## Why do we need a removable media policy?

1. GCHQ has a responsibility to manage the use of Removable Media (RM) on its sites and for its business. Where possible users should find an alternative way of storing and transferring data and should treat RM as the last resort. However, in the absence of secure electronic connectivity, RM can be a significant enabler for the business. Nevertheless, its use also brings risk to the business on three principle counts:

- **Risk to technical capability** - if malware were introduced onto one of the department's systems;
- **Risk to information security** - if a leak happened as a result of use or misuse of RM;
- **Risk to reputation** - if an attributable piece of RM were lost offsite and found by an unauthorised person.

2. This policy aims to manage these risks by effectively enabling the business, whilst controlling the use of RM and by keeping the amount of RM in use to a minimum.

## What is the definition of RM?

3. For the purposes of this policy, RM is defined as any readable or writable media that is easily transportable as a discrete item that can be introduced to an Information and Communications Technology (ICT) system to import or export data. The computing technology and other mobile devices that utilise the media are specifically excluded from this policy.

## Who does this policy apply to?

4. This policy applies to everyone operating on GCHQ premises and includes employees, contractors, service providers, military and other integrees and visitors. Users of RM must follow this policy and the associated processes and may be subject to disciplinary measures if they do not comply. You have responsibility for your visitors' actions and must ensure they comply with this policy too.

5. This policy applies to all classifications of data stored on RM.

## Principles

6. There are eight principles which underpin this policy:

- You are personally accountable and responsible for the RM you use;

- You should not use RM unless you have to;
- If you use RM, you should use the minimum amount of data and RM necessary;
- The Information Asset Owners (IAOs) or their nominated approvers will approve individuals' use of RM;
- The IAOs or their nominated approvers will approve the use of RM for specific business purposes only;
- You must only use RM for its approved purpose;
- You must only use GCHQ supplied RM for GCHQ business purposes;
- The Department has a responsibility to manage its RM holdings.

## Roles and responsibilities

### The Information Asset Owners (IAOs) and nominated approvers

7. The IAOs are responsible for managing the risks to information within their MBU or BU on behalf of GCHQ's Information Risk Owners (IROs) and Senior Information Risk Owner (SIRO) and as such have a key role in RM use. They will draw on their understanding of the risks in their area to authorise individuals to use RM and to decide for which business purposes RM can be used within the business unit. They may nominate approvers to carry this out on their behalf.

### Users

8. You must be aware of the risks involved in using RM and your responsibilities for handling it, as set out in this policy, and consider them carefully before deciding to use RM. You must be sure that you have thought about alternative solutions for storing or transferring your data and that you are using RM as a last resort. You must be sure that the business requirement justifies the risks you are taking by using RM. You may only use blank RM obtained from an approved issuer.

9. You must support the Department by ensuring that you and those around you handle RM within corporate processes.

10. If you receive media from other organisations or partners, you must comply with the handling requirements set out in this policy, as well as any further requirements stipulated by the other organisation or partner. You may only seek approval to bring it on site where there is a clear business requirement and where there is no alternative means of transferring the data.

11. Remember that you are personally accountable and responsible for the RM you use and may face disciplinary measures if you do not comply with this policy.

Issuers

12. Only certain roles will be authorised to procure, hold and issue blank RM. In order to ensure that RM is protected from unauthorised use, people in these roles are required to store blank RM securely. The issuers will be vital in enabling the Department to understand its RM holdings and will have responsibility for updating the corporate record when RM is allocated, transferred or destroyed.

[redacted]

18. If you have a requirement to use RM, you must first have approval from the relevant IAO or nominated approver for the specific transaction in question.

Allocation

19. The Department must know how much RM is in use and who is using it. To support this, all RM must be issued via an approved route. All RM will be registered to an individual (not a team or post) when first allocated and will be uniquely identifiable.

Use

20. To safeguard the Department's information, a number of controls have been placed on the use of RM. You are only able to use RM for its specifically approved business purpose and when this is completed, the RM must be returned to the issuer for disposal. RM should not be stockpiled.

