Office 365 Policy:
Online collaboration, communication and document storage

July 2020

Approving authority:	University Executive
Consultation via:	Professional Services Leadership Board, Global Information Governance and Data Protection Group, Enhancing Online Collaboration Project Board
Approval date:	7 July 2020
Effective date:	7 July 2020
Review period:	Five years from date of approval or more frequently if required
Responsible Executive:	Secretary of the University
Responsible Office:	Information Governance, Information Services
Territorial Scope	University Group, Global

HERIOT-WATT UNIVERSITY
OFFICE 365 POLICY
CONTENTS

1. INTRODUCTION

Following the introduction of the Microsoft Office 365 environment, this policy sets out a framework of governance, accountability and responsibilities for managing Intranet Hub sites, online Workspaces, Teams and OneDrive across the University Group. It replaces the Intranet Policy.

Heriot-Watt University relies on the effective management and flow of information to enable staff to communicate and work effectively on its business worldwide. This policy supports the University's Strategy 2025 to be "a global, connected University" and the University's values through:

- Intranet Hub sites that build "an organisational culture which reinforces our global, connected identity" and disseminate information that supports colleagues to "belong to a diverse, inclusive and international community working together across boundaries and cultures"
- Online Workspaces and Teams that support the "establish[ment of] wider shared working" and that allow colleagues to "collaborate by working in partnership"
- An information management framework for information contained in the Office 365 environment that represents "One Heriot-Watt Way of Doing Things"

This policy recognises that the Microsoft Office 365 environment is a rapidly evolving and complex technological environment with the need for clear and sustainable framework of responsibilities and rules to make the most effective use of this powerful software while managing information risks.

POLICY STATEMENT

2. PURPOSE

This policy sets out the governance framework to help the University to:

- Maximise the benefits of the Office 365 environment, in particular Teams, Hubs and Workspaces (SharePoint), OneDrive and Outlook
- Manage the legal, compliance and reputational risks
- Create and manage effective documents and records necessary for business, regulatory, legal and accountability purposes
- Create and manage an effective Intranet which provides high quality, relevant, accurate and up-to-date information from every school and professional service of the University, to support University business in line with Strategy 2025

3. OBJECTIVES

3.1 All Office 365 users will:

- Communicate with clarity, professionalism, courtesy and respect, remembering the University's values and that all information recorded in Office 365 (including chats, recordings, documents, emails, emojis and gifs) is legally discoverable and may need to be disclosed under freedom of information or data protection law or in court
- Only create information, including chats and meeting recordings, where there is a legal basis and business need to do so. The creation of unnecessary information is a waste of resources and presents a compliance risk
- Use their Workspace Zone as the document storage area for work documents to ensure that it contains the 'single point of truth', with the exception of work documents that are held in line of business systems (e.g. Banner) and personal work records that are more appropriately held in OneDrive
- Apply good information management principles by:
    - Using naming conventions and version control
    - Following business rules on what to file, where and with the correct labels

  To ensure that in their absence, other colleagues with a business or legal need to do so can readily find the right information
- Regularly delete content that no longer needs to be kept from their OneDrive and Outlook
- Respect Workspace access permissions and not give access to any part of the Workspace (e.g. documents, folders or libraries) to any other user without first agreeing it with the Activity Manager
- Undertake training and awareness activities provided by the University to support compliance with this policy, and apply what they have learned

3.2 Each School and Professional Service will have a Hub site provisioned by Information Services to enable internal communications.

The Intranet of Hub sites:

- Assist staff to become better informed of what is happening within the University and what each school and professional service is doing through the provision of one central point for the dissemination and sharing of key information and key documents throughout the University in a co-ordinated approach. Thus, enhancing communication and effectiveness along with coherence and co-operation throughout the University
- Provide consistency of quality and content across sites and managed creation and use of sites and subsites through an agreed site approval process and common templates and conventions
- Support staff to maintain posted information through devolution of content management to Activity Managers and authors to ensure that information is kept current and up to date.

POLICY

Any records posted through Hubs and Hub Zones will be reference copies of records whose lead copy (and 'single point of truth') is captured in the appropriate Workspace.

