Stratford College
Co-educational Secondary School

Data Protection Policy & Appendices

APPENDICES:

Policies & Statements

- *Data Protection Terms, Definitions & Legal Obligations*
- *Records Retention Schedule*
- *CCTV Policy*
- *Privacy Statement - Students & Parents / Guardians*
- *Privacy Statement - Staff*
- *Privacy Statement – School Website*

Forms

- *Personal Data Access Request Form*
- *Personal Data Rectification or Erasure Form*
- *Department of Education and Skills Student Enrolment Returns Form*
- *Data Protection Statement Consent Form for inclusion on relevant forms when personal information is being requested*
- *Data Protection Impact Assessment Form*

Procedural Protocol

- *Personal Data Access Request (DAR)*
- *Personal Data Rectification or Erasure Request*
- *Breach of Personal Data Response Plan*
- *Transfer of Student Personal Data*

Table of Contents

Table of Contents 2
Introduction 3
Scope 3
Objectives of this Policy 3
Rationale 3
Our Mission 4
Personal Data and Sensitive Personal Data (“Data”) 4
CCTV Images/Recordings 7
Examination Results 7
October Returns 8
Application of the Data Protection Principles to the Personal Data obtained and held 8
Data Access Requests (“DAR”) 11
Third Party Agreements 14
Transfer of Data 15
Breach of Data 15
Data Protection Impact Assessments 15
Data Protection Rights 16
Implementation Arrangements, Roles and Responsibilities 16

Introduction

Stratford College's Data Protection Policy applies to the personal data held by the school which is protected by the Data Protection Acts 1988 to 2018, EU Data Protection Directive 95/46/EC and EU GDPR 2018.

The policy applies to all school staff, the board of management, parents/guardians, students and others (including prospective or potential students and their parents/guardians and applicants for staff positions within the school) insofar as the measures under the policy relate to them. Data will be stored securely, so that confidential information is protected in compliance with relevant legislation. This policy sets out the manner in which personal data and sensitive personal data will be protected by the school.

Scope

The Data Protection Acts 1988 to 2018 apply to the keeping and processing of *Personal Data and Personal Sensitive Data*, both in manual and electronic form. The purpose of this policy is to assist Stratford College to meet its' statutory obligations, to explain those obligations to School staff, and to inform staff, students and their parents/guardians how their data will be treated.

The policy applies to all school staff, the board of management, parents/guardians, students and others (including prospective or potential students and their parents/guardians, and applicants for staff positions within the school) insofar as the school handles or processes their *Personal Data* in the course of their dealings with the school.

This policy relates to the retention, use and dissemination of information of records, held in written or electronic format.

In the spirit of a caring and supportive community Stratford College aims to ensure that a system of record keeping is established and maintained which supports the teaching and learning process and recognises the value of good communication. Such a policy will also promote a sense of community with teachers, students and parents adopting a partnership approach.

Objectives of this Policy

- Excellent communication based on factual and accurate data will be a feature of the school
- The school will meet statutory requirements under the relevant areas of legislation
- Clarity will exist in the school community in relation to a system of record keeping including creation, maintenance, use of, storage and access.
- The school will ensure that the information kept in individual student's records is accurate and secure and conforms to the terms of this policy
- Parents and guardians and students over the age of 18 will have their requests for review of their records dealt with in accordance with this policy.

Stratford College is a data controller of Personal Data relating to its past, present and future staff, students, parents/guardians and other members of the School community. As such, Stratford College is obliged to comply with the principles of data protection set out in the Data Protection Acts 1988, 2003 and GDPR 2018.

Rationale

In addition to its legal obligations under the broad remit of educational legislation, Stratford College has a legal responsibility to comply with the Data Protection Acts, 1988, 2003 and GDPR 2018.

This policy explains what sort of data is collected, why it is collected, for how long it will be stored and with whom it will be shared. As more and more data is generated electronically and as technological advances enable the easy distribution and retention of this data, the challenge of meeting the school's legal responsibilities has increased.

Stratford College takes its responsibilities under data protection law very seriously and wishes to put in place safe practices to safeguard individual's personal data. It is also recognised that recording factual information accurately and storing it safely facilitates an evaluation of the information, enabling the principal and board of management to make decisions in respect of the efficient running of the School. The efficient handling of data is also essential to ensure that there is consistency and continuity where there are changes of personnel within the school and board of management.

