Smart Device Usage Agreement

1) In support of existing *HSE I.T. Security Policies* this agreement specifically governs the use of HSE approved smart devices. For the purpose of this Agreement, smart devices are defined as any handheld mobile computer device which is capable of wireless connection (via WiFi, 3G, 4G etc), voice and video communication and, internet browsing. (for example: Apple IOS enabled devices (i.e. iPhone & iPad), Google Android enabled devices (i.e. Samsung Galaxy tablet), Windows Mobile enabled devices and, Blackberry RIM enabled devices etc)

2) HSE approved smart devices are to be used primarily for HSE business related purposes. Occasional personal use is permitted provided it is in accordance with *HSE I.T. Security Policies*, it is not excessive, it does not interfere with the persons work or performance and it does not incur any significant costs to HSE.

3) HSE approved smart devices must not be used for any commercial activities, such as running any sort of private business, advertising or performing any sort of work for personal gain or profit.

4) HSE approved smart devices must only be accessible by authorised personnel and must not under any circumstances be accessible by family members or others.

5) HSE approved smart devices must have device encryption enabled at all times.

6) Personnel who have been issued with a HSE approved smart device must take all reasonable measures to ensure the smart device is kept secure at all times and is protected against unauthorised access, damage, loss and theft. The smart device must be kept with you at all times when working off-site and not left unattended and, locked away securely when not in use.

7) The password used to access the HSE approved smart device must not be written down on the smart device or stored with or near the smart device.

8) When using a HSE approved smart device in a public place precautions should be taken to ensure any confidential or restricted information (as defined by the *HSE Information Classification & Handling Policy*) displayed on the smart device screen cannot be viewed by others.

9) HSE approved smart devices should not be used for the long term storage of confidential and restricted information. Confidential and restricted information (as defined by the *HSE Information Classification & Handling Policy*) must where possible be stored on a secure HSE network server. Where confidential or restricted information is stored on a HSE approved smart device the information must be backed up on a regular basis.

10) Confidential and restricted information (as defined by the *HSE Information Classification & Handling Policy*) should always be deleted from the HSE approved smart device when it is no longer required.

11) Any confidential and restricted information (as defined by the *HSE Information Classification & Handling Policy*) stored on the HSE approved smart device must not be transferred to any internal (except a secure HSE network server) or external system in an unencrypted form

12) The hardware and software configuration of the HSE approved smart device must not be altered without the authorisation of the HSE ICT Directorate.

13) Personnel who have been issued with a HSE approved smart device will be held responsible for all internet connections made from their smart device. They must ensure that all internet access from their device is in accordance with requirements of the *HSE I.T. Acceptable Use Policy*, *HSE Electronic Communications Policy* and the *HSE Internet Filter Standard.*

14) HSE approved smart devices must not be used to create, view, download, host or transmit any material (i.e. images, video clips, audio recordings etc) which is:

    a) Prohibited by law;
    b) Pornographic or of a sexual nature;
    c) Threatening, racist, extremist, offensive or obscene;
    d) Protected as trade secrets or copyrighted.

15) Personnel who have been issued with a HSE approved smart device will be held responsible for all software applications (i.e. apps) downloaded and installed on their smart device. They must ensure they only download and install software applications on the smart device when (1) there is a valid HSE business related reason for installing and using the software application, (2) the software application can add value to the HSE staff members work for the HSE and (3) they have the correct and proper license for the software application.

16) Under no circumstances should any software application (i.e. app) be downloaded and installed on a HSE approved smart device where the HSE staff member is prompted as part of the install to allow any access to the device contents

17) Under no circumstances should HSE confidential or restricted information (as defined by the *HSE Information Classification & Handling Policy*) which is stored on a HSE approved smart device be uploaded onto a software application (i.e. app) without the prior approval of the HSE ICT Directorate.

18) HSE information which is sent via email from a HSE approved smart device must be sent using the persons official work email account. The use of personal or third party web based email accounts (i.e. eircom.net, hotmail, Gmail, Yahoo Mail, doctors.net etc) for the transmission of HSE confidential or restricted information (as defined by the *HSE Information Classification & Handling Policy*) is strictly prohibited.

19) Recipients of a HSE smart device must report any loss or theft of the smart device immediately to their line manager and the ICT Directorate.

20) The HSE reserves the right to recall and/or inspect the smart device at anytime and to alter, add or delete software or hardware.

21) HSE issued smart devices and the information they contain remain the property of the HSE. Personnel who intend leaving the employment of their employer must ensure they return their HSE issued smart device to their line manager before they leave.

22) The HSE reserves the right to take such action as it deems appropriate against any person who breaches the conditions of this agreement. Personnel who breach this agreement may have their HSE issued smart device withdrawn and maybe subject to appropriate disciplinary action. The HSE will refer any use of its smart devices for illegal activities to the Gardai.

Smart Device Recipient Statement:

I fully accept and understand my obligations under the existing *HSE I.T. Security Policies* and this Agreement and I agree to be bound by the terms therein. I understand that I maybe subject to disciplinary procedures should I fail to comply with the existing *HSE I.T. Security Policies* and this Agreement.

Print Name: ……

Grade / Job Title: ……. Personnel No: …….

Telephone No: ……. Email: …….

Functional Area: ……

Location: …….. …….

…….

Signature: ……. Date: .....