Hubs and Hub Zones will not be used to post information intended for both internal and external audiences. This information will be published on the University's external website. The University has a legal obligation to publish certain types of information on its external website, for example information about income, expenditure, services, strategy, performance, standards, policies, environmental information etc. Moreover, each school and professional service has its own external stakeholder audiences. To avoid duplication of content, Hubs and Hub Zones will link to the external website where appropriate.

If there is a requirement for a new Hub or Hub Zone, the Activity Manager will follow the procedure to request it.

3.3 Each school and professional service will have a Workspace site provisioned by Information Services to support the objectives of the Information Governance and Records Management Policy by providing an electronic document and record repository to act as the 'single point of truth' for core business activities that do not have a dedicated line of business solution (e.g. Banner).

Each Workspace is set up to support schools and professional services to manage their information so that it is:

- Fit-for-purpose and achieves the University's mission and objectives (Effective)
- Protected from unauthorised access and disclosure (Confidentiality)
- Deleted or transferred to the University Archive at the end of its lifecycle (Lifecycle)
- Available to authorised individuals timeously whenever and wherever required (Availability)
- Reliable, authentic, accurate, complete and protected from unauthorised amendment or deletion (Integrity)
- Resistant to the impact of incidents that would otherwise have serious adverse impact on its confidentiality, integrity or availability (Resilient)

When deciding where to capture content, the default will normally be the relevant Workspace or Workspace Zone.

If there is a requirement for a new Workspace or Workspace Zone, the Activity Manager will follow the procedure to request it.

3.4 Where there is a business need for colleagues from different schools and professional services to collaborate, co-edit files, chat and video meet in relation to cross-functional, short lifecycle activities, the lead school or professional service will create a Teams site and invite

POLICY

collaborators to join. Example use cases include: Policy and procedure development, working groups, setting up an event, project boards, consultation groups.

Teams sites enable colleagues to:

- Securely share confidential information on a need to know basis
- Collaborate on document creation and engagement with internal closed member groups and guests

Business as usual activities must be conducted on Workspaces.

Teams sites that are inactive for 30 days will automatically be made read-only and the site Owners will receive a notification asking them to either:

- Provide a justification for the site's continued activity, or
- Move content that needs to be retained to the Activity Manager's Workspace and delete the Team

At six months from creation, Team sites will automatically be made read-only and the site Owners will receive a notification asking them to either:

- Provide a justification for the site's continued activity, or
- Move content that needs to be retained to the Activity Manager's Workspace and delete the Team

If a Teams site's Owners take no action following the notification and reminders, the Teams site will remain read-only until it is 12 months old, at which point it will be assessed by the Teams and Workspaces Management Group.

All Teams sites (both active and read-only) more than 12 months old will be assessed by the Activity Managers for the relevant school or professional service and a report made to the Teams and Workspaces Management Group. Active sites will be assessed to determine if there is an ongoing need for the site, and how that need should be met, for example by the creation of a new Workspace Zone. Read-only sites will be reviewed to determine whether any of the content needs to be kept and if so the most appropriate location to move it to. In each case the Teams site will be deleted after content that needs to be retained has been moved.

4. SCOPE

4.1 What is included in the Policy

This policy applies to all information recorded in Heriot-Watt University Office 365 accounts (including, but not limited to chats, recordings, files, folders, documents, emails, and gifs) created or received in the course of University business, of any age.

4.2 Who is affected by the Policy

The policy applies to:

POLICY

- all colleagues and other people contracted to work for or on behalf of organisations within the University Group, including members of the governing body
- postgraduate research students
- anyone else given access to the University Hubs, online Workspaces and Teams sites, including external collaborators, guests and visitors

4.3 Where the Policy Framework applies

The policy applies to all locations from which users access Heriot-Watt University Office 365 accounts.

As the University Group operates internationally, through its campuses in Dubai and in Malaysia and through arrangements with partners in other jurisdictions the remit of the policy shall include such overseas campuses and international activities and shall pay due regard to non UK legislation that might be applicable.