21. To reduce the risk of introduction or spread of malware, all RM must be virus-scanned before being used to import or export information to or from GCHQ systems. This includes internal transfers. RM must be scanned each time a transfer occurs, even if this is in quick succession. If you have been supplied with software on an official SAM registered CD or DVD (with a 'CDC' reference number) there is no requirement for you to re-scan this in Gryphon Pearch as the SAM service will have

[redacted]

## Working with other organisations

### Background

25. The aim of the RM policy is to reduce the risks surrounding RM. This can be supported by reducing the amount of RM in use and circulation within GCHQ buildings and the movement of information via RM. This includes the distribution and use of RM by service providers and other organisations. The movement of data between other organisations must where possible be via electronic means.

### Receiving RM from other organisations

26. If RM is received from other organisations when you are offsite and you intend to bring it back into GCHQ buildings, you must have approval in RMT to bring it on-site before you do so. The GCHQ RM registration and management processes, including virus-checking, must also be applied.

27. If you receive unexpected RM via postal or secure courier channels, it needs particularly careful checking before use, but not automatic destruction. If you intend to use the RM on GCHQ systems or retain the RM on GCHQ sites, you must have approval before you use it. Corporate registration and management processes, including virus-checking, must be applied. Any RM received via postal or secure courier channels that is not required for specific business reasons must be destroyed. If you are unsure and need advice on how to handle unsolicited media, contact Sense.

### Other organisations' staff on GCHQ sites

28. Approval must also be sought via the RM tool where staff from other organisations, such as contractors, integrees or secondees, intend to bring information on RM onto or take it off GCHQ sites, even if it is not to be used on GCHQ systems.

29. One-off visitor movements will continue to use existing processes (form FC 300/81b) for obtaining approval to hand carry RM to and from GCHQ sites. If visitors bring RM that is to be retained, the RM must be registered, approved and managed using the corporate RM process.

30. Use of encrypted RM solutions to transfer data to other organisations must be approved by the IAO or their nominated approver and where possible GCHQ corporately available and supported encryption solutions should be used. Consideration must be given to the compatibility and acceptability of the encryption solution at the recipient organisation.

### Disposal

31. The use of RM is authorised for a specific business purpose. When this use has been completed, the RM should be disposed of *by the issuer, not the user*, and not

[redacted]

38. This requirement does not apply to RM that meets all of the following criteria: commercially pressed, read only, bearing any classification and unattributable to GCHQ, eg commercial music CDs or read-only for sale items. However, these items must still be presented if you are stopped for entry and exit searches.

## Personal use of RM

39. Since the risk is assessed to be low, the Department will support the personal use of RM in the following two cases. In these two cases, there is no requirement to record movements on and offsite.

### Commercial music CDs

40. The Department trusts staff to act responsibly. Music CDs are allowed onsite for personal use and there is no requirement to register them or record their movement, provided that they are:

- Commercially-pressed read-only CDs;
- Not introduced into any departmental system;
- Only used in stand-alone devices.

41. Access to CD drives will not be given for personal music use.

### For sale items

42. Commercial read-only media items that are for sale via GCForum are also permitted without the requirement to register the media or record their movement. Any writeable media items are prohibited.

## How will compliance with import / export rules be monitored?

43. If you are stopped for entry and exit searches you must declare any item of RM you are carrying. Security personnel will record details of the items to assist compliance monitoring. These logs will be checked against business use approvals and records of movement in and out. A proportion of personal use music CDs will be subject to retention for detailed analysis.

## Unattributable or covert use of removable media

44. If you have a requirement to procure, handle and move unattributable or covert RM, corporate RM management processes must be used where possible. If they do not meet the business requirements, local RM handling processes must be implemented to identify and control the RM and these will be subject to audit. The relevant IAO must be made aware of any such processes and RM holdings.

45. Individuals who have been granted Security dispensation / or waivers do not need to present RM if the RM movement is covered by the agreed business use.

## Exceptions

46. Where crises or operational necessity require exceptional measures, the SIRO may approve an exception to statements in the RM Policy.

47. All requests for exceptions must be raised with the relevant IAO or their nominated approver for consideration in the first instance. The IAO will take into

[redacted]