Stony Dean School

DATA PROTECTION POLICY

Date created: September 2020

Date for review: September 2022

Index of Policy

1. GDPR Introduction and GDPR definitions

The EU General Data Protection Regulation or "GDPR" is the most important change to data protection and privacy law in two decades. It was approved by the EU Parliament in April 2016 and comes into force in the UK on 25th May 2018. The GDPR will replace the Data Protection Act 1998 and, while it is similar to the current regime under the 1998 Act in many ways, it is a great deal more modern, taking into account major advances in science and technology. Its purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

GDPR definitions

Orchard End Avenue, Pineapple Road, Amersham, HP7 9JW Tel: 01494 762538 Fax: 01494 765631

www.stonydean.bucks.sch.uk

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special Category data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data subject – any living individual who is the subject of personal data held by an organisation.

Data subject consent - means any freely given, specific, informed and unequivocal indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behavior. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise

processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Child – the GDPR defines a child as anyone under the age of 16 years old, although this may be lowered to 13 by Member State law. The processing of personal data of a child is only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

2. Data protection principles

All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. Stony Dean School policies and procedures are designed to ensure compliance with the principles.

2.1 Personal data must be fairly, lawfully and transparently processed

The GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The Regulation states that processing of personal data shall be lawful, processed fairly and transparently.

Lawful – Lawfully means within the bounds of the Law. Identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing", for example consent.

Fairly – in order for processing to be fair, the data controller has to ensure that the data collected is transparent with the data subjects at the point of collecting the data. This applies whether the personal data was obtained directly from the data subjects or from other sources.

The GDPR specifies that information should be made available to data subjects regarding processing, which is covered in the 'Transparency' requirement.

Orchard End Avenue, Pineapple Road, Amersham, HP7 9JW Tel: 01494 762538 Fax: 01494 765631

www.stonydean.bucks.sch.uk

Transparently – the GDPR includes guidelines on giving privacy information to data subjects in Articles 12, 13 and 14. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an easy to understand manner using clear and plain language.

Stony Dean School Privacy Policy is issued by being available on our website

The specific information that must be provided to the data subject must, as a minimum, include:

2.1.1 the identity and the contact details of the controller and the controller's representative;

2.1.2 the contact details of the Data Protection Officer where applicable;

2.1.3 the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

2.1.4 processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child;

2.1.5 the period for which the personal data will be stored, or if that is not possible the criteria used to determine that period;

2.1.6 the existence of the rights to request from the controller, access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;

2.1.7 the recipients or categories of recipients of the personal data, if any;

2.1.8 processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

2.1.9 where applicable the fact that the controller intends to transfer personal data to a third country or an international organisation and appropriate suitable safeguards will be maintained and the means by which to obtain a copy of them or where they have been made available;

2.2 Processed for Specified, Explicit and Legitimate Purposes

2.2.1 The Data Protection Officer is responsible for ensuring that Stony Dean School does not use the personal data for a purpose other than that for which they were collected, the controller should provide the data subject prior to that further processing the information on that other purpose.

2.2.2 All data collection forms (electronic or paper), including data collection requirements in new information systems, must include a fair processing statement or link to privacy statement and approved by the Data Protection Officer.

2.2.3 The Data Protection Officer will ensure that, on a one year basis all data collection methods are reviewed by data controllers to ensure that collected data continues to be adequate, relevant and not excessive and is up to date where necessary.

2.2.4 Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

2.3 **Adequate, Relevant and Not Excessive**

2.3.1 Data that is stored by the data controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

2.3.2 The Data Protection Officer is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

2.3.3 It is also the responsibility of the data subject to ensure that data held by Stony Dean School is accurate and up to date. Completion of a registration or application form by a data subject will include a statement that the data contained therein is accurate at the date of submission.

2.3.4 Employees / Staff / customers / others should be required to notify Stony Dean School of any changes in circumstance to enable personal records to be updated accordingly. Instructions for updating records are contained *[file location]*. It is the responsibility of Stony Dean School to ensure that any notification regarding change of circumstances is recorded and acted upon.

2.3.5 The Data Protection Officer is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

2.3.6 On at least an annual basis, the Data Protection Officer will review the retention dates of all the personal data processed by Stony Dean School, by reference to the data inventory, and will identify any data that is no longer required in the context of the registered purpose. This data will be securely deleted/destroyed in line with the Secure Disposal of Storage Media Policy.