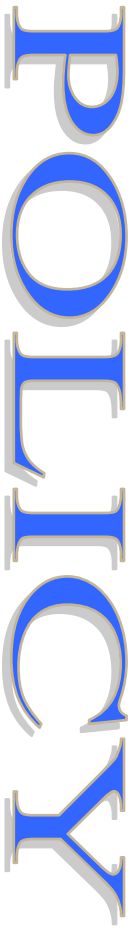
5. LINES OF RESPONSIBILITY

5.1 All users of Office 365 are responsible for:

- Undertaking relevant training and awareness activities provided by the University to support compliance with this policy
- Following the Information Governance and Records Management Policy, procedures, guidelines and training to:
  - Maintain effective records in line with their roles and responsibilities
  - Capture information in the correct place and label it correctly
- Following Information Security Policy, procedures and training, especially when sharing information and synchronising information on unmanaged devices
- Making change requests through the relevant Activity Manager

5.2 Activity Managers are responsible for:

- Fulfilling the site 'Owner' role for the sites covered by their area of activity
- Managing the access permissions for their sites. This includes:
  - Keeping the site membership up-to-date so that access is removed when colleagues move roles or leave
  - Monitoring the use of granular access permissions and removing such permissions as soon as they are no longer needed
- Maintaining the file plan and monitoring its usage to ensure information is captured in the correct place and labelled correctly so that information is easily retrievable by authorised individuals and it can be deleted at the end of its retention period
- Where necessary, providing training and guidance to members of their site to support them to use the site appropriately. For



example, providing business rules concerning what to file, where, and how to label it with appropriate metadata
- Identifying records with digital preservation requirements and taking action to protect them
- Identifying vital records and taking action to protect them, for example from accidental amendment or deletion
- Liaising with colleagues responsible for web content management to ensure that information that needs to be publicly available is published on the external website, rather than the Intranet
- Reviewing and supporting requests for the provisioning of new Zones within their area of responsibility
- Referring change requests jointly to Information Services and Information Governance, including requests for new Hub and Workspace Zones
- Liaising with their head of school, directoriate or division as necessary and appropriate to ensure the objectives of this policy are met

5.3 **The Secretary of the University** has senior management accountability for information governance, reporting to the University Executive and the Risk and Audit Committee on relevant risks and issues.

5.4 **The Global Director of Governance and Legal Services** has senior management responsibility for information governance and for providing proactive leadership to instil a culture of information governance within the University through clear direction, demonstrated commitment, explicit assignment and acknowledgement of information governance responsibilities.

5.5 **The Head of Information Governance** is responsible for recommending information governance strategy and policies to the Global Director of Governance and Legal Services, leading the information governance programme, promoting good practice, monitoring compliance and recommending revisions to these policies in line with business need, legal requirements and professional standards.

5.6 **Information Governance** is responsible for:
- Recommending information governance policies and procedures.
- Oversight of site governance. In particular: file plans and metadata; information lifecycle management; security and access permissions
- Establishing the security and compliance framework and providing oversight
- Providing information governance training, awareness and guidance
- Advising on external publication requirements
- Working jointly with Information Services to maintain the Office 365 information governance framework, including a programme of auditing and review
- Developing and maintaining a network of Activity Managers

POLICY

- Coordinating an annual review of the Records of Processing Activities by Activity Managers
- Monitoring the accessibility of information that needs to be published externally

5.7 **The Global Director of Information Services** is responsible for the management and delivery of centrally managed IT systems and services across all University campuses and for maintaining the infrastructure and security of the Office 365 environment and its applications.

5.8 **Information Services** is responsible for**:**

- Provisioning Hubs and Workspaces
- Developing and maintaining the IT infrastructure on which the Office 365 environment runs
- Providing IT training
- Delivering audits and reports on usage at the direction of Information Governance
- Working jointly with Information Governance on:
    - Authorising applications to run on Office 365
    - Establishing the security and compliance framework
    - A programme of auditing and review

5.9 **Heads of schools, directorates and divisions** are accountable for the use of Hubs, Workspaces, Zones and Teams by Office 365 users within their area of responsibility, and are responsible for:

- The appointment of Activity Manager(s) for their areas of responsibility
- Being or appointing a backup Owner for each Hub, Workspace, Zone and Teams site within their area of responsibility
- Monitoring the creation and use of Teams sites within their area of responsibility to ensure compliance with this policy

5.10 **The Global Information Governance and Data Protection Group (GIGDPG)** is responsible for:

- Maintaining governance oversight of the University's use of Office 365
- Monitoring compliance with this policy
- Receiving reports from the Teams and Workspaces Management Group
- Endorsing actions recommended by the Teams and Workspaces Management Group
- Reviewing the procedures and guidelines developed to support this policy

