will want to ensure the metadata of the original is captured along with the record.

For this element, it is recommended that the authority liaises with their identified archive repository.

Questions:

- Can certain categories of record be allocated an 'archive' designation at the time of creation (for example, could records identified as 'board minutes' be allocated a permanent preservation retention decision automatically)?
- Can an authority transfer those records identified for permanent preservation from M365 to an archive, carrying across the original metadata?
- Is the authority certain their archive can accept these transfers?

Element 8 - Information security

Records are held in accordance with information security compliance requirements.

"An authority's RMP must make provision for the proper level of security for its public records. An authority's RMP must therefore include evidence that the authority has procedures in place to adequately protect its records … The security procedures must put in place adequate controls to prevent unauthorised access, destruction, alteration or removal of records."

8.1 Access Controls

An authority may have to rewrite some of its information security policies to account for new systems and mechanisms specific to M365, but generally M365 should be able to keep its information assets secure.

Beyond revising policies and procedures, an authority will want to make sure that suitable monitoring can be undertaken by those responsible for information security, and that audit logs can be accessed, and access control applied, with the same robustness as was agreed by the Keeper under the authority's Records Management Plan.

For this element, it is recommended that the records manager liaise with the identified information security lead.

Questions:

- M365 allows the application of access permissions to certain groups or individuals. Is the authority clear on how this is done? Is it clear on how this can be changed – if someone changes roles for example – and on who has the relevant administrative permissions to do this?
- Has the organisation deployed appropriate controls to ensure that information and records are not inappropriately downloaded onto non-corporate devices (given that users can access Office.com from any web connection)?
- Has the organisation written a System Security Policy for use of the platform?

Element 9 - Data protection

Records involving personal data are managed in compliance with data protection law.

"The Keeper will expect an authority's RMP to indicate compliance with its data protection obligations … If an authority holds and processes personal data about stakeholders, clients, employees or suppliers, it is legally obliged to protect that information. Under data protection law an authority must only collect information needed for a specific business purpose, it must keep it secure and ensure it remains relevant and up to date. The authority must also only hold as much information as is needed for business, historical or research purposes and only for as long as is set out on an agreed retention schedule."

9.1 Management of Personal Data

The authority's responsibilities under Data Protection Act 2018 (DP2018) are technology-neutral and, theoretically, this will not change under M365. However, under M365, an authority must pay particular attention to General Data Protection Regulations (GDPR) Principle 5 that data should be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed".

As noted under Element 4 above, the M365-package offers users a wide range of applications where records may be stored. The records manager must be confident that no records are accidentally hidden away, in contravention of principle 5, outside of the main recordkeeping systems. Unfortunately, the M365 cross-application search facility will be of limited use in this scenario.

For this Element, it is recommended that the records manager liaise with the identified Data Protection Officer.

Questions:

(Some of the questions posed under Element 4 will apply under this element)

- Is the authority absolutely clear which applications are actively being used to create records? If not, how can the records manager be provided with reports/alerts that will give them this information?
- Authorities may wish to consider how they assign ownership of records, ensuring that personal data, regardless of which application it is held in, can be managed in line with DPA2018.
- How might an authority control 'data sprawl' (where record around a specific topic or project are scattered across multiple applications)? Could this lead to incomplete record collections in the future where, for example, the authority wishes to refer to past activities, but only the records moved to SharePoint are still locatable?

- How can the authority's Data Protection Officer ensure that documents and records containing personal identifiable information are not retained for longer than is necessary?

- If required, could the organisation easily provide all information requested, held within the M365 platform, under a subject access request? Is the Data Protection Officer confident that appropriate permission controls can be applied to all personal identifiable information held on the platform to ensure access is limited to only those who require it for the purposes of performing their role?

Element 10 - Business continuity and vital records

Record recovery, prioritising vital records, is an integral part of the authority's business continuity planning.

"An authority's business continuity arrangements should include the recovery of records made temporarily unavailable due to an unexpected event. Current data protection law emphasises that the loss of personal data may constitute a breach."

10.1 Back-Up and Recovery

As records created on M365 are not held in an authority's servers, this element may in some cases be significantly improved by the adoption of M365.

There will now be no need to mark certain records as 'vital' or 'priority'. Everything can be returned immediately.

However, it remains important that the records manager understands what is backed up and for how long it remains available. This is important with regard to confidence in what records are 'held' at any particular time.

