DATA PROTECTION POLICY

Policy Created: November 2011
Date Reviewed: November 2018
Review: As required

EXECUTIVE STATEMENT

At Sullivan Upper School (the "School"), we believe privacy is important. We are committed to complying with our data protection obligations and to being concise, clear and transparent about how we obtain and use Personal Information and how (and when) we delete that information once it is no longer required.

Sullivan Upper School is registered as a Data Controller with the Information Commissioners Office (ICO) on an annual basis**.** The school's registration number is Z7350535.

We will review and update this data protection policy (the "Policy") regularly in accordance with our data protection obligations.

Any queries in relation to this Policy or any of the matters referred to in it should be submitted to the Headmaster who will deal with your query. The Headmaster can be contacted via his Personal Assistant, Mrs Amanda Graham, by email agraham813@c2kni.net or by telephone on 028 9042 8780 or by post to Sullivan Upper School, Belfast Road, Holywood, BT18 9EP.

Anyone who works for, or acts on behalf of Sullivan Upper School (including staff, volunteers, Governors and service providers) should also be aware of and comply with this data protection policy and the relevant policies and privacy notices.

The following policies, procedures and documents are also relevant to this Policy:

- Disposal of Records Schedule
- E-Safety, ICT Acceptable Use and Digital Media Policy
- Bring your own Device Policy
- Privacy Notice for Alumni
- Privacy Notice for Applicants
- Privacy Notice for Non-Teaching Staff
- Privacy Notice for Pupils & Parents/Families/Carers/Legal Guardians
- Privacy Notice for Teaching Staff

DATA PROTECTION POLICY

1. SCOPE

1.1. The School is subject to the Data Protection Act (2018) and General Data Protection Regulation (GDPR) which impose obligations on the School as a data controller in relation to the protection, use, retention and disposal of Personal Information. This Policy sets out the procedures that are to be followed when dealing with Personal Information and applies to all Personal Information processed by or on behalf of Sullivan Upper School.

1.2. You must read this Policy because it gives important information about:

1.2.1. the data protection principles with which Sullivan Upper School must comply;

1.2.2. what is meant by Personal Information and Special Category Data;

1.2.3. how we gather, use and (ultimately) delete Personal Information and Special Category Data in accordance with the data protection principles;

1.2.4. where more detailed Privacy Information can be found, eg about the Personal Information we gather and use about you, how it is used, stored and transferred, for what purposes, the steps taken to keep that information secure and for how long it is kept;

1.2.5. your rights and obligations in relation to data protection; and

1.2.6. the consequences of our failure to comply with this Policy.

1.3. Please refer to the School's privacy notices available on the school's website and/or staff intranet:

1.3.1. Privacy Notice for Applicants
1.3.2. Privacy Notice for Non-Teaching Staff
1.3.3. Privacy Notice for Pupils & Parents/Families/Carers/Legal Guardians
1.3.4. Privacy Notice for Teaching Staff
1.3.5. Disposal of Records Schedule

2. DATA PROTECTION PRINCIPLES

2.1. GDPR sets out the following principles with which any party handling Personal Information must comply. All Personal Information must be:

2.1.1. processed lawfully, fairy and in a transparent manner;

2.1.2. collected for specified, explicit and legitimate purposes only, and will not be further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

2.1.3. adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

2.1.4. accurate and, where necessary, kept up to date and take reasonable steps to ensure that inaccurate Personal Information are deleted or corrected without delay;

2.1.5. kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the information is processed; Personal Information may be stored for longer periods insofar as the data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes subject to implementation of the appropriate technical and organisational measures required by GDPR in order to safeguard the rights and freedoms of the individual; and

2.1.6. processed in a manner than ensures appropriate security of the Personal Information, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3. LAWFUL, FAIR AND TRANSPARENT PROCESSING

3.1. The School will, before any processing of Personal Information starts for the first time, and then regularly while it continues:

3.1.1. process the Personal Information on at least one of the following bases:

3.1.1.1. **Consent:**

- the individual has given their express agreement to the processing of their Personal Information for one or more specific purposes;
- parental consent will be obtained for any child aged under 13 years old or for children aged over 13 who are not considered capable of giving consent themselves.