5.11 **The Change Advisory Board (CAB)** is responsible for:

- Reviewing and approving changes to the University's IT infrastructure, including Office 365
- Advising and planning the technical delivery of the change

5.12 **Teams and Workspaces Management Group** is responsible for:

POLICY

- Keeping this policy under review and recommending changes to GIGDPG
- Receiving audit and monitoring reports and advising GIGDPG on the action the University should take in response
- Reporting on compliance with this policy and making recommendations for action to GIGDPG
- Monitoring changes to the Office 365 environment and advising the CAB what action the University should take in response
- Considering and recommending change requests to the CAB
- Maintaining oversight and direction of Activity Managers particularly in relation to monitoring Teams sites and reviewing their retention and disposal

The Group's membership will include the University Records Manager, Webmaster and representative Activity Managers and Office 365 users, as set out in the terms of reference for the Group.

6. MONITORING AND EVALUATION

6.1 The University Webmaster will monitor all school and service Intranet Hub sites and raise any issues with the relevant areas. A quarterly report will be presented to GIGDPG and the Professional Services Leadership Board advising of any issues that may have arisen during the monitoring period. It is the overall responsibility of each site Owner to ensure that Hub content is current and up-to-date and in line with University procedures.

6.2 The Records Manager and Webmaster will have joint oversight of how the Workspace, Teams and OneDrive sites are being used. They will develop a programme of auditing and review in consultation with Activity Managers and report to Teams and Workspaces Management Group and then GIGDPG with recommendations for appropriate actions.

6.3 The Records Manager will agree and monitor the implementation of records retention, transfer and disposal schedules so that each school and professional service retains records on their Workspaces only as long as needed. The Records Manager will implement information disposition through the Office 365 Security & Compliance Centre based on the University's agreed retention schedules and the retention information assigned to documents by Office 365 users.

6.4 Information Governance will develop and maintain a network of Activity Managers as a sub-section of the information governance coordinator network. The network will:

- Act as a forum to identify training and support needs
- Recommend changes and improvements
- Provide representatives to join the Teams and Workspaces Management Group

POLICY

6.5 Information Governance will coordinate an annual review of the Records of Processing Activities by Activity Managers.

6.6 The Information Governance Officer will monitor the accessibility of information that needs to be published externally and liaise with the Activity Managers and Webmaster to maintain external web links to relevant information and documents. The Information Governance Officer will report any ongoing issues relating to accessibility to the Head of Information Governance and the GIGDPG. The Head of Information Governance will report to GIGDPG on any issues relating to the security classification of information held or published on the Intranet or external website.

6.7 Members of the Teams and Workspaces Management Group, particularly the Webmaster and Records Manager, will monitor and keep up to date with changes being made by Microsoft to the Office 365 environment to ensure the University continues to maximise the benefits of the Office 365 environment while also managing legal, compliance and reputational risks.

7. IMPLEMENTATION

This policy is implemented through:

- The development, implementation, monitoring and review of procedures, training and guidance for Activity Managers and Office 365 users, that will cover each phase of the information lifecycle
- The network of Activity Managers
- The Teams and Workspaces Management Group

8. RELATED POLICIES, PROCEDURES AND FURTHER REFERENCE

8.1. University Policies and procedures

This policy forms part of an interconnected set of **University Information Governance and IT Policies** and procedures. These aim to develop a positive culture of information governance throughout the University.

8.2 Legal Requirements and external standards

Effective information governance is essential for compliance with U.K. and Scottish law and other relevant law in all jurisdictions in which the University operates.

Legislation that places specific information security and record keeping obligations on organisations includes, but is not limited to:

Computer Misuse Act 1990
Data Protection Act 2018
European Union General Data Protection Regulation (GDPR)
Environmental Information (Scotland) Regulations 2004

POLICY

Freedom of Information (Scotland) Act 2002
Privacy and Electronic Communications Regulations 2003
Regulation of Investigatory Powers Act 2000
Regulation of Investigatory Powers (Scotland) Act 2000
Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