Question:

- Is the records manager clear about the M365 back-up procedure? For example, Yammer chat (if retention is applied) saves to a back-up in the associated Exchange mailbox. This is explained at Enable archive mailboxes in the Microsoft 365 compliance center - Microsoft 365 Compliance | Microsoft Docs.
- How can the authority ensure continuity of access to records which are stored within the application (as recommended by Microsoft), e.g. Exchange if the account owner/creator of the information is on long term leave?
- Is the 93-day recovery timescale acceptable to the organisation?

Element 11 - Audit trail: Tracking and version control

The location of records is known and changes recorded.

"The Keeper will expect an authority's RMP to provide evidence that the authority maintains a complete and accurate representation of all changes that occur in relation to a particular record. For the purpose of this plan 'changes' can be taken to include movement of a record even if the information content is unaffected. Audit trail information must be kept for at least as long as the record to which it relates. This audit trail can be held separately from or as an integral part of the record. It may be generated automatically, or it may be created manually."

11.1 Versioning

The key to this element is that a record can be located and the correct version identified. The adoption of M365, which has a powerful search functionality, should provide a noticeable improvement in this area.

The Keeper's Model Plan sets out best practice aspirations that, for digital records, version control is in place and that movement and amendment logs are maintained and available. Again, much of this is automated in M365.

However, it is important that the individual identified at Element 2 has the correct 'roles' and permissions to allow these functions to be used to their full potential (see questions under Element 2),

Questions:

- Is the records manager satisfied that the 'audit log' functionality is adequate for their needs? For example, can they use it to track changes to an individual record (rather than just a container)?
- How long will audit log information remain available? Are the timeframes suitable for the needs of the authority?

11.2 Naming Conventions

As noted above, the M365 search facility is powerful and can search for particular record titles across SharePoint, Teams, Exchange, Sway, Yammer etc. However, for it to work in the way M365 expects, staff will need to name records correctly. The system does not expect a user to rely on simply opening a 'folder' and scanning what is in there. Previously, as long as it was held in the correct folder, a records manager may have been able to discover a record even if it has been misnamed or suffered from a typo in the document title. Now there is a reliance on M365 to find the relevant material which might be held in various locations throughout the system. M365 will need to be able to recognise it, and so record-creators must name correctly.

Questions:

- Has the records manager been able to influence the metadata collected when documents and records are saved into SharePoint?
- Does the authority operate robust naming convention guidance? Is the records manager convinced that record creators are using it?
- Is there a process by which the records manager or local records management 'champions' routinely check this?
- Can M365 reports help with this and, if so, does the records manager have routine access to the appropriate reports?

11.3 Microsoft AI and Intelligent Applications

Microsoft is currently developing an Artificial Intelligence (AI) functionality which, in theory, may alleviate some of the risks of misnaming. It may be possible in the future to locate records by subject rather than title (i.e. M365 will learn to 'understand' what a record is about). However, this is not yet functional. It will almost certainly take time to bed-in to an authority's system while it learns and will, one imagines, initially be subject to false negatives and positives. It may also come at a premium cost.

Most Records Management Policies, seen by the Keeper as evidence under PRSA, make reference to the importance of authenticity. This means that any changes to a record should be obvious. In SharePoint editing is recorded, but this may not apply to other M365 systems. For example, if someone says something in a Teams chat they can go back and edit or delete it later. This may make authenticity a problem.

Questions:

- Is the authority clear what changes are actually recorded in each application that is being used?
- Is it clear who in the authority can access the version history of a record? Is this functionality properly enabled?

Element 12 - Records management training for staff

Staff creating, or otherwise processing records, are appropriately trained and supported.

"The Keeper will expect an authority's RMP to detail how the day-to-day operation of activities described in the elements in the authority's RMP are explained to the staff who will be required to carry them out. It is important that authorities recognise that records management processes are likely to be implemented by staff in various roles and business areas out-with the immediate information governance officers. These staff members must be trained and supported accordingly."

Obviously, all record creators will need training on M365. The records managers will have to receive much more in-depth training, as they must be aware of how records are managed in all the apps used in the organisation (see Element 2 above). The extent and depth of the training required will be determined by the complexity of the software package used. The risks of accidental mismanagement or deletion of information, for example, can be significantly mitigated by ensuring that all staff (who are likely to be record creators) regularly undertake training on the records management system used, naming conventions and responsible disposal, and that key staff members responsible for records management receive more in-depth guidance.