3.1.1.2. **Contractual**:

- the processing is necessary for the performance of a contract to which the individual is party or in order to take steps at the request of the individual prior to entering into a contract;

3.1.1.3. **Legal Obligation**:

- the processing is necessary for compliance with a legal obligation to which the School is subject;

3.1.1.4. **Vital Interests**:

- the processing is necessary for the protection of the vital interests of the individual or another natural person; or

3.1.1.5. **Public Interest**:

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

3.1.1.6. **Legitimate Interests**:

- the processing is necessary for the purposes of legitimate interests of the School or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the individual, in particular where the individual is a child.

3.1.2. except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose);

3.1.3. document our decision as to which lawful basis applies to help demonstrate our compliance with the data protection principles;

3.1.4. include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notices:

- Privacy Notice for Applicants *(available at www.sullivanupper.co.uk)*
- Privacy Notice for Non-Teaching Staff *(available in staff shared resources area)*
- Privacy Notice for Pupils & Parents/Families/Carers/Legal Guardians *(available at www.sullivanupper.co.*uk)
- Privacy Notice for Teaching Staff *(available in staff shared resources area)*

3.1.5. where Special Category Data is processed, identify a lawful special condition for processing that information and document it; and

3.1.6. where criminal offence information is processed, identify a lawful condition for processing that information and document it.

4. RIGHTS OF THE INDIVIDUAL

4.1. The GDPR states that individuals have the following rights in respect of the processing of their Personal Information:

4.1.1. **The right to be informed**:

4.1.1.1. The School will keep individuals informed of its processing activities through its privacy notices **– see above.**

4.1.2. **The right of access**:

4.1.2.1. An individual may make a subject access request ("**SAR**") at any time to find out more about the Personal Information which the School holds on them. All SARs must be forwarded to the the Headmaster. The Headmaster can be contacted via his personal assistant, Mrs Amanda Graham, by email at agraham813@c2kni.net or by telephone on 028 9042 8780 or by post to Sullivan Upper School, Belfast Road, Holywood, BT18 9EP. The School is required to respond to a SAR within one month of receipt but this can be extended by up to two months in the case of complex and/or numerous requests and, in such cases, the individual will be informed of the need for such extension. The School does not charge a fee for the handling of a straightforward SAR.

4.1.3. **The right to rectification**:

4.1.3.1. If an individual informs the School that Personal Information held by the School is inaccurate or incomplete, the individual can request that it is rectified.

4.1.4. **The right to erasure**:

4.1.4.1. An individual is entitled to request that the School ceases to hold Personal Information it holds about them.

4.1.4.2. The School is required to comply with a request for erasure unless the School has reasonable grounds to refuse.

4.1.5. **The right to restrict processing**:

4.1.5.1. An individual is entitled to request that the School stops processing the Personal Information it holds about them in certain circumstances.

4.1.6. **The right to data portability:**

4.1.6.1. An individual has the right to receive a copy of their Personal Information and use it for other purposes.

4.1.7. **The right to object:**

4.1.7.1. An individual is entitled to object to the School's processing of their Personal Information.

4.1.8. **Rights in relation to automated decision making and profiling:**

4.1.8.1. An individual has the right to challenge any decision that is made about them on an automated basis (subject to certain exceptions).

4.1.8.2. The School is also required to comply with certain conditions if it uses Personal Information for profiling purposes.

5. STAFF RESPONSIBILITIES

5.1. Everyone who works for, or on behalf of, the School has responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and the School's Data Retention Schedule.

5.2. Throughout the course of working with the school, staff will have access to various extracts of Personal Data pertaining to Staff/students, depending on the nature of their role. Staff must adhere to all Data Protection related policies and procedures to ensure the confidentiality, integrity and availability of personal data.