Our Mission

Stratford College aims to provide a teaching and learning community committed to quality and excellence in education by:

- Promoting personal achievement and academic success
- Respecting the unique potential of every student and encouraging each student to maximise it

We aim to achieve these goals while respecting the privacy and data protection rights of students, staff, parents/guardians and others who interact with us. The school wishes to achieve these aims/missions while fully respecting individuals' rights to privacy and rights under the Data Protection Acts.

Personal Data and Sensitive Personal Data ("Data")

The Data records held by the school **may** include:

A. Staff records:

(a) **Categories of staff data**: As well as existing members of staff (and former members of staff), these records may also relate to applicants applying for positions within the school, trainee teachers and teachers under probation. These staff records may include:
- Name, address and contact details, PPS number
- Original records of application and appointment to promotion posts
- Details of approved absences (career breaks, parental leave, study leave etc.)
- Details of work record (qualifications, classes taught, subjects etc.)
- Details of any accidents/injuries sustained on school property or in connection with the staff member carrying out their school duties
- Records of any reports the school (or its employees) have made in respect of the staff member to State departments and/or other agencies under mandatory reporting legislation and/or child-safeguarding guidelines (subject to the DES Child Protection Procedures).

(b) **Purposes**: Staff records are kept for the purposes of:
- the management and administration of school business (now and in the future)
- to facilitate the payment of staff, and calculate other benefits/ entitlements (including reckonable service for the purpose of calculation of pension payments, entitlements and/or redundancy payments where relevant)
- to facilitate pension payments in the future
- human resources management

- recording promotions made (documentation relating to promotions applied for) and changes in responsibilities etc.
- to enable the school to comply with its obligations as an employer including the preservation of a safe, efficient working and teaching environment (including complying with its responsibilities under the Safety, Health and Welfare At Work Act. 2005)
- to enable the school to comply with requirements set down by the Department of Education and Skills, the Revenue Commissioners, the National Council for Special Education, TUSLA, the HSE, and any other governmental, statutory and/or regulatory departments and/or agencies
- and for compliance with legislation relevant to the school.

(c) **Location & Security.** All manual records are kept **i**n a secure, locked filing cabinet that only personnel who are authorised to use the data can access. All soft copy records are password protected in folders with firewall software measures in effect. All records that are required to be retained under legislation for a specific period of time are kept in an Archives Room which is locked at all times and can only accessed by authorised personnel. All employees are required to maintain the confidentiality of any data to which they have access.

B. Student records:

(a) **Categories of student data**: These **may** include:

- Information which may be sought and recorded at enrolment and may be collated and compiled during the course of the student's time in the school. These records may include:
  - name, address and contact details, PPS number
  - date and place of birth
  - names and addresses of parents/guardians and their contact details (including any special arrangements with regard to guardianship, custody or access)
  - religious belief
  - racial or ethnic origin
  - membership of the Traveller community, where relevant
  - whether they (or their parents) are medical card holders
  - whether English is the student's first language and/or whether the student requires English language support
  - any relevant special conditions (e.g. special educational needs, health issues etc.) which may apply
- Information on previous academic record (including reports, references, assessments and other records from any previous school(s) attended by the student
- Psychological, psychiatric and/or medical assessments
- Attendance records
- Photographs and recorded images of students (including at school events and noting achievements).
- Academic record – subjects studied, class assignments, examination results as recorded on official School reports
- Records of significant achievements
- Whether the student is repeating the Leaving Certificate
- Whether the student is exempt from studying Irish
- Records of disciplinary issues/investigations and/or sanctions imposed
- Garda vetting outcome record (where the student is engaged in work experience organised with or through the school/ETB which requires that they be Garda vetted)
- Other records e.g. records of any serious injuries/accidents etc.
- Records of any reports the school (or its employees) have made in respect of the student to State departments and/or other agencies under mandatory reporting legislation and/or child safeguarding guidelines (subject to the DES Child Protection Procedures).

(b) **Purposes**: The purposes for keeping student records are:

- to enable each student to develop to their full potential
- to comply with legislative or administrative requirements
- to ensure that eligible students can benefit from the relevant additional teaching or financial supports
- to support the provision of religious instruction
- to enable parents/guardians to be contacted in the case of emergency or in the case of school closure, or to inform parents of their child's educational progress or to inform parents of school events etc.
- to meet the educational, social, physical and emotional requirements of the student
- photographs and recorded images of students are taken to celebrate school achievements, compile yearbooks, establish a school website, record school events, and to keep a record of the history of the school. Such records are taken and used in accordance with the school's "Guidance for Taking and Using Images of Pupils in Schools" (see template)
- to ensure that the student meets the school's admission criteria
- to ensure that students meet the minimum age requirements for their course,
- to ensure that any student seeking an exemption from Irish meets the criteria in order to obtain such an exemption from the authorities
- to furnish documentation/ information about the student to the Department of Education and Skills, the National Council for Special Education, TUSLA, and other Schools etc. in compliance with law and directions issued by government departments
- to furnish, when requested by the student (or their parents/guardians in the case of a student under 18 years) documentation/information/ references to third-level educational institutions and/or prospective employers
- In respect of a work experience placement, (where that work experience role requires that the student be Garda vetted) the School will assist the student in obtaining their Garda vetting outcome (with the consent of the student and their parent/guardian) in order to furnish a copy of same (with the consent of the student and the student's parent/guardian) to the work experience employer.

