**USB Memory Agreement Stick Usage**

1. In support of existing [*HSE I.T. security policies*](https://www.hse.ie/eng/services/publications/pp/ict/) this agreement specifically governs the use of HSE approved USB memory sticks.
2. Only **HSE approved USB memory sticks** which are distributed by the ICT Directorate maybe used to store or transfer HSE data. Existing [*HSE I.T. security*](https://www.hse.ie/eng/services/publications/pp/ict/) [*policies*](http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/) specifically prohibit the storage of HSE data on **unapproved** encrypted / unencrypted USB memory sticks and USB memory sticks which are the personal property of staff and are not owned or leased by the HSE.
3. HSE employees who have been issued with a HSE approved USB memory stick must take all reasonable measures to ensure the memory stick is kept secure at all times and is protected against unauthorised access, damage, loss and theft. Therefore, memory sticks must be (1) kept with you at all time when working off- site and not left unattended (2) locked away securely when not in use and, (3) only accessible by authorised HSE staff and not family members or others.
4. The encryption password used to access the HSE approved USB memory stick must not be **written down** on the memory stick or stored with or near the memory stick.
5. HSE employees must note and accept that should their encryption password be forgotten by them, their HSE approved USB memory stick allows for a new password to be created, but this could involve reformatting the memory stick and thus **a total loss of all data currently stored on the memory stick**. Therefore the HSE approved USB memory stick must not be used to keep data that is not backed up securely and regularly in accordance with existing [*HSE I.T. security*](https://www.hse.ie/eng/services/publications/pp/ict/) [*policies.*](http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/)
6. HSE approved USB memory sticks must only be used on an **exceptional** basis where it is essential to store or temporarily transfer confidential or personal data. They must **not be used for the long term storage of confidential and personal data**, which must where possible be stored on a secure HSE network server.
7. Any confidential and personal data stored on the HSE approved USB memory stick must not be **transferred** to any internal (except a secure HSE network server) or external system in an **unencrypted form**.
8. All confidential and personal data should always be deleted from the HSE approved USB memory stick when it no longer required.
9. The encryption software embedded into the HSE approved USB memory sticks

# must not be tampered with.

1. All HSE approved USB memory sticks and the data they contain remain the property of the HSE. When a HSE employee transfers to another HSE Directorate

/ Service Area or leaves the employment of the HSE, the employee has a responsibility to ensure they relocate or delete any data stored on the HSE approved USB memory stick and return the **empty** USB memory stick to the ICT Directorate for redistribution.

1. In accordance with existing HSE I.T. security policies, HSE approved USB memory sticks must not be used for the creation or transmission of:
   1. Any material prohibited by law;
   2. Threatening, racist, extremist, offensive, pornographic or obscene material;
   3. Material protected as trade secrets or copyrighted.
2. HSE employees must report any loss or theft of their HSE approved USB memory stick immediately to their HSE line manager and the ICT Directorate.
3. The HSE reserves the right to take such action as it deems appropriate against employees who breach the conditions of this agreement. Employees who breach this agreement may have their HSE approved USB memory stick withdrawn, and maybe subject to disciplinary action, including suspension and dismissal as provided for in the HSE disciplinary procedure. The HSE will refer any use of the USB memory stick for illegal activities to the appropriate law enforcement agencies.

# Employee Statement and User Declaration

# Please use Microsoft Word to complete the required details in the ‘grey boxes’. Press tab key to move to each box or ‘click in’ using your mouse and complete

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| \*I fully accept and understand my obligations under the existing [*HSE I.T. security*](https://www.hse.ie/eng/services/publications/pp/ict/) [*policies*](http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/) and this Agreement and I agree to be bound by the terms therein. I understand that I may be subject to the HSE’s disciplinary procedures should I fail to comply with the existing HSE I.T. policies and this Agreement. | | | | | | \***Tick to denote agreement:** | |
|  | | | |  | | | |
| \***Your Full Name:** | | | | \***Personnel Number:** | | | |
| \***Grade:** | | \***Job Title:** | | | | | |
| \***Work contact number:** | | | \***Email address:** | | | | |
| \***Department:** | | | | | | | |
| \***Full Work address:** | | | | | \***Eircode:** | | |
| \***Device asset tag number:** | | | \***Device username:** | | | | |
| \***My Line Manager supports this request:** | \***Yes** | | Your Line manager will be required to approve this request as part of the self-service process. You will be prompted to specify their email address. | | | | |
| \***Line Manager name:** | | | \***Line Manager email:** | | | | |
| \***HSE approved USB memory sticks are intended for use by permanent HSE employees only, please confirm you are a permanent member of staff:** | | | | | | | \***Yes** |
| **Date:** | | | | | | | |
| **\*\*NOTE: If details are omitted, your request will be cancelled and not processed\*\*** | | | | | | | |