IMPORTANT NOTES:

1. This Security Policy and Procedures (“Policy”) apply without exception to all Red Dot 365 and Wellbeing Service Provider staff, together with contractors, consultants, volunteers and any other supplier of services to the Company or a Wellbeing Service Provider, who have access to any Red Dot 365-related data, including (but not limited to) Participants’ personal information (e.g. names, addresses, phone numbers, wellbeing history, health and wellbeing records etc.).
2. In this Policy, the “Authority” means Red Dot 365, (Contracted Wellbeing Service Provider of wellbeing services or employer)
3. Participant means any employee or citizen to whom the Red Dot 365 and/or members of the Company’s network who provide services, under the four areas of wellbeing, physical, mental, personal and professional.
4. Notwithstanding the definition of “Authority Data” in the contract definitions:
    a. “Authority Data” in this Policy means any data, text, drawings, diagrams, images or sounds (in any media) the loss or theft of which would cause financial or reputational damage to the Authority. All such data is referred to as “Authority Data” in this document.
    b. Personal Data” in this Policy means personal data for which the Authority is the Data Controller (i.e. Participants’ personal ” .)data
5. This Policy supplements the Red Dot 365 and Wellbeing Service Providers’ existing information security Policy, Procedures and Guidance Notes and, in the event of conflict or inconsistency, this Policy will prevail for all staff accessing Authority Data and/or Personal Data.
6. In particular, classification of information (and its consequent labelling) for any Authority and/or Personal Data generated in the course of this contract will be classified and labelled in accordance with HMG’s definitions (i.e. Top Secret, Secret, Official or Official – Sensitive). When employees working on the Wellbeing Service Provider contracts are classifying non-Wellbeing Service

Provision information (e.g. internal staff reviews, employment details etc.), they should use the Red Dot 365's Protective Marking System and Procedures.

7. This Policy is subject to revision, as may be required from time to time by the Authority.
8. All Red Dot 365 and Wellbeing Service Provider staff are required to read this Policy and sign the declaration to confirm that they understand the contents and will comply with the Policy. Fully signed copies must be returned to the Red Dot 365 information e mail (info@reddot365.co.uk).

1. INFORMATION RISK MANAGEMENT PROCEDURES

Red Dot 365 will:

- Identify, keep and disclose to the Authority upon request a record of those members of Red Dot 365 and Wellbeing Service Provider staff with access to or who are involved in handling Personal Data ("users"); and
- Provide to the Authority details of its policy for reporting, managing and recovering from information risk incidents, including losses of Personal Data and ICT security incidents and its procedures for reducing risk and raising awareness; and
- Immediately report information security incidents to the Authority. Significant actual or potential losses of personal data may be shared with the Information Commissioner and the Cabinet Office by the Authority.

2. PERSONNEL

2.1. User Permissions

- Prior to being permitted to have any type of access to Authority Data or Personal Data in any format, or to use the Red Dot 365 Platform software, all Red Dot 365 and Wellbeing Service Provider staff must have completed and signed the appropriate forms. The Appendix (attached) show the form:

- Appendix 1: Form A1 Wellbeing Service Provider - Data Usage Agreement (incorporating the Incident Management Procedure)

.

IMPORTANT NOTE 1: The document contains specific requirements and procedures, which are deemed to form part of this Policy. Compliance is essential.

IMPORTANT NOTE 2: Ensure that all individuals accessing Authority Data or Personal Data sign Form A1 (e.g. those who open incoming mail, undertake audit / compliance functions, work within Finance on this programme etc.)

- All Red Dot 365, Wellbeing Service Provider (as applicable) or other staff with any type of access to Personal Data must fully complete and sign form A1.
- All fully completed and individually signed forms (both for the Red Dot 365 and Wellbeing Service Providers) are to be sent to and retained by the Red Dot 365's Service Desk to enable spot checks to be carried out by Red Dot 365.
- The Red Dot 365 and Wellbeing Service Providers must ensure that forms are reviewed by users on an annual basis, with email acceptance that they have done so. These emails must be sent to the Red Dot 365's Service Desk.
- Must supply this information to the Red Dot 365's Service Desk in real time.
- In the event of a suspected security breach, the Authority reserves the right to suspend any user accounts in relation to that breach.

2.2. Staff Vetting

All Red Dot 365 and Wellbeing Service Provider staff working on a service must have been vetted to the level appropriate to their role, before being permitted to access Authority Data or Personal Data in any format.