All current UK Legislation is published at https://www.legislation.gov.uk/

9. DEFINITIONS

Office 365 users	Any individual who has access to and uses the Heriot-Watt University Office 365 environment. This includes all University staff and postgraduate students, as well as anyone granted visitor or guest access.
Hub sites and Zones	An area where staff and postgraduate students can easily access information posted by a school or professional service. Hubs comprise the University Intranet. Each Hub may have multiple 'Zone' sub-sites for distinct areas of activity. Information posted on Hubs and Hub Zones is available to all University staff and postgraduate students. Hubs are created and managed using Microsoft SharePoint. Each Hub and Zone sub-site must have at least one site Owner. The information architecture is described in Appendix 1.
Workspaces and Zones	An area where colleagues in a particular school or professional service can work together as a group to create, edit, review and manage information. Each Workspace may have multiple 'Zone' sub-sites for distinct areas of activity. Information in Workspaces is only available to members of the relevant

POLICY

	school or professional service. Information in Workspace Zones is only available to members of the relevant institute or division. Workspaces hold the “single point of truth” for core business activities that do not have a dedicated line of business solution (e.g. Banner). Workspaces are created and managed using Microsoft SharePoint. Workspaces may also be Teams site. Workspaces replace S: drives. Each Workspace and Zone must have at least one Site Owner. The information architecture is described in Appendix 1.
Teams site	A short-life area where colleagues from different schools and professional services can collaborate, co-edit files, chat and video meet in relation to: • Cross-functional activities which are considered non-core e.g. Working group • Ad-hoc, short lifecycle activities e.g. Setting up an event Teams sites are created and managed using Microsoft Teams. Each Teams site must have at least one Site Owner.
OneDrive	A document storage area provided for each Office 365 user using Microsoft OneDrive. The place to keep personal records, e.g.: • Professional development notes and records • Work planning notes and documents • Personal copy of PDR documentation • Personal reference material

- Notes of meetings with line manager or supervisor

By default, information on OneDrive is only available to the individual Office 365 user. Users can give others access to specific documents or folders on their OneDrive.

OneDrive replaces H: drives.

Site Owner

Any individual who is designated as having the 'Owner' role for a particular Hub, Workspace or Zone. Site Owner privileges are determined by the Office 365 environment. Site Owners have control over the particular site. For example, they are able to amend site wide access permissions.

A site Owner may be the owner of a particular Zone sub-site or for a Hub or Workspace site and all Zone sub-stes for that Hub or Workspace.

The site Owner role must be given to both:

- The Activity Manager responsible for the site, and
- The head of school, directorate or division responsible for the site

Activity Manager

The individual designated by their head of school, directorate or division to manage a Hub, Workspace or Zone. Activity Managers must be designated as one of the site Owners for each of the sites for which they are responsible.

An Activity Manager may be the information governance coordinator for a school or service (as described by the Information Governance and Records Management Policy).

Activity Managers of Hubs and Workspaces should have oversight of the Zone sub-sites within their Hub or Workspace while also taking into account the Information Security Policy principle of "need to see".

POLICY

Information

The definition of information includes, but is not confined to, paper and electronic documents and records, email, voicemail, still and moving images and sound recordings, the spoken word, data stored on computers or tapes, transmitted across networks, printed out or written on paper, carried on portable devices, sent by post, courier or fax, posted onto intranet or internet sites or communicated using social media.

Confidential Information

The definition of confidential information can be summarised as:

- Any personal information that would cause damage or distress to individuals if disclosed without their consent.
- Any other Information that would prejudice the University's or another party's interests if it were disclosed without authorisation.

A more detailed definition can be found in the University Information Security Classification Scheme.

Information lifecycle

Information can be described as having a lifecycle comprising three stages:

Active: Planning for the creation of the records, creating records, capturing and organising records, using and maintaining records (which may include distribution).

Semi-active: The records are no longer in active day-to-day use, but are occasionally referred to for business, legal or regulatory purposes.

Inactive: The records are no longer needed for business, legal or regulatory purposes. They have reached the end of their retention period, as expressed in the University's retention schedules. At this point records with archival value should be transferred to the Heriot-Watt University Museum and Archive where they will have an afterlife. All other records must be securely deleted or destroyed.

POLICY

Vital records	Recorded information which enables a school or professional service to perform its core function or provide evidence that it has performed its function. Vital records are those which are crucial to the conduct of the University's business, without which the University could not continue to operate. Examples of vital records include: • Student records • Contracts • Insurance records • Building plans • Research records and data
Records of Processing Activities	Detailed records of the personal data processing activities that a Data Controller or Processor is required to maintain and make available under the GDPR.

