ICO Ref: **ENF0381336**

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Bay House School

Gomer Lane
Alverstone
Gosport
Hants
PO12 2QP

I, Ian Potter, Head Teacher of Bay House School, for and on behalf of Bay House School hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. Bay House School 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 Bay House School 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 provided with a report explaining how a substantial volume of personal data, including some sensitive personal data, was put at risk of disclosure during a hacking attack on the school's website.

3. Computer hackers, including at least one of the school's own pupils, gained access to the data controller's internal information management system via an attack on its remotely hosted website. Despite having a policy in place prohibiting the use of duplicate passwords, the data controller failed to identify that a staff member was employing the same password to access both the school's web and management systems. This presented a significant information security risk and provided the hackers with sufficient system administration information in order to access the data in question.

4. The Commissioner has considered the data controller's compliance with the provisions of the Act in the light of this matter. The relevant provision of the Act is the Seventh Data Protection Principle. This Principle is set out in Schedule 1 Part I to the Act. The Commissioner has also considered the fact that some of the data compromised in this incident consisted of information as to the physical health of the data subjects. Personal data containing such information is defined as 'sensitive personal data' under section 2(e) of the Act.

5. The Commissioner has further considered that, although the data included some sensitive personal data this was limited in nature and its disclosure appears not to have caused substantial damage or distress to the data subjects.

6. 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 it shall:

(1) Implement appropriate measures in order to encrypt and segregate sensitive and confidential information held on the data controller's information management system, from basic identification and contact details;

(2) All appropriate users are made aware of the data controller's password protocols and updated password policy, and are appropriately trained in their use;

(3) School IT systems will be made subject of appropriate penetration testing, completed on at least an annual basis;

(4) 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 Ian Potter, Head Teacher
Bay House School

Dated: …….

Signed: ……

Sally-Anne Poole, Head of Enforcement
For and on behalf of the Information Commissioner

Dated: …….