(d) **Location & Security.** All manual records are kept **i**n a secure, locked filing cabinet that only personnel who are authorised to use the data can access. All soft copy records are password protected in folders with firewall software measures in effect. All records that are required to be retained under legislation for a specific period of time are kept in an Archives Room which is locked at all times and can only accessed by authorised personnel. All employees are required to maintain the confidentiality of any data to which they have access.

C. Board of Management Records:

(a) **Categories of** board of management data: These may include:

- Name, address and contact details of each member of the board of management (including former members of the board of management)
- Records in relation to appointments to the Board
- Minutes of Board of Management meetings and correspondence to the Board which may include references to particular individuals.
-

(b) **Purposes:** To enable the Board of Management to operate in accordance with the Education Act 1998 and other applicable legislation and to maintain a record of board appointments and decisions.

(a) **Location & Security.** All manual records are kept **i**n a secure, locked filing cabinet that only personnel who are authorised to use the data can access. All soft copy records are password protected in folders with firewall software measures in effect. All records that are required to be retained under legislation for a specific period of time are kept in an Archives Room which is locked at all times and can only accessed by authorised

personnel. All employees are required to maintain the confidentiality of any data to which they have access.

D. Other records:

The school will hold other records relating to individuals. The format in which these records will be kept are manual record (personal file within a relevant filing system), and/or computer record (database). Some examples of the type of other records which the school will hold are set out below (this list is not exhaustive):

Creditors

(a) **Categories of data**: the school may hold some or all of the following information about creditors (some of whom are self-employed individuals):
- name
- address
- contact details
- PPS number
- tax details
- bank details and
- amount paid.

(b) **Purposes**: This information is required for routine management and administration of the school's financial affairs, including the payment of invoices, the compiling of annual financial accounts and complying with audits and investigations by the Revenue Commissioners.

(a) **Location & Security.** All manual records are kept **i**n a secure, locked filing cabinet that only personnel who are authorised to use the data can access. All soft copy records are password protected in folders with firewall software measures in effect. All records that are required to be retained under legislation for a specific period of time are kept in an Archives Room which is locked at all times and can only accessed by authorised personnel. All employees are required to maintain the confidentiality of any data to which they have access.

CCTV Images/Recordings

Closed Circuit Television Systems (CCTVS) are installed in Stratford College, on the premises at No. 1, Zion Road, Rathgar, Dublin 6. Fourteen (14) cameras are located externally and internally. Recording equipment is located in the Bursar's Office. .Any new CCTV systems will be introduced in consultation with staff, the Board of Management and the Parents Association. A comprehensive separate policy on CCTV is maintained by Stratford College and attached to this Data Protection Policy as an Appendix.

Examination Results

(a) **Categories**: The school will hold data comprising examination results in respect of its students. These include class, mid-term, annual, continuous assessment and mock-examinations results.

(b) **Purposes**: The main purpose for which these examination results and other records are held is to monitor a student's progress and to provide a sound basis for advising them and their parents or guardians about subject choices and levels. The data may also be aggregated for statistical/reporting purposes, such as to compile results tables. The data may be transferred to the Department of Education and Skills, the National Council for Curriculum and Assessment and such other similar bodies.

(c) **Location & Security.** All manual records are kept **i**n a secure, locked filing cabinet that only personnel who are authorised to use the data can access. All soft copy records are password protected in folders with firewall software measures in effect. All records that are required to be retained under legislation for a specific period of time are kept in an Archives Room which is locked at all times and can only accessed by authorised

personnel. All employees are required to maintain the confidentiality of any data to which they have access.