10. FURTHER HELP AND ADVICE

For further information and advice about this policy contact:
Information Governance
Telephone: 0131 451 3216/3274/3219
Email: Infogov@hw.ac.uk

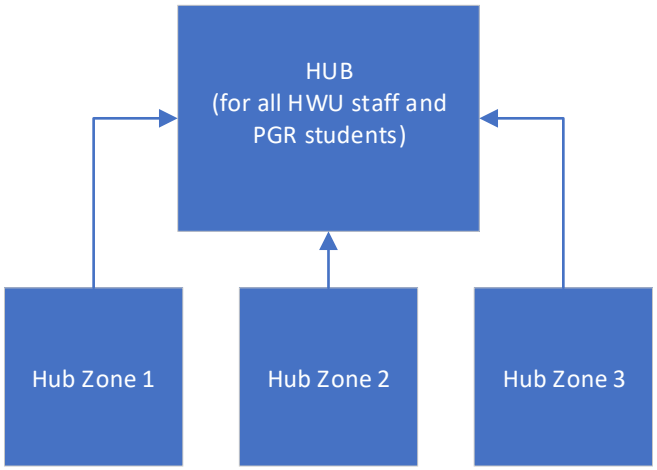
Information Services
Email: ISHelp@hw.ac.uk

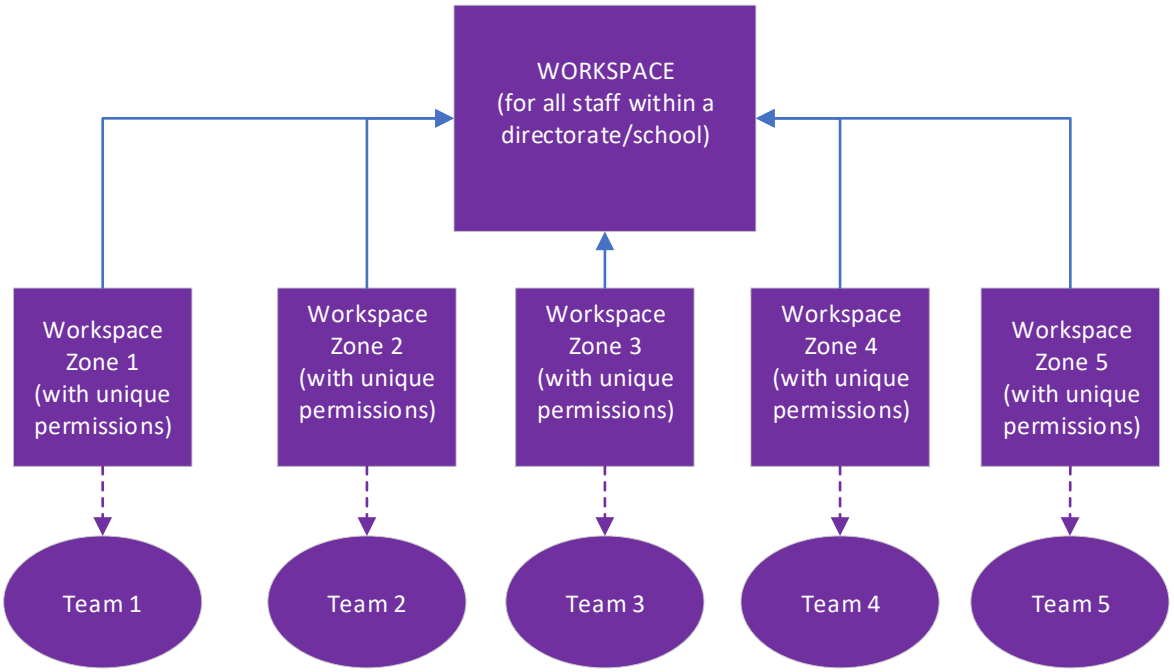
11. POLICY VERSION AND HISTORY

Version No	Date of Approval	Approving Authority	Brief Description of Amendment
V1.1 17 June 2020	7 July 2020	University Executive	Draft for consideration following input from EOC project
V2.1 18 June 2020			Draft presented to GIGDPG for endorsement
V2.2 24 June 2020			Draft containing amendments discussed by GIGDPG

POLICY

Appendix 1: Office 365 Information Architecture





POLICY