2.3. Staff Training

Prior to being permitted to have any type of access to Personal Data or Authority Data:

2.3.1. All Wellbeing Service Provider staff must have successfully completed the Wellbeing Service Provider's own Information Security and/or Data Protection course(s);

3. PERSONAL DATA

3.1. Paper records containing Personal Data must be shredded in a cross-cut shredder.

Red Dot 365 does not specify the grade of cross-cut shredder required, save to state that it must deal with OFFICIAL-SENSITIVE information. Accordingly, a P-4 (as a minimum) grade cross-cut shredder must be used for disposal of Personal Data.

- The specification of the containers must be approved by a member of the Red Dot 365's Information Security Dept. and they must be secured by combination locks;
- The combination of each container must be kept securely and not be disclosed other than to those authorised to view the contents;
- When not in use, the containers must be stored in a secure room, with access restricted to staff members only and access permissions (granting and revocation of permission) controlled;
- A register of the containers and of their combinations must be maintained and retained securely on site;
- The containers must never be removed from site.

3.2. All Red Dot 365 and Wellbeing Service Provider staff must maintain a register of paper documentation containing Personal Data, which includes a signed confirmation of secure disposal. A register template will be made available for the use of Red Dot 365 and Wellbeing Service Provider staff.

3.3. Until its destruction, Personal Data must be stored in a metal filing cabinet or other approved secure container located in secure premises. If approved secure containers are used, see 4.4 above for additional security controls. Access to cabinet keys must be restricted to authorized users only and a key register and/or a container register and combination register must be maintained. Personal Data may be transported only in a nondescript bag in order to not draw attention to the contents. If it

is necessary, for logistical reasons, for Personal Data to be stored overnight at an employee's home, the bag must be stored out of view. Under no circumstances may Personal Data be left unattended in motor vehicles, whether in a briefcase or not.

4. SECURITY HANDLING GUIDANCE FOR "OFFICIAL" CLASSIFICATION LEVEL

Red Dot 365 definitions:

a) OFFICIAL:

This marking applies to the majority of information that is created or processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile.

For the purpose of this Policy, all routine correspondence and data will be treated as OFFICIAL, unless covered by the criteria below.

b) OFFICIAL – SENSITIVE:

A limited subset of OFFICIAL information could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media. This subset of information should still be managed within the "OFFICIAL" classification tier but may attract additional measures (generally procedural or personnel) to reinforce the "need to know". In such cases where there is a clear and justifiable requirement to reinforce the "need to know", assets should be conspicuously marked: OFFICIAL–SENSITIVE.

All Red Dot 365 Data is, at a minimum, "OFFICIAL".

"OFFICIAL – SENSITIVE" information is of a particularly sensitive nature. The "SENSITIVE" caveat must be used in limited circumstances (depending on the subject area, context and in some cases, any statutory or regulatory requirements) where there is a clear and justifiable requirement to reinforce the 'need to know'.

For the avoidance of doubt, all Personal Data must be classified, marked and handled as "OFFICIAL – SENSITIVE".

4.1. Marking

There is no requirement to mark routine OFFICIAL information.

In limited circumstances where there is a clear and justifiable 'need to know' requirement, the "SENSITIVE" caveat must be used. **OFFICIAL – SENSITIVE information must always be clearly marked**.

Mark "OFFICIAL – SENSITIVE" in capital letters at the top and bottom of each document page, and in the Subject line and body of all emails. This could be followed by any handling or access requirements.

4.2. Handling of Information You Create

This applies to all material, whether paper, electronic or digital media.

Handling instructions are there to identify why special handling is required; who is to be allowed access to the information; how that information or data is allowed (or not) to be circulated or forwarded on and how it is to be stored.

You control how the information you create is to be handled: you can describe any particular sensitivities of the information and offer meaningful handling advice. Additional handling instructions must be included following advice from the Information Asset owner to identify handling requirements.

Handling instructions must be included:

- On the front page of any document, and at the top of each page.
- As the first paragraph of any letter or minute.
- As the first paragraph of any email.
- Highlighted in the operations instructions for any dataset.

4.3. Handling of Others' Information

This applies to all material, whether paper, electronic or digital media.

You must follow any handling guidance stipulated by the Information

OFFICIAL:

- Lock computers when away from your desk.
- Adhere to the Red Dot 365's or Wellbeing Service Provider's Clear Desk & Screen Guidance Notes.

- OFFICIAL – SENSITIVE: as above (OFFICIAL) plus:
- Ensure documents are seen by, or passed to individuals only on a 'need to know' basis.

4.3.1. Emailing Material:

- All users of Secure e Mail are also required to abide by the relevant legislation pertaining to the sharing of information, including the Data Protection and Freedom of Information Acts.
- In some exceptional circumstances, organisation administrators will be able to access other users' accounts. This is a privilege to help the smooth functioning of Secure e Mail in the event of a user's serious illness, absence or death, and must not be abused.