October Returns

(a) **Categories**: At the beginning of each academic year (and for 1st year or transferring students, on enrolment) parents/guardians and students are asked to provide the school with certain information so that the School can make returns to the Department of Education and Skills ("DES") referred to as "October Returns". These October Returns will include sensitive personal data regarding personal circumstances which are provided by parents/guardians and students on the basis of explicit and informed consent. The October Return contains individualised data (such as an individual student's PPS number) which acts as an "identifier" for the DES to validate the data that belongs to a recognised student. The DES also transfers some of this data to other government departments and other State bodies to comply with legislation, such as transfers to the Department of Social Protection pursuant to the Social Welfare Acts, transfers to the State Examinations Commission, transfers to the Educational Research Centre, and transfers to the Central Statistics Office pursuant to the Statistics Acts. The data will also be used by the DES for statistical, policy-making and research purposes. However the DES advises that it does not use individual data, but rather aggregated data is grouped together for these purposes. The DES has a data protection policy which can be viewed on its website (www.education.ie). The DES has also published a "Fair Processing Notice" to explain how the personal data of students and contained in October Returns is processed. This can also be found on www.education.ie (search for Circular Letter 0047/2010 in the "Circulars" section).

(b) **Purposes:** The school asks parents/guardians and students to complete October Returns for the purposes of complying with DES requirements to determine staffing and resource allocations and to facilitate the orderly running of the school. The main purpose of the October Returns is for the DES to determine whether the student qualifies for English language support and/or additional resources and support to meet their particular educational needs. The October Returns are submitted to the DES electronically. The DES has their own policy governing the security of the data sent to them by all post-primary schools. The co-operation of each student and/or their parents/guardians in completing the October Return is greatly appreciated as the school's aim is to ensure that each student is assisted in every way to ensure that s/he meets his/her full potential.

(c) **Location & Security.** All manual records are kept in a secure, locked filing cabinet that only personnel who are authorised to use the data can access. All soft copy records are password protected in folders with firewall software measures in effect. All records that are required to be retained under legislation for a specific period of time are kept in an Archives Room which is locked at all times and can only accessed by authorised personnel. All employees are required to maintain the confidentiality of any data to which they have access.

Application of the Data Protection Principles to the Personal Data obtained and held

This policy sets down the arrangements in place to ensure that all Personal Data records held by Stratford College are obtained, processed, used and retained in accordance with the following eight rules of data protection (based on the Data Protection Acts).

Data Protection Principles:

- Obtain and process the information fairly
- Keep it only for one or more specified and law purpose
- Process it only in ways compatible with the purposes for which it was given to you initially
- Keep it accurate and up-to-date

- Keep it safe and secure
- Ensure that it is adequate, relevant and not excessive
- Retain it no longer than is necessary for the specified purpose or purposes
- Give a copy of his/her personal data to any individual, on request

Note: While these rules apply to all computer-held data and any new manual records created from July 2003, they only apply to existing manual records from October 2007.

1. Obtain and process Personal Data fairly

Stratford College will ensure that data subjects (staff, students, parents, board of management members, etc.) are aware, at the time the personal data is being collected, of the following information:

- the name of the school (the "data controller")
- the purpose of collecting the data
- the persons or categories of persons to whom the data may be disclosed
- whether replies to questions asked are obligatory and the consequences of not providing replies to those questions
- the existence of the right of access to their Personal Data
- the right to rectify or delete their data if inaccurate, excessive or processed unfairly
- any other information which is necessary so that processing may be fair and to ensure the data subject has all the information that is necessary so as to be aware as to how their data will be processed.

Please note that the Freedom of Information Act, 1997 does not apply to schools, including Stratford College. However, if Stratford College has furnished information to a body covered by the Freedom of Information Act (such as the Department of Education and Skills, etc.), these records could be disclosed if a request is made to that body.

In the case of Sensitive Personal Data, explicitly given consent is required unless consent may be implied to be given, for example where it is necessary:

- urgently to prevent injury or other damage to the health of a person or to prevent serious loss or damage to property
- for the purpose of obtaining legal advice or in the course of legal proceedings in which the person doing the processing is a party or witness
- required by or under any enactment or by a rule of law or court order.

The minimum age at which consent can be legitimately obtained for processing and disclosure of personal data is not defined in the Data Protection Acts. However, the Data Protection Commissioner recommends the following model as a general rule for processing data:

- A student aged eighteen or older (so long as they do not suffer from a disability or medical condition that would impair their ability to understand the implications of their giving consent) may give consent themselves.

- If a student (aged 18 and over) has some disability or medical condition that would impair their ability to understand the implications of their giving consent, then parental/guardian consent should be sought.

- A student aged from twelve up to and including seventeen should give consent themselves and, in addition, consent should also be obtained from the student's parent or guardian. Consent may not be considered to be in place for processing of personal data for students in this age unless it is given by both the student and a parent/guardian.