2.3.7 The Data Protection Officer is responsible for responding to requests for rectification from data subjects within one month. This can be extended to a further two months for complex requests. If Stony Dean School decides not to comply with the request, the Data Protection Officer must respond to the data subject to explain its reasoning and inform them of their right to complain to the supervisory authority and seek judicial remedy.

2.3.8 The Data Protection Officer is responsible for making appropriate arrangements that, where third-party organisations may have been passed inaccurate or out-of-

date personal data, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required.

2.3.9 Where personal data is retained beyond the processing date, it will be *[encrypted/pseudonymised]* in order to protect the identity of the data subject in the event of a data breach.

2.3.10 Personal data will be retained in line with the Retention of Records Procedure and, once its retention date is passed, it must be securely destroyed as set out in this procedure.

2.3.11 The Data Protection Officer must specifically approve any data retention that exceeds the retention periods defined in Retention of Records Procedure and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written.

3. Responsibility and accountability

3.1 Stony Dean School (Buckinghamshire County Council) is a public authority or body under the GDPR.

3.2 The Organisation's Data Protection Officer is JSL Services Group Limited of The Old Post Office, Wycombe Road, Studley Green, Bucks, HP14 3XA

3.3 Data Protection Officer is responsible for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes:

3.3.1 development and implementation of the GDPR as required by this policy.

3.3.2 security and risk management in relation to compliance with the policy.

3.4 Stony Dean School shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

- The purposes for which the Organisation processes personal data;
- Details of the types of personal data collected, held, and processed by Stony Dean School; and the types of data subject to which that personal data relates;
- Details of any third parties that will receive personal data from the Organisation;
- Details of how long personal data will be retained by the Organisation; and
- Detailed descriptions of all technical and organisational measures taken by the organisation to ensure the security of personal data.
- Details of any transfers of personal data to non-EEA countries including all procedures and security safeguards for the data (including Cloud Service Providers).

3.5 Data Protection Officer, Stony Dean School considers to be suitably qualified and experienced, has been appointed to take responsibility Stony Dean School compliance with this policy on a day-to-day basis and, in particular, has direct responsibility for ensuring that Stony Dean School complies with the GDPR in respect of data processing that takes place within their area of responsibility.

3.6 The Data Protection Officer has specific responsibilities in respect of procedures such as the Subject Access Request Procedure and are the first point of call for Employees/Staff seeking clarification on any aspect of data protection compliance.

3.7 Compliance with data protection legislation is the responsibility of all Employees/Staff of Organisation Name who process personal data.

3.8 Stony Dean School Training Policy sets out specific training and awareness requirements in relation to specific roles and Employees/Staff of Organisation Name generally.

3.9 Employees/Staff of Stony Dean School are responsible for ensuring that any personal data about them and supplied by them to Stony Dean School is accurate and up-to-date.

4. Data subjects' rights

The GDPR sets out the following rights applicable to data subjects, and the data that is recorded about them:

- The right to be informed;
- The right to make subject access requests regarding the nature of information held and to whom it has been disclosed.
- The right to rectify, block, erase, including the right to be forgotten, or destroy inaccurate data.
- The right to erasure (also known as the 'right to be forgotten');
- The right to object to or restrict processing;
- The right to data portability.
  The right to prevent processing for purposes of direct marketing.
- Rights to be informed about automated decision-making and profiling that will directly affect them.
- The right to have personal data provided to them in a structured, commonly used format, and the right to have that data transmitted to another controller
- To seek for compensation if they suffer damage by any contravention of the GDPR.

Automated Decision making

In the event that the Organisation uses personal data for the purposes of automated decision-making and those decisions have a legal (or similarly significant effect) on data subjects, data subjects have the right to challenge to such decisions under the Regulation, requesting human

intervention, expressing their own point of view, and obtaining an explanation of the decision from the Organisation.

This right does not apply in the following circumstances:

- The decision is necessary for the entry into, or performance of, a contract between Stony Dean School and the data subject;
- The decision is authorised by law; or
- The data subject has given their explicit consent.

