ICO Ref: **ENF0525289 and ENF0516099**

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Council of the Isle of Scilly
Town Hall
St Mary's
Isles of Scilly
TR21 0LW

I, Mr Theo Leijser, Chief Executive of The Council of the Isle of Scilly, hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. The Council of the Isle of Scilly is the data controller as defined in section 1(1) of the Data Protection Act 1998 (the 'Act'), in respect of the processing of personal data carried out by the Council of the Isle of Scilly and is referred to in this Undertaking as the 'data controller'. Section 4(4) of the Act provides that, subject to section 27(1) of the Act, it is the duty of a data controller to comply with the data protection principles in relation to all personal data in respect of which it is a data controller.

2. The Information Commissioner (the 'Commissioner') was informed of an incident in June 2013, whereby an attachment was included in error within an email. The attachment contained information relating to a disciplinary hearing, and included unredacted personal data relating to third parties. The recipients of the email were the employee who was subject to the disciplinary hearing and their union representative.

3. The Commissioner's investigation determined that whilst the individual who sent the email was aware of the information governance implications of sending such data via this medium, in general there was no formal data protection training in place at the authority.

4. The Commissioner was further informed of another incident which came to light in September 2013, involving the disclosure of two documents containing sensitive personal data. The documents were disclosed to authorised parties initially but the security controls around their sharing was weak which resulted in the documents ending up in public circulation. The information disclosed related to the conduct and an investigation of a former Head Teacher and included an audit report and a transcript of an interview. There is evidence that the documents were emailed to personal accounts and distributed from a Council meeting.

5. A number of persons and organisations were privy to the information and the Council considered that they had a legitimate business need to receive the information. However, weaknesses surrounding the distribution of the documents, which prevented the effective control of the information contained within them, were identified during the Commissioner's Investigation. For instance, paper documents were shared without using appropriate redaction techniques.

6. The investigation revealed that documents had been emailed to non-corporate personal accounts without password or encryption controls in place. In addition, the Commissioner's investigation determined that staff training and awareness of the requirements of the Act in general could be improved.

7. Following consideration of the remedial action that has been taken by the data controller, it is agreed that in consideration of the Commissioner not exercising his powers to serve an Enforcement Notice under section 40 of the Act, the data controller undertakes as follows:

The data controller shall, as from the date of this Undertaking and for so long as similar standards are required by the Act or other successor legislation, ensure that personal data are processed in accordance with the Seventh Data Protection Principle in Part I of Schedule 1 to the Act, and in particular that:

(1) The data controller shall implement and enforce mandatory data protection training in relation to both the requirements of the Act and the data controller's policies concerning the use of personal data. Completion of such training shall be recorded and monitored to ensure compliance;

(2) The data controller shall set up a refresher programme to ensure that data protection training shall be updated at regular intervals; Completion of such training shall be recorded and monitored to ensure compliance;

(3) Appropriate guidance should be drafted and communicated to staff with respect to the safe transfer of personal data by email. The use of an encryption platform to protect all forms of electronic information when shared both internally and externally should also be considered where appropriate;

(4) A policy on the application of redactions should be drafted and implemented;

(5) Compliance with the data controller's policies on data protection and I.T security shall be appropriately and regularly monitored;

(6) The data controller shall implement such other security measures as it deems appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage.

Signed .....
Mr Theo Leijser, Chief Executive
Council of the Isle of Scilly

Dated .....

Signed .....
Stephen Eckersley, Head of Enforcement
For and on behalf of the Information Commissioner

Dated .....