In all cases where Stratford College is asked to assist a student in obtaining their Garda vetting clearance (e.g. for the student to participate in work experience placement which requires that the student be Garda vetted), the school will obtain the explicit written consent of the student and their parent/guardian as part of the Garda Vetting application and must obtain

the explicit, written consent of the student and their parent/guardian for the Garda vetting outcome report being transferred to the prospective work experience employer.

2. Keep it only for one or more specified, explicit and lawful purposes

Stratford College will ensure that:

- the persons whose data is collected knows the reason/s why it is collected and kept
- the purpose for which the data is collected and kept is a lawful one
- that school management are aware of the different sets of data which are kept and the specific purpose of each

3. Use and disclose it only in ways compatible with these purposes

- That data is used only in ways consistent with the purpose/s for which it was obtained
- That data is disclosed only in ways consistent with that purpose
- That there is a procedure in place, which is in accordance with the Data Protection Acts, facilitates the transfer of information to another school when a student transfers

4. Keep it safe and secure

Appropriate security measures have been taken against unauthorised access to, or alteration, disclosure or destruction of any and all data obtained and kept and against their accidental loss or destruction, including the following:

- access to the information (including authority to add/amend/delete records) is restricted to authorised staff on a "need to know" basis
- access to what information based on a "need to know" policy
- computer systems are password protected, encrypted and protected by up-to-date anti-virus and firewall software
- information on computer screens and manual files is kept out of view of callers to the school/office
- back-up procedures are in operation for computer held data, including off-site back-up
- all reasonable measures are taken to ensure that staff are made aware of the security measures and comply with them
- all waste papers, printouts etc. are disposed of carefully
- no unauthorised person can access data from computers which are no longer in use or subject to change of use
- a designated person is responsible for data security and periodic reviews of the measures and practices takes place
- the school premises are secure when unoccupied
- a contract is in place with any data processor which imposes an equivalent security obligation on the data processor
- Stratford College staff know what to do if there is a breach of data

5. Keep it accurate, complete and up-to-date

- All clerical and computer procedures are adequate to ensure high levels of data accuracy
- appropriate procedures are in place, including periodic review and audit, to ensure that each data item is kept up-to-date
- Up-to-date information is obtained from the appropriate source in the context of the particular family arrangements of that student.

6. Ensure that it is adequate, relevant and not excessive

Stratford College will take all steps possible and maintains a records retention schedule to ensure that:

- the information held is adequate in relation to the purpose/s for which it is kept
- the information held is relevant in relation to the purpose/s for which it is kept
- the information held is not excessive in relation to the purpose/s for which it is kept

7. Retain it for no longer than is necessary for the purpose or purposes

- Stratford College maintains a defined Records Retention Schedule for the retention periods for all items of Personal Data kept

- That appropriate management, clerical and computer procedures are in place to implement such the policy
- That a safe disposal/safe destruction policy is in place for data which is being purged

8. Give a copy of their Personal Data to that individual on request

On making an access request any individual, subject to the restrictions set out in Data Protection legislation, about whom a school keeps Personal Data, is entitled to:

- a copy of the data which is kept about him/her (unless one of the exemptions or prohibitions under the Acts applies in which case the individual will be notified of this and informed of their right to make a complaint to the Data Protection Commissioner)
- know the purpose/s for processing their data
- know the identity or categories of those to whom the data is disclosed
- know the source of the data, unless it is contrary to the public interest
- where the processing is by automated means

Details of all restrictions / exceptions to data to be provided is set out in the Data Access Requests section of this policy.

All access requests must be made in writing in writing to The Principal using the Data Access Request Form, attached as an appendix to this policy. All access requests will be handled promptly and responded to within the timeframe set out under data protection legislation.

Proof of identity will be required in order to access Personal Data.

Procedures are in place to ensure that all relevant manual files and computers are checked for the data in respect of which the access request is made. Procedures are also in place to rectify or erase any inaccurate, unfairly collected or excessive information, as identified by the individual on whom the data is kept, within the required time period (40 days of receiving the request or, in respect of examinations data, within 60 days of receiving the request or 60 days of first publication of the results (whichever is the later)/

Data Access Requests ("DAR")

Data access requests in Stratford College will be processed in line with the data subjects' rights. Data subjects have a right to:

(a) Request access to any data held about them by a data controller
(b) Prevent the processing of their data for direct-marketing purposes
(c) Ask to have inaccurate data amended
(d) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

The following Data Protection restrictions apply:

Access Requests by Students: Age of Consent for Access Requests

In relation to access requests made by a student, the Office of the Data Protection Commissioner has recommended that the following guidance be followed as a general rule:

- A student **aged eighteen years or older** (and not suffering under any medical disability or medical condition which may impair his or her capacity to give consent) may give consent themselves
- If a student **aged eighteen years or older** has some disability or medical condition which may impair his or her ability to understand the information, then parental/guardian consent will be sought by the school before releasing the data to the student.
- A student aged from **twelve up to and including seventeen** can be given access to their personal data, depending on the age of the student and the nature of the record, i.e. it is suggested that:
    - If the information is ordinary, routine or non-controversial (e.g. a record of a test result) the student could readily be given access

- If the information is of a sensitive nature, it would be prudent to seek parental/guardian consent in writing before releasing the data to the student. Where the parent/guardian does not give their consent to releasing the data to the student, legal advice should be sought
- If the information would be likely to be harmful to the individual concerned, parental/guardian consent should be sought before releasing the data to the student.

Copy to Parents where Students Make Access Request
Where an access request is made by a student under 18 years, Stratford College will inform the student that:

a) Where they make an access request, their parents will be informed that they have done so
b) A complete copy of the access request materials being furnished to the data subject by Stratford College will also be furnished to the student's parent/guardian.

Parental Access Requests

A parent/guardian may make an access request asking for their child's data. At all times that the right of access is a right of the data subject, the student, and therefore the parent/guardian is making the request on behalf of the student. In such a case, the access materials should be sent to the child, not to the parent who requested them. This means that the documentation should be sent to the address at which the child is registered on the school's records, and should be addressed to the child. The documentation should not be sent to or addressed to the parent/guardian who made the request.

Where parents are separated/estranged, the access materials will still be sent to the student, not to the parent who requested them. Stratford College may invite the parent to make an application under Section 11 Guardianship of Infants Act 1964 which enables the court (on application by a guardian) to make a direction on any question affecting the welfare of the child. Where a court issues an order stating that Stratford College should make certain information available to a parent, the school can release the data on foot of the court order.

Data protection regulations also prohibit the supply of:

- **Health data** to a patient in response to a request for access if that would be likely to cause serious harm to his or her physical or mental health. This is to protect the individual from hearing anything about himself or herself which would be likely to cause serious harm to their physical or mental health or emotional wellbeing. In the case of health data, the information can only be released after the school/ETB has consulted with the appropriate health professional (usually the data subject's GP).

- **Personal Data** obtained in the course of carrying on social work ("social work data") (personal data kept for or obtained in the course of carrying out social work by a Government department, local authority, the HSE, TUSLA, etc) is also restricted in some circumstances if that would be likely to cause serious harm to the health or emotional condition of the data subject concerned. In the case of social work data, the information cannot be supplied at all if the school/ETB believes it would be likely to cause serious harm to the physical or mental health or emotional condition of the data subject. If the social work data includes information supplied to the school/ETB by an individual (other than one of the school's/ETB's employees or agents) while carrying out social work, the school/ETB is not permitted to supply that information to the data subject without first consulting that individual who supplied the information.

- Health data to a patient in response to a request for access if that would be likely to cause serious harm to his or her physical or mental health. This is to protect the individual from hearing anything about himself or herself which would be likely to cause serious harm to their physical or mental health or emotional wellbeing. In the case of health data, the information can only be released after the school has consulted with the appropriate health professional (usually the data subject's GP).

- Personal Data obtained in the course of carrying on social work ("social work data") (personal data kept for or obtained in the course of carrying out social work by a Government department, local authority, the HSE, TUSLA, etc) is also restricted in some circumstances if that would be likely to cause serious harm to the health or emotional condition of the data subject concerned. In the case of social work data, the information cannot be supplied at all if the school believes it would be likely to cause serious harm to the physical or mental health or emotional condition of the data subject. If the social work data includes information supplied to the school by an individual (other than one of the school's employees or agents) while carrying out social work, the school is not permitted to supply that information to the data subject without first consulting that individual who supplied the information.

All staff have a right to request a Data Access Request and all parents have a right to request a DAR for their child. All students aged 18 years and over have a right to request a DAR. Under the Data Protection Acts, all parties are entitled to be told what information the school holds about them and to be furnished with copies of same.

Outside Requests: those who are not parents / guardians or students over the age of 18 will not have access to records, except in exceptional circumstances such as a request by the Gardai, Child and Family Agency (Tusla) personnel etc. All such requests must be made to the Principal and will only be released on the production of proof of identity and the reason for the request.