4.3.2. Moving assets by hand or post:

You must follow any handling guidance stipulated by the Information Asset owner.

- BY HAND:
  - OFFICIAL (Red Dot 365 Data)
    - Protected at least by one cover/envelope.

        - Authorisation secured from the Information Asset owner if moving a significant volume of assets / records / files.
    - OFFICIAL – SENSITIVE (Personal Data): as above (OFFICIAL) plus:
        - Carried in a nondescript bag in order to not draw attention to the contents.
        - Never leave papers unattended.

- BY POST/COURIER:
    - OFFICIAL (Red Dot 365 Data)
        - Use single, unused envelope.
    - OFFICIAL – SENSITIVE (Personal Data): as above (OFFICIAL) plus:
        - Include return address on back of the envelope.
        - Never mark the classification on envelope.
        - Consider double envelope for highly sensitive assets (write the classification on the inner envelope only).
        - Always use a fully tracked service (reputable courier or Royal Mail's Special Delivery).

5. TELEPHONES

When discussing work on telephones (landline or mobile), either verbally or in text messages, in video conferences or in public places, you must assume that telephony systems and video conferencing are inherently insecure.

- OFFICIAL:
    - No restrictions but be careful of straying into areas that could be deemed as OFFICIAL – SENSITIVE.
- OFFICIAL – SENSITIVE:
    - Details of sensitive material must be kept to an absolute minimum.

6. SUBJECT ACCESS REQUESTS

A Subject Access Request (SAR) is a request from a data subject to have access to his/her Personal Data

Red Dot 365 and Wellbeing Service Provider staff must notify the Red Dot 365's team info@reddot365.co.uk within two working days of:

- any request from a Participant to have access to his/her Personal Data (a Subject Access Request) or
- any complaint or request relating to the Authority's obligations under the Data Protection Legislation,

so that the Red Dot 365 can notify the Authority within the prescribed period.

- The Red Dot 365's Customer Care Team must notify the Wellbeing Service Provider.

All Red Dot 365 and Wellbeing Service Provider staff are reminded that they must transfer information in a responsible and professional manner, and that this information could be viewed by a data subject through a Subject Access Request.

7. FREEDOM OF INFORMATION ACT REQUESTS

The Freedom of Information Act (FOIA) gives any member of the public the right to access recorded information held by public sector organisations. The Red Dot 365 and its Wellbeing Service Providers are, therefore, not bound by the FOIA. However, Red Dot 365 and / or a wellbeing service provider may find themselves working with a public body who is bound by the Act.

Public sector organisations require that the Red Dot 365 must notify it of any such requests received by the Red Dot 365 or by Wellbeing Service Providers.

Red Dot 365 and Wellbeing Service Provider staff must notify the Red Dot 365's Customer Care (info@reddot365.co.uk) of any Request for Information that it receives as soon as is practicable and in any event within one working day of receiving that Request for Information, so that the Red Dot 365 can notify the Authority within the prescribed period.

Appendix 1: Form A1 SERVICE PRVIDER - Data Usage Agreement (incorporating the Incident Management Procedure)

Area of control	All Staff
Personnel Security **(Training and Awareness)**	• You must re-acknowledge agreement to the latest version of this Data Usage Agreement on an annual basis or following any updates • If you have line management responsibilities, you must ensure that all your staff that use Red Dot 365 data / systems carry out their responsibilities in support of information security and are aware of, and familiar with, all relevant security policies as per the contract with Red Dot 365.
System Security **(Data Handling)**	• Do not allow unauthorised personnel to observe Red Dot 365 data / systems. • You should only use the Red Dot 365 data / systems for the businesses purposes for which it is intended. Data must not be used for any other purpose. • You must only access Red Dot 365 data / systems from a secure location (as defined by your employer's local policies) using equipment provided by your employer. • You must apply Red Dot 365 data handling procedures to any information processed, taking careful account of the sensitivity of the information. • You must follow a 'clear desk policy' and store hard-copy data in lockable, secure containers, with restricted access, when it is not in use. • You must destroy paper documents as soon as they are no longer required in a shredder with cross-shredding functionality. • Records in any format that contain personal or sensitive information must not be removed from your office location without prior agreement from your line manager. • You must not divulge any information after cessation of employment.
Communications **(Sending / Receiving)**	• If you send personal or sensitive information to Red Dot b365 or another recipient, the data is your responsibility until the receiver verifies that the data has been received and has not been compromised (opened or tampered with). It is your responsibility to ensure that the recipient address is correct before sending information. • Appropriate tracking should be used for sending information between locations such as utilising a courier service or Royal Mail Recorded / Special Delivery – though it should be remembered that the Recorded Delivery tracking service provides limited information.
Email Communications	• Red Dot 365 data must only be sent to authorised recipients. It is your responsibility to ensure the recipient email address is correct. • Personal or sensitive information transferred by email, must be done so securely.
Security Incident Reporting	• You must be aware of and comply with the Incident Management procedure. • You must report any incident involving a suspected or known security breach involving personnel, hardware, software, communications, document or physical security as per the procedure outlined in "Incident Management Procedure"

