Line Manager approval

# Line Manager approval

This guidance applies to all staff and contractors who work for the Ministry of Justice (MoJ).

Some MoJ IT Policy documents need you to get a review or approval from a Line Manager or other senior person. Do this before taking an action or working in a particular way.

Examples include:

* [General advice on taking equipment abroad](general-advice-on-taking-equipment-abroad.html).
* [Security Guidance for Using a Personal Device](personal-devices.html).

This guidance describes what you should do. The guidance contains steps to follow for [Line Managers](#steps-to-follow-line-managers), and their [Direct Reports](#steps-to-follow-direct-reports).

## Steps to follow (Line Managers)

Note: If at any time you need help about this process, or the applicable MoJ IT Policies, just ask: [security@digital.justice.gov.uk](mailto:security@digital.justice.gov.uk).

1. Check that your direct report (DR) has said what they want in their request. The request should identify which MoJ IT Policies apply.
2. Check that the request is valid from a business perspective. If not, deny the request ([step 7](#steps-to-follow-line-managers__step7) ).
3. Check that [Acceptable Use](acceptable-use.html) is in the list of applicable policies.
4. Review the requirements or obligations within the MoJ IT Policies that apply to the request.
5. Check that the DR understands and will follow the requirements or obligations. For example, have a discussion with them, or ask them for more information or evidence.
6. If they are able to follow the applicable MoJ IT Policies, send a formal approval to the DR. An email is enough for this.
7. If you don't think they can follow the Policies, or there's a weak business case for the request, refuse it.
8. Keep a copy of your formal reply, in accord with Data Retention requirements.
9. Some MoJ IT Policies need a copy of formal approval for other parties. For example, before your DR travels to some countries on MoJ business, send a copy of your approval to Operational Security: [OperationalSecurityTeam@justice.gov.uk](mailto:OperationalSecurityTeam@justice.gov.uk).

## Steps to follow (Direct Reports)

Note: If at any time you need help about this process, or the applicable MoJ IT Policies, just ask: [security@digital.justice.gov.uk](mailto:security@digital.justice.gov.uk).

1. Check that your business need is valid.
2. Check which MoJ IT Policies apply to your request. Include [Acceptable Use](acceptable-use.html) in the list of applicable policies.
3. Check that you understand the requirements or obligations within those MoJ IT Policies.
4. Prepare evidence to show that you will follow all the requirements or obligations. Check that you have all the required information.
5. Send a formal approval request to the authorities required by the MoJ IT Policies. Ensure that you include:
   * Your request.
   * The business case.
   * The list of applicable MoJ IT Policies.
   * Evidence that you understand and can follow the requirements or obligations.
6. Be ready to have a more detailed discussion about your request, or to supply more information.
7. If you get formal approval, keep a copy, in accord with Data Retention requirements.
8. If your request is denied, check that you understand the reasons. Use this understanding to tackle your business task again, if appropriate.

## Contact details

For any further questions relating to security, contact: [security@digital.justice.gov.uk](mailto:security@digital.justice.gov.uk), or for security advice, contact the Cyber Assistance Team [CyberConsultancy@digital.justice.gov.uk](mailto:CyberConsultancy@digital.justice.gov.uk).

## Feedback

If you have any questions or comments about this guidance, such as suggestions for improvements, please contact: [itpolicycontent@digital.justice.gov.uk](mailto:itpolicycontent@digital.justice.gov.uk).