Mural Acceptable Use Policy 1.2

23 April 2021

Introduction

This policy tells you how you must use Mural, a cloud browser-based tool for visual collaboration. This tool is provided for usage by Home Office staff, selected suppliers who provide services to Home Office and specific third parties for collaboration purposes.

This agreement is designed to work alongside existing Home Office (HO) policies and does not replace them.

By using and accessing this application, you are indicating your acceptance of the terms laid out below.

Breaches of this policy will be investigated and, if necessary, remedial or disciplinary action taken.

Any queries with this Policy should be raised with Chris Taylor by email at chris.taylor@digital.homeoffice.gov.uk.

1.1 Scope of Mural

Mural is a cloud, browser-based tool for visual collaboration.

It provides shared, virtual boards where teams can work together in real-time to perform many of the activities that they typically would do in person including, but not limited to:

- Post-it note sorting activities from user research sessions
- Collaborative mapping exercises such as journey mapping or business process diagrams
- Facilitating workshops
- Agile ceremonies including retros and sprint planning

You must sign up for Mural (after receiving an invite) using an approved gov.uk email address when conducting business for the HO. A gov.uk email address can be used to send and receive OFFICIAL information. This includes anything marked OFFICIAL-SENSITIVE with the appropriate handling instructions.

Personal email addresses must not be used for work.

"Supplier" email addresses should only be used where your organisation has a prior agreement with the HO.

1.2 Who this policy applies to

This policy applies to anyone using the Home Office Mural instance including the following:

- Civil Servants
- Contractors
- Employees of Suppliers

1.3 User Access & Security Clearances

Access to Mural is controlled by username and password. User accounts are assigned to named individuals who are accountable for all actions taken on that account, including data that is accessed.

Mural has several types of user account:

- Workspace admins manage the workspace.
- Company admins manage company-wide settings.
- Members are core team members or facilitators that have full collaboration access.
- Guests are external stakeholders, partners, and clients outside of your company's domain. They have slightly restricted access.
- Visitors are one-time collaborators with restricted access. If enabled, visitors will also be able to collaborate anonymously in a mural without an account via the visitor share link.

More information can be found on Murals help pages:
https://support.mural.co/en/articles/2113719-types-of-users-in-mural

Mural users must be cleared to the level of CTC or agreed equivalent before they are issued with a Mural account. Exceptions to this must be approved and provided in writing to the relevant Information Asset Owner or Senior Responsible Officer for that projects data.

By inviting guest or visitors to a Mural room or board you must be sure that they are authorised and appropriate to view that boards information and collaborate on that board.

Where there is no longer a business need for an individual to have access to Mural, access should be removed, following your business areas joiners, movers and leavers policy.

User accounts that are not regularly using the service will be disabled.

1.4 Misuse of the service

You must not misuse Mural. "Misuse" including but not limited to:

- any activity that is illegal under national or international law
- download or export of HO information from Mural to unassured or unauthorised devices
- introducing malicious programmes or codes
- allowing your account to be used by others
- inviting or in any way allowing unauthorised users access to Mural
- using other people's accounts or passwords
- monitoring or intercepting the files or electronic communications of other employees or third parties
- hacking or obtaining access to systems or accounts you're not authorised to use
- sending email or other electronic communications in a way that attempts to hide the identity of the sender, or represent the sender as someone else i.e. spoofing
- moving or storing inappropriate HO information on Mural, or uploading documents that are not Official
- Inappropriate usage of messaging and chat functionality
- Uploading personally identifying information
- copying, retrieving, modifying or forwarding copyrighted materials, unless allowed by the copyright owner
- anything inflammatory, sexually explicit, sexist, racist, homophobic, religiously offensive or which amounts to harassment.

1.5 Guidance on the type of information that is suitable to be hosted on Mural

There are greater security risks associated with SaaS (Software as a Service) tools than those that run locally on an approved Home Office device. This guidance is aimed at SAAS products but you should also refer to it when using locally installed

tools.

When using tools to create Home Office design assets, consider what the impact would be if this fell into unauthorised hands. How might it be misinterpreted or exploited? What might the repercussions be for the Home Office and for you? Use the following principles.

1. Do not use real department data within these services.
2. Do not use politically sensitive phrases or material.
3. Make it clear that any prototypes or mock-ups you create with the tool are marked as such - not to be confused with real or official services.
4. Make sure that names and addresses cannot be mistaken for real people or places.
5. Make plans to delete boards and associated data, when no longer needed.
6. Only give authorised personnel access control to source material.
7. When presenting or demoing work online, make sure you have access control or a method of identifying who is attending. If you think someone's there that shouldn't be, don't continue.
8. Make sure that strong passwords are used: minimum of 12 characters made up of letters, numbers and characters.
9. If possible, enable multi-factor authentication.
10. If in doubt, ask for guidance from your local security team or Home Office Cyber Secuirty

2 Working with Mural

2.1 Wi-Fi networks, VPNs and access abroad

You should avoid using public Wi-Fi for accessing Mural. If you must use public Wi-Fi, then make sure it's from a reputable provider and requires authentication.

A Virtual Private Network (VPN) connection can be used provided it's UK/Ireland based.

2.2 File storage and sharing

Documents and information worked on within Mural will be classed as OFFICIAL.

You're responsible for ensuring that any information you upload or share has the correct access permissions.

You must:

- make an informed decision on what to share and the editing rights you set
- not share information with anyone who doesn't need to know it
- only share data with named users
- consider using links that expire after a period of time.

2.3 Laptops and IT equipment accessing Mural

Devices you use to access Mural must be appropriately secure to work with OFFICIAL data.

This must include a minimum number of security controls such as:

- The device must have full disk encryption enabled
- The device must require a password to logon
- User accounts on the device must be unique and attributable to a specific individual
- The device must have antivirus/malware protection
- The device must be patched
- The device must have a firewall

It is YOUR responsibility to ensure that your device meets these criteria and your device may be audited, without prior notice to ensure it complies.

For more information on device security see: https://www.ncsc.gov.uk/guidance/end-user-devices-security-guidance-introduction-0

If you send your company device for repair, you must ensure that HO data and/or Mural credentials can't be accessed by third parties. Make sure any data has been uploaded to O365 and data/credentials have been deleted from the device.

When you stop working for the HO you must remove all HO owned information from the company owned device, and your company must provide written confirmation of this to the hiring manager.

2.4 Safeguarding your account

- Your Mural account must only be used by you, and you're responsible for all actions performed using your account
- You must not share your account credentials
- Never re-use your HO passwords on external systems
- If your Mural account password is compromised in any way, you must immediately change it
- You may use reputable password management software like KeePass to store your Mural passwords.

2.5 Useful Contacts

HO Cyber Security Team
Email: HOcybersecurity@homeoffice.gov.uk

Data Protection Office
Email: dpo@homeoffice.gov.uk

CSOC Incidents
Email: CSOC@homeoffice.gov.uk

HO Security Team
Email: ContactUs@cluster2security.gov.uk

The ITnow Service Desk
Telephone: 08450 000 050
Email: ITnowServiceDesk@homeoffice.gov.uk Online: https://lssiprod.service-now.com/ess

Version control

Date	Version	By who	Changes
26/03/2021	1.0	Karwai Pun, Chris Taylor	Initial draft
12/04/2021	1.1	Chris Taylor	Amends following review by HO Cyber Security (Sanjay Gurung)
23/04/2021	1.2	Chris Taylor	Added extra bullet to section 1.4 – not downloading Mural info to unauthorised devices