Incident Management Procedure

Personal Data relates to any information which identifies an identifiable living individual, including any expression of opinion about that person or expression of intentions towards them. Personal Data compromise can occur through theft, loss or deliberate or unintentional damage or destruction.

The list below is not exhaustive, but examples include:

- Loss of a participant's files / paperwork, or one turning up where it should not be;
- Information missing in the post or from a fax transmission;
- Theft of a computer or memory stick containing Personal Data (Note: no data relating to participants must be held on or used with unapproved devices);
- Loss of a mobile phone containing Personal Data;
- Deliberate or accidental disclosure of Personal Data;
- Leaving a computer disk or laptop containing personal information on a train or in any non-secure environment.

How "significant" a compromise is will depend on a number of factors and on the individual circumstances of a case. In all cases of data loss or compromise in relation to the delivery of the WELLBEING SERVICE PRVIDER, you must:

While some assessment of the significance of the loss will only be apparent after this investigation, it is important that all losses or potential losses are reported immediately (within one hour), without waiting for the results of investigations or risk assessments.

The investigation should cover the following points:

- Numbers of individuals affected;
- Type of data compromised (e.g. Personal Data, sensitive corporate data, non-sensitive data);
- Circumstances of the incident (including physical environment, time of day);
- Whether the incident concerns or affects other organisations;
- Full assessment of the possible risks arising, covering risks to data subjects, the public.

You are advised to keep notes, especially if the incident is complex or developments are moving fast and details need to be captured.

Report the results of the investigation to Red Dot 365's Head of Information Security, without delay.

Use all reasonable efforts to rectify the cause of such breach, following consultation with the Red Dot 365's Head of Information Security.

Next steps will include recommendations on whether and how to inform data subjects (those whose data has been lost / compromised) or other parties. These should be based on an objective and accurate assessment of the statutory duties, the potential risks and the benefits of disclosure. The decision concerning whether to inform the Information Commissioner's Office and the Police. For example, if the incident involves risk information or where the loss involves possible theft of data from premises or systems.

Your local data protection officers are:

Organisation	**Name and Role**	**Contact Details**
RED DOT 365	John Williams	Email: j.williams@reddot365.co.uk Mobile: 07425 558130
[to be completed by Wellbeing Service Provider]	[to be completed by Wellbeing Service Provider]	[to be completed by Wellbeing Service Provider]
[to be completed by Wellbeing Service Provider]	[to be completed by Wellbeing Service Provider]	[to be completed by Wellbeing Service Provider]

NOTE: Red Dot 365 requires assurance that all Authority Data is also protected and, therefore, Red Dot 365 staff and Wellbeing Service Providers must notify the Red Dot 365's Head of Information Security of any incidents arising in connection with Authority Data, giving full details of:

- **Type of data compromised (e.g. sensitive corporate data, non-sensitive data);**
- **Circumstances of the incident (including physical environment, time of day);**
- **Whether the incident concerns or affects other organisations;**
- **Full assessment of the possible risks arising, covering risks to data subjects, the public, Red Dot 365 operations and reputation;**
- **Proposed corrective / preventive actions, with a timeframe for implementation.**

By signing below I acknowledge that I have read the Red Dot 365 Data Usage Agreement (DUA) policy and Incident Management Procedure for Red Dot 365 provided IT systems, and agree to be bound by them. I also agree to comply with any organisational and local policies that are not covered, but do not conflict with the above agreement.

Name: _____ Date: _____

Signature: _____

All Red Dot 365 and Wellbeing Service Provider staff are required to sign the following, prior to being authorized to access any Authority or Personal Data.

By signing below I acknowledge that I have read the Red Dot 365 Security Policy and Procedures, and that I agree to adhere to them. I also agree to comply with any organisational and local policies that are not covered, but do not conflict with the above agreement. I understand that failure to comply with any aspect of the Security Policy and Procedures may lead to disciplinary proceedings, including dismissal for a gross breach or continued non-compliance.

Name: _____ Date: _____

Signature: _____