Right to be Informed (Article 3):
an individual has the right to be informed whether Stratford College holds data/information about them and to be given a description of the data together with details of the purposes for which their data is being kept. The individual must make this request in writing and the data controller will accede to the request within the legislated time frame.

Right to a Copy of Personal Data (Article 4)

Individuals are entitled to a copy of their personal data on written request.

- The individual is entitled to a copy of their personal data (subject to some exemptions and prohibitions set down in Section 5 of the Data Protection Act)
- Request must be responded to within one month
- Where a subsequent or similar request is made soon after a request has just been dealt with, it is at the discretion of the school as data controller to comply with the second request (no time limit but reasonable interval from the date of compliance with the last access request.) This will be determined on a case-by-case basis.
- No personal data can be supplied relating to another individual unless that third party has consented to the disclosure of their data to the applicant. Data will be carefully redacted to omit references to any other individual and only where it has not been possible to redact the data to ensure that the third party is not identifiable would the school refuse to furnish the data to the applicant.

Providing information over the phone
Any employee in Stratford College dealing with telephone enquiries should be careful about disclosing any personal information held by the school over the phone. In particular the employee should:

- Check the identity of the caller to ensure that information is only given to a person who is entitled to that information
- Suggest that the caller put their request in writing if the employee is not sure about the identity of the caller and in circumstances where the identity of the caller cannot be verified
- Refer the request to the principal for assistance in difficult situations. No employee should feel forced into disclosing personal information.

Personal Data Access Request Refusals
Stratford College, as the Data Controller can refuse a Personal Data Access Request and the reasons for the rejection must be clearly set out in writing to the Requestor. Requestors do not have a right to see information relating to them (1) If the information is kept only for the purpose of statistics or research, and/or (2) where the results of the statistical work or

research are not made available in a form that identifies any of the individuals. Requests made for other, non-data protection purposes can be rejected.

Third Party Agreements

For the purposes of this policy a data processor is a person who processes personal information on behalf Stratford College as the data controller, but does not include an employee of a data controller who processes such data in the course of their employment. Data Protection legislation places responsibilities on such entities in relation to their processing of the data.

Such data processors may include but are not limited to any external company providing HR services (assistance with payroll etc.); external IT services companies; school text service providers; biometric systems operators; an external company monitoring the school's CCTV system; external company providing "cloud computing" electronic storage facilities for the school.

When Stratford College enters into an agreement with a data processor, a written service-level agreement or data processing agreement will be put in place between the school as data controller and the contracted company. This is a requirement under Data Protection legislation. The written agreement/contract will include at a minimum the following obligations on the data processor:

1. To act only on the instruction of the data controller, Stratford College

2. To comply with the obligations imposed on data controllers by section 2(1)(d) of the Data Protection Acts (i.e. to ensure that appropriate steps are taken against the accidental destruction, damage or loss of data)

3. To ensure that the data processor provides sufficient guarantees in respect of technical security measures and organisational measures governing the processing.

4. A warranty and indemnity from the data processor to Stratford College for any breaches of the provisions of the contract or the data processor's obligations under law, and to use trained, competent and compliant staff.

5. A commitment to provide prompt and full assistance to enable Stratford College to comply with any access request received by the school

6. An agreement to inform Stratford College immediately where there are any data security breaches in the data processor's company. In such circumstances, the principal of the school should be contacted immediately.

7. A right to engage in an adequacy audit and/or compliance audit to check compliance with the commitments in the agreement/contract (especially the security obligations).

8. Ensure that a copy of Stratford College's Data Protection Policy is given to the data processor and that the data processor is committed to complying with the terms of the Policy.

9. The agreement should require that on termination or expiry of the contract for any reason, all personal data held by the data processor should be either returned to the data controller or deleted entirely from the data processor's systems and files.

**** Items 1 – 3 are required by law to be included in any agreement / contract. Items 4 – 9 are optional but considered good practice. ****

Transfer of Data

Any and all personal data obtained by Stratford College will not be used for any other purpose than it was collected, and will not be divulged to any other Third Party, except in ways that are compatible with the specified purpose.

Prior to the transfer of any personal data to third parties including official bodies or State agencies evidence of a legitimate legal basis for the transfer of any such data must be provided.

Transfer of data by Stratford College to other schools, the Department of Education and Skills, the Child and Family Agency (Tusla) and any other official bodies or State Agency is permitted under Section 28 of the Welfare Act 2000.

Transfers of personal data to agents of Stratford College, who are carrying out operations upon the data on behalf of Stratford College and not retaining it for their own purposes, does not constitute "disclosures" of data for the purposes of Data Protection legislation.