5. Subject Access Requests

Stony Dean School ensures that a data subject may make a subject access request ("SAR") , as per Subject Access Request Procedure, at any time to find out more about the personal data which Stony Dean School holds about them. Any such requests will be handled by the Data Protection Officer within 30 days of receipt.

Stony Dean School does not charge a fee for the handling of normal SARs. The organisation does reserve the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are evidentially unfounded or excessive, particularly where such requests are repetitive.

Data subjects have the right to complain to Stony Dean School related to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled in line with Stony Dean School Complaints Procedure.

6. Consent

- Stony Dean School understands 'consent' to mean that it has been explicitly and freely given, and a specific, informed and unequivocal indication of the data subject's consent. A written confirmation to the processing of personal data relating to him or her will be recorded. The data subject can withdraw their consent at any time.
- In the case of sensitive data (special category data) being collected, clear and concise written consent of data subjects must be obtained unless there is an alternative legitimate basis for processing exists.
- Stony Dean School understands 'consent' to mean that the data subject has been fully informed of the intended processing and has clearly indicated consent, while in a fit state of mind to do so and without pressure being exerted upon them.

- Consent will not be implied from non-response to a communication. The Controller must be able to demonstrate that consent was obtained for the processing operation and a response to that consent was agreed with the data subject.
- In most instances, consent to process personal and special category data is obtained routinely by Stony Dean School using standard consent documents e.g. when a child joins the school, etc. as per our Consent Procedure.
- Where Stony Dean School provides online services to children, parental or custodial authorisation must be obtained. This requirement applies to children under the age of 16 (unless the Member State has made provision for a lower age limit, which may be no lower than 13).

7. Security of data

1. All Employees/Staff are responsible for ensuring that any personal data that Stony Dean School holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by Stony Dean School to receive that information and has entered into a confidentiality agreement.
2. All staff to sign the Stony Dean School Acceptable Use Policy
3. All personal data should be accessible only to those who need to use it, and access may only be granted in line with our Access Control Policy. All personal data should be treated with the highest security and must be kept:
   - in a lockable room with controlled access.
     or
   - in a locked filing cabinet or locked cupboard / drawer.
     or
   - if computerised, password protected in line with correct levels of access permitted to access as per our Access Control Policy.

- any external storage computer media will be encrypted in line with our Use of USB and data storage devices policy. Stony Dean School shall ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. If necessary, risk assessment will be carried out taking into account all the circumstances of Stony Dean School controlling or processing operations. In this assessment, the Data Protection Officer should also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or pupils / parents) if a security breach occurs, the effect of any security breach on Stony Dean School itself, and any likely impact damages including the possible reputation damage.

  When assessing appropriate technical measures, the Data Protection Officer will consider the following:

- Password protection policies for all users in line with Stony Dean School Access Control Policy
- Encryption of sensitive personal data (Special category data)
- Automatic locking of idle terminals
- Removal of access rights for USB and other memory media
- Access rights of employees including those assigned to temporary staff
- Encryption of devices that leave the organisations premises such as laptops
- Security of local and wide area networks
- Privacy enhancing technologies such as pseudonymisation and anonymisation;
- Identifying appropriate international security standards relevant to Stony Dean School.
- Virus checking software and firewall protection

8. Disclosure of data

- Stony Dean School must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police unless there is a legal obligation to do so. All Employees/Staff should exercise caution when asked to disclose personal data held on another individual to a third party and will be required to attend specific training that enables them to deal effectively with any such risk. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of Stony Dean School business.
- All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Data Protection Officer.

9. Retention and disposal of data

- Stony Dean School shall not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.
- Stony Dean School may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

- The retention period for each category of personal data will be set out in the Retention of Records Procedure, along with the criteria used to determine this period including any statutory obligations Stony Dean School has to retain the data.
- Stony Dean School data retention and data disposal procedures (Storage Removal Procedure) will apply in all cases.
- Personal data must be disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of data subjects. Any disposal of data will be done in accordance with the secure disposal of storage media.

10. Transferring Personal Data

GDPR has stronger requirements on controllers transferring data to processors overseas. Stony Dean School will ensure that any data transfer is made securely with an appropriate strength encryption to protect the data in transit and must obtain appropriate guarantees that a processor will adhere to necessary levels of security.