5.3. All Staff must complete mandatory training on GDPR and adhere to regular information updates on new policies and procedures as they become operational.

5.4. Compliance is the responsibility of all staff. Any breach of this Data Protection Policy may lead to disciplinary action being taken, access to school information facilities being withdrawn, or in substantial cases, a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up initially with the Headmaster.

5.5. The Headmaster and Bursar are responsible for reviewing this policy and updating the Board on the School's data protection responsibilities and any risks in relation to the processing of data. You should direct any questions in relation to this policy or data protection to them.

5.6. You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of the School and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.

5.7. You should not share personal data informally.

5.8. You should keep personal data secure and not share it with unauthorised people.

5.9. You should regularly review and update personal data which you have to deal with for work. This includes telling us if your own contact details change.

5.10. You should not make unnecessary copies of personal data and should keep and dispose of any copies securely when you have finished with the data eg at the end of a school trip.

5.11. You should use strong passwords.

5.12. You should lock your computer screens when not at your desk.

5.13. Personal data should be encrypted before being transferred electronically to authorised external contacts. Please speak to ICT Systems Support Officer for more information on how to do this.

5.14. Consider anonymising data or using separate keys/codes so that the data subject cannot be identified.

5.15. Do not save personal data to your own personal computers or other devices.

5.16. Personal data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of the Headmaster.

5.17. You should lock drawers and filing cabinets. Do not leave paper with personal data lying about. **Cover it/Lock it/Shred it.**

5.18. If you are taking personal data home or off-site (pupil exam scripts/pupil details/recruitment files etc.) – you have a duty to protect this eg use of locked briefcase. Personal data must not be left in cars and should be locked in the car boot for the journey home and kept securely at home with access restricted to authorised staff.

5.19. Personal data should be shredded and disposed of securely when you have finished with it – see the Disposal of Records Schedule.

5.20. You should ask for help from the Headmaster/Bursar if you are unsure about data protection or if you notice any areas of data protection or security which we can improve upon.

5.21. Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you in accordance with our disciplinary procedure.

5.22. It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.

6. DATA SUBJECT RESPONSIBILITIES

6.1. As Data Subjects, all employees, workers, contractors, agency workers, consultants, governors, pupils, parents/guardians/ are responsible for:

- ensuring that any personal information they provide to the school in connection with their employment, enrolment/attendance or other contractual agreement is accurate;
- informing the school of any changes to any personal information which they have provided, eg changes of address, bank details;
- responding to requests to check the accuracy of the personal information held on them and processed by the school and informing the school.

6.2. The school cannot be held responsible for any errors unless the data subject has informed the school of the changes of any errors or changes to be made.

7. DATA PROTECTION OFFICER

7.1. A Data Protection Officer (DPO) is appointed who will monitor adherence to this policy.

7.2. Our Data Protection Officer is the Education Authority and it monitors the school's data protection procedures to ensure they meet the standards and requirements of the GDPR. Please contact the Education Authority (Data Protection Officer) at:

Email: dpo@eani.org.uk
Tel: 028 8241 1300

7.3. The DPO is required to have an appropriate level of knowledge.

8. PRIVACY BY DESIGN

8.1. The School has adopted the principle of privacy by design and will ensure that the definition and planning of all new or significantly changed systems that collect or process Personal Information will be subject to due consideration of privacy issues, including the completion of one or more data protection impact assessments.