Breach of Data

Stratford College has robust procedures in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use.

Should a data breach occur where the security or integrity of personal data is compromised through misappropriation; loss or theft of data or equipment; unauthorised individuals gaining access; a deliberate attack on systems; equipment failure; human error of malicious acts such as hacking, viruses or deception,. Stratford College will follow all procedures as set out in data protection legislation and policy.

Where a data breach is likely to result in a risk for the rights and freedoms of an individual(s) the breach will be reported to the Data Protection Commissioner, within 72 hours of first becoming aware of the breach. Where it is not possible to report the breach within 72 hours, Stratford College will provide reasoned justification of the time delay.

Stratford College will also notify the individual(s) concerned of any breach that may bring harm to such individual without undue delay after first becoming aware of any such data breach.

In appropriate cases, Stratford College will also notify organisations that may be in a position to assist in protecting data subjects including, where relevant, An Garda Siochana, financial institutions etc.

Any data breach, comprising the facts relating to personal data breach will be documented and maintained.

Data Protection Impact Assessments

Stratford College will, where a type of processing of data is likely to result in a high risk to the rights and freedoms of an individual(s), prior to the processing, carry out a data protection impact assessment ("DPIA"). Specifically, a DPIA will be carried out where a significant change to an existing processing operation takes place after 25th May 2018.

Data Protection Rights

Data protection legislation provides an individual(s) with the right to request Stratford College to rectify inaccurate or incomplete personal data hold by the school about the individual(s). Specifically the following rights are afforded:

Right to Complain to supervisory authority – the right to notify the r

Right of Access -the right to request a copy of the personal data that Stratford College holds about you, together with other information about our processing of your personal data

Right to Rectification – the right to request that any inaccurate data that is held about you by Stratford College is corrected, or if Stratford College has incomplete information that you may request that Stratford College updates the information such that it is complete

Right to be Forgotten (Erasure) - the right to request Stratford College to erase your data. Stratford College must erase your data if one of the following applies:

- The data is no longer needed for the purpose it was collected
- You have withdrawn your consent to the processing of your data
- You object to the processing of your data
- There is no lawful basis for the processing
- The data must be erased to comply with law

The Right to be Forgotten includes the right to have publicly available personal data erased or as far as technologically possible, removed from public availability, including search engine results.

The Right to be Forgotten is not an absolute right and requests under the procedure are assessed on a case-by-case basis. This right does not apply where processing is necessary because of an overriding freedom of expression, legal or public interest.

Right to Restrict Processing – the right to restrict Stratford College from processing your personal data where, the accuracy of the data is in question, the processing of the data is unlawful, Stratford College no longer needs the data for the original purpose but it is required by you for other reasons and you have challenged the legal basis for the processing.

Right to Data Portability – the right to request Stratford College to provide you, or a Third Party, with a copy of your personal data in a structured, commonly used machine readable format, including the right to request Stratford College Data Controller to transfer your personal data to another controller.

Right to Object and Automated Decision making / profiling – the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning you or similarly significantly affects you

To exercise any of the above rights please contact, The Principal, Stratford College, 1 Zion Road, Rathgar, Dublin 6.

Implementation Arrangements, Roles and Responsibilities

In Stratford College the Board of Management is the data controller and the Principal will be assigned the role of co-ordinating implementation of this Data Protection Policy and for ensuring that staff who handle or have access to *Personal Data* and *Sensitive Personal Data* are familiar with their data protection responsibilities.

The following personnel have responsibility for implementing the Data Protection Policy:

Name	**Responsibility**
Board of management:	Data Controller
Principal:	Implementation of Policy
Teaching personnel:	Awareness of responsibilities
IT personnel	Security, encryption and confidentiality
Administrative personnel:	Security, confidentiality

Disciplinary procedures will be invoked if sensitive information regarding Stratford College students or employees is misplaced.

This Policy will be reviewed as necessary but at a minimum after two years and will take cognisance of changing information or guidelines (e.g. from the Data Protection Commissioner, Department of Education and Skills, Tusla, legislation and feedback from parents/guardians, students, school staff and others. The policy will be revised as necessary in the light of such review and evaluation and within the framework of school planning.

For further information and resources regarding data protection please visit:

www.dataprotectionschools.ie
www.dataprotection.ie
www.education.ie

This policy known as Stratford College Data Protection Policy is:

Ratified by:

Ms Imelda Reynolds

Ms Imelda Reynolds
Acting Chair of Board of Management

Patricia Gordon

Ms. Patricia Gordon
Principal

Date: 30 May 2018