The transfer of personal data outside of the EEA is should conform to one or more of the following specified safeguards:

- An adequacy decision The European Commission can and does assess third countries, a territory and/or specific sectors within third countries to assess whether there is an appropriate level of protection for the rights and freedoms of natural persons. In these instances no authorisation is required. Countries that are members of the European Economic Area (EEA) but not of the EU are accepted as having met the conditions for an adequacy decision. A list of countries that currently satisfy the adequacy requirements of the Commission are published in the *Official Journal of the European Union.* *http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm*
- Privacy Shield if Stony Dean School wishes to transfer personal data from the EU to an organisation in the United States it should check that the organisation is signed up with the Privacy Shield framework at the U.S. Department of Commerce. The obligation applying to companies under the Privacy Shield are contained in the "Privacy Principles". The US DOC is responsible for managing and administering the Privacy Shield and ensuring that companies live up to their commitments. In order to be able to certify, companies must have a privacy policy in line with the Privacy Principles e.g. use, store and further transfer the personal data according to a strong set of data protection rules and safeguards. The protection given to the personal data applies regardless of whether the personal data is related to an EU resident or not. Organisations must renew their "membership" to the Privacy Shield on an annual basis. If they do not, they can no longer receive and use personal data from the EU under that framework.

Assessment of adequacy by the data controller

In making an assessment of adequacy, the UK based exporting controller should take account of the following factors:

- the nature of the information being transferred;
- the country or territory of the origin, and final destination, of the information;
- how the information will be used and for how long;
- the laws and practices of the country of the transferee, including relevant codes of practice and international obligations; and
- the security measures that are to be taken as regards the data in the overseas location.

- Binding corporate rules Stony Dean School may adopt approved binding corporate rules for the transfer of data outside the EU. This requires submission to the relevant supervisory authority for approval of the rules that Stony Dean School is seeking to rely upon.

- Standard contract clauses

  Stony Dean School may adopt approved binding corporate rules for the transfer of data outside the EU. This requires submission to the relevant supervisory authority for approval of the rules that Stony Dean School is seeking to rely upon. may adopt approved model contract clauses for the transfer of data outside of the EEA. If Stony Dean School adopts the model contract clauses approved by the relevant supervisory authority there is an automatic recognition of adequacy. The GDPR allows standard contractual clauses from the EU Commission or a Supervisory Authority (such as the ICO) to be used in contracts between controllers and processors. However, no standard clauses are currently available.

- Exceptions

  In the absence of an adequacy decision, Privacy Shield membership, binding corporate rules and/or model contract clauses, a transfer of personal data to a third country or international organisation shall only take place on one of the following conditions:

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims; and/or
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

11. Personal Data

All Personal data is defined by the Act as data which relates to a living individual who can be identified from that data or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Special Category Data

Special category data will only be processed with a legitimate lawful basis for processing under Article 6, in exactly the same way as we do for personal data. Special category data will be recorded as such.

Special category data is more sensitive, and will be subject to further levels of protection such as access controls, encryption, etc. For example, information about an individual's:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health

Orchard End Avenue, Pineapple Road, Amersham, HP7 9JW Tel: 01494 762538 Fax: 01494 765631

www.stonydean.bucks.sch.uk

- sex life or sexual orientation.

Stony Dean School only holds personal data which is directly relevant to its dealings with a given data subject. That data will be held and processed in accordance with the data protection principles and with this Policy. The following data may be collected, held and processed by the Organisation from time to time:

- Full names of users
- Temporary passwords
- Dates of birth
- Home address details
- Private and work based telephone details
- Private and work based email addresses
- Names and ages of children
- Next of kin
- Contact details in cases of illness, etc.
- Disciplinary records
- Absence and attendance records
- Previous employment information
- Working hours

Orchard End Avenue, Pineapple Road, Amersham, HP7 9JW Tel: 01494 762538 Fax: 01494 765631

www.stonydean.bucks.sch.uk

12. Data Breach Notification

All personal data breaches must be reported immediately to the Company's data protection officer.