Furthermore, as the suite of applications and their individual functionality may change over time, there should be a formal procedure to ensure that staff using these applications are kept informed of any changes when it is likely that they will have a significant effect. It is probably not a good idea to alert staff to every technical behind-the-scenes tweak, as this may result in information overload – it is not necessary for non-IT staff to divert their attention away from their day jobs to become M365 experts. However, an authority's records manager should be knowledgeable about how M365 works, and should be routinely alerted to changes within the system.

Questions:

- Has the person named at Element 2, responsible for day-to-day records management for the authority, been adequately trained?
- Is M365 training in place, and is it mandatory for all record creators?
- Does the authority have somebody at Microsoft available for advice (even for a limited period after roll-out)?
- Is there a process by which staff are alerted to changes to the system (as M365 is developing constantly)? This will need to be kept limited or it may become overwhelming.

Element 13 - Assessment and review

Records Management arrangements are regularly and systematically reviewed with actions taken when required.

"*Section 1(5)(i)(a) of the Act says that an authority must keep its RMP under review. An authority's RMP must describe the procedures in place to regularly review it in the future. It is important that an authority's RMP is regularly reviewed to ensure that it remains fit for purpose. It is therefore vital that a mechanism exists for this to happen automatically as part of an authority's internal records management processes.*"

M365 provides reports on system usage. The reports should be added to the pre-existing review procedures agreed by the Keeper under an authority's agreed Records Management Plan.

As discussed above (see Element 4), it is important that the records manager can access all the reports necessary in order to be satisfied that the system is working as expected. The constant development of the M365-package will make a routine review of the system more pressing. In some cases, changes will be directed through the authority's IT professionals who will have to make internal adjustments. Where these changes impact on records management, the records manager should be involved. Alternatively, there may be software updates made by Microsoft directly. It is important that there is a process in place for alerting the records manager to these, too.

Question:

- Does the authority have a formal process whereby changes to the M365 system, where it affects records management, are notified to the records manager?
- Are records managers consulted on the changes? Are they part of the decision-making process where there is a requirement for decisions?
- As with Element 2 above, is the records manager properly consulted about potential changes that may have an impact on the records management provision within the authority?

As well as changes applied to the system by the constantly developing M365-package, it is possible that, once carried out, a review might itself highlight where tweaks may be required to keep the authority's records management provision compliant with the Act.

Question:

- How does the records manager request changes to the system? Can they make changes themselves? Is there an established internal process for doing this?

As with any records management system it is important that procedures are in place to monitor whether policies and guidance are being followed.

Questions:

- What M365 reports are automatically generated, and are these being appropriately shared with the records manager?
- Are there other useful reports that can be requested? How does the records manager request these reports?
- Does the M365 licence allocated to the records manager adequately allow them to assess whether the policies and instructions they have issued are being followed? How can misuse by users be flagged up by the system?

Element 14 - Shared Information

Information sharing, both within the Authority and with other bodies or individuals, is necessary, lawful and controlled.

"The Keeper will expect an authority's RMP to reflect its procedures for sharing information. Authorities who share, or are planning to share, information must provide evidence that they have considered the implications of information sharing on good records management. An authority's arrangements must, for example, take data protection into account and demonstrate robust arrangements for the safe and secure sharing of personal sensitive data."

The requirement to consider records management and data protection when creating information-sharing agreements does not change with M365.

However, M365 has tools that may enhance and support an authority's information sharing processes.

Questions:

- What guest access control have been put in place?
- Has external sharing been turned on or off?
- What controls have been put in place with the implementation of sensitivity labels?

Element 15 - Public records created or held by third parties

Adequate arrangements must be in place for the management of records created and held by third parties who carry out any functions of the authority.

"Section 3 of the Act describes the meaning of 'public records' for the purposes of the Act. It says that public records in relation to a named authority means records created by or on behalf of the authority in carrying out its functions. This is extended to records created by or on behalf of a contractor carrying out the authority's functions and includes records that have come into the possession of the authority or contractor in carrying out the authority's functions … An authority's plan must include reference as to what public records are being created and held by a third party carrying out a function of the authority and how these are being managed to the satisfaction of the authority."

The requirement to ensure that third parties, undertaking contracted functions of an authority, have adequate records management provision in place to manage the resulting public records does not change under M365.