8.2. The data protection impact assessment will include:

8.2.1. Consideration of how Personal Information will be processed and for what purposes;

8.2.2. Assessment of whether the proposed processing of Personal Information is both necessary and proportionate to the purpose(s);

8.2.3. Assessment of the risks to individuals in processing the Personal Information;

8.3. What controls are necessary to address the identified risks and demonstrate compliance with legislation.

8.4. A data protection impact assessment is conducted by the Headmaster:

8.4.1. On every business process periodically, at least once a year and more frequently where the amount and/or sensitivity of Personal Information processed, dictates so;

8.4.2. As part of the project calendar admission requirements checklist;

8.4.3. At every high-impact change, and/or at the request of the Data Protection Officer.

9. CCTV

The school's CCTV system is set up to monitor specific areas of the school and not to monitor individuals. All employees, students and visitors should have a reasonable expectation of being captured on CCTV on a daily basis. The use of CCTV is for the following purposes:

- deterring, prevention and detection of a crime including misuse/abuse of school property.
- identification, apprehension and prosecution of offenders.
- security of school buildings and grounds.
- safeguarding/health and safety.

Access to the recorded images is restricted to the Headmaster, Facilities Manager, Vice-Principal and such other members of staff as may be required to assist in the solution of pastoral or disciplinary issues.

Recorded images will not normally be copied onto transferable media except (i) where the image is to be supplied to PSNI in order to assist with official Police investigations (ii) where the image is to be supplied to the school's insurers/legal/professional team when it is in the school's legitimate interests for example - to seek advice to clarify our rights and obligations and appropriately defend ourselves from potential claims or when it is necessary to establish, exercise or defend legal claims.

10. DATA RETENTION & DISPOSAL

10.1. The longer that Personal Information is retained, the higher the likelihood is accidental disclosure, loss, theft and/or information growing stale.

10.2. Any Personal Information kept by the School is managed in accordance with the School's Disposal of Records Schedule.

11. DATA BREACH

11.1. A data breach is any (potential) unintended loss of control over or loss of Personal Information within the School's environment. Preventing a data breach is the responsibility of all the School staff and its workforce.

11.2. Please refer to the School's Data Breach Management Procedure.

12. THIRD-PARTY SERVICES AND SUBCONTRACTING

12.1. The School may decide to contract with a third party for the collection, storage or processing of data, including Personal Information (for example - Parentmail (email communication with parents), Infineer (cashless catering system), Midyis and Yellis (standardised test providers).

12.2. If the School decides to appoint a third party for the processing of Personal Information, this must be regulated in a written agreement in which the rights and duties of the School and of the subcontractor are specified. A subcontractor shall be selected that will guarantee the technological and organisational security measures required in this Policy, and provide sufficient guarantees with respect to the protection of the personal rights and the exercise of those rights.

12.3. The subcontractor is contractually obligated to process Personal Information only within the scope of the contract and the directions issued by the School.

13. INTERNATIONAL TRANSFERS OF DATA

13.1. Under the GDPR, transfers of personal data to countries outside the EEA (that means the European Union, Iceland, Liechtenstein and Norway) are restricted to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. Personal Data is transferred out of the EEA it is transmitted, sent, viewed or accessed in or to a different country.

13.2. Any transfers of Personal Information outside of the EEA will be carefully reviewed before any transfer takes place to ensure they fall within the limits imposed by the GDPR. This depends partly on the European Commission's judgement as to the adequacy of the safeguards for personal data applicable in the receiving country and this may change over time.

14. COMPLAINTS

14.1. Complaints will be dealt with in line with the School's complaints policy.

14.2. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues. The ICO's details are as follows:

The Information Commissioner's Office – Northern Ireland
3rd Floor
14 Cromac Place
BELFAST
BT7 2JB

Telephone: 028 9027 8757 / 0303 123 1114
Email: ni@ico.org.uk

15. DEFINITIONS

"consent"	is any freely given, specific and transparently, well-informed indication of the will of the individual, whereby the individual agrees that his or her Personal Information may be processed. Particular requirements about consent can arise from the respective national laws.
"Personal Information"	(sometimes known as "personal data") means any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly — in particular, by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.
"processing"	means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with Personal Information.
"Special Category Data"	(sometimes known as "sensitive personal data") means Personal Information that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric data and the processing of data concerning health or sex life.