- If a personal data breach occurs and that breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay (e.g. financial loss, discrimination, reputational damage, breach of confidentiality etc.) the data protection officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

- In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the data protection officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

- Data breach notifications shall include the following information:

- The categories and approximate number of data subjects concerned;

- The categories and approximate number of personal data records concerned;

- The name and contact details of the Organisation's data protection officer (or other contact point where more information can be obtained);

- The likely consequences of the breach;

- Details of the measures taken, or proposed to be taken, by the Organisation to address the breach including, measures to mitigate its possible adverse effects and plan of action to prevent reoccurrence of a breach.
- The Data Protection Officer will keep records any personal data breaches, regardless of whether it affects individuals' rights and freedoms and whether a notification to data subjects is necessary.

13 Information Asset register

Stony Dean School has established a data inventory and data flow process as part of its approach to address risks and opportunities throughout its GDPR compliance project.

3.1 Stony Dean School is aware of any risks associated with the processing of particular types of personal data.

3.1.1 Stony Dean School assesses the level of risk to individuals associated with the processing of their personal data. Data protection impact assessments, DPIAs, (Data Protection Impact Assessment Procedure) are carried out in relation to the processing of personal data by Stony Dean School, and in relation to processing undertaken by other organisations on behalf of Stony Dean School.

3.1.2 Stony Dean School shall manage any risks identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy.

3.1.3 Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, Stony Dean School shall, prior to the processing, carry out a DPIA of the impact of the envisaged processing operations on the protection of personal data. A single DPIA may address a set of similar processing operations that present similar high risks.

3.1.4 Where, as a result of a DPIA it is clear that Stony Dean School is about to commence processing of personal data that could cause damage and/or distress to the data subjects, the decision as to whether or not Stony Dean School may proceed must be escalated for review to the Data Protection Officer/.

3.1.5 The Data Protection Officer shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the supervisory authority.

3.1.6 Appropriate controls will be selected and applied to reduce the level of risk associated with processing individual data to an acceptable level, by reference to Stony Dean School documented risk acceptance criteria and the requirements of the GDPR.

14 Organisational Measures

Stony Dean School shall ensure that the following measures are taken with respect to the collection, holding and processing of personal data:

A Data Protection Officer within the Organisation will be appointed with the specific responsibility of overseeing data protection and ensuring compliance with the Act.

- All employees, contractors, agents, consultants, partners or other parties working on behalf of the Organisation are made fully aware of both their individual responsibilities and the Organisation's responsibilities under the Act and shall be furnished with a copy of this Policy.

- All employees, contractors, agents, consultants, partners or other parties working on behalf of the Organisation handling personal data will be appropriately trained to do so.
- All employees, contractors, agents, consultants, partners or other parties working on behalf of the Organisation handling personal data will be appropriately supervised.
- Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed.
- The Performance of those employees, contractors, agents, consultants, partners or other parties working on behalf of the Organisation handling personal data shall be regularly evaluated and reviewed.
- All employees, contractors, agents, consultants, partners or other parties working on behalf of the Organisation handling personal data will be bound to do so in accordance with the principles of the Act and this Policy by contract. Failure by any employee to comply with the principles or this Policy shall constitute a disciplinary offence. Failure by any contractor, agent, consultant, partner or other party to comply with the principles or this Policy shall constitute a breach of contract. In all cases, failure to comply with the principles or this Policy may also constitute a criminal offence under the Act.
- All contractors, agents, consultants, partners or other parties working on behalf of the Organisation handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Organisation arising out of this Policy and the Act.
- Where any contractor, agent, consultant, partner or other party working on behalf of the Organisation handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Organisation against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

15 Notification to the Information Commissioner's Office

As a data controller, the Organisation is required to notify the Information Commissioner's Office that it is processing personal data. The Organisation is registered in the register of data controllers.

Data controllers must renew their notification with the Information Commissioner's Office on an annual basis. Failure to notify constitutes a criminal offence.

Any changes to the register must be notified to the Information Commissioner's Office within 28 days of taking place.

The Data Protection Officer is responsible for notifying and updating the Information Commissioner's Office.

16 Implementation of Policy

This Policy shall be deemed effective as of 25/05/2018. No part of this Policy shall have retroactive effect and will apply only to matters occurring on or after this date.

SECURITY INFORMATION FOR THIS DOCUMENT Owner of document	**This document is available to**	**Date of issue**	**Next review**
DPO	*All school stakeholders*	*26th March 2020*	*2 Year*

N. Strain — Approved By

26th March 2020 — Date