Introduction - Awareness

For the purpose of this document:

- the Data Controller is St. Peter's School
- the Data processors are staff involved with handling school related data
- the Data Subjects are the students and staff whose data we hold

St. Peter's School should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature.

It is the responsibility of all members of the school community to take care when processing / handling, using or transferring personal data; that it cannot be accessed by anyone who does not:

- have permission to access that data
- need to have access to that data.

Any loss of personal data can have serious effects for individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action and / or criminal prosecution. All transfers of data are subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data legislation and relevant regulations and guidance from the Local Authority.

The Data Protection Act (1998) lays down a set of rules for processing of personal data (both structured manual records and digital records). It provides individuals (data subjects) with rights of access and security and requires users of data (data processors) to be open about how it is used and to follow "good information handling principles". This is being superseded by the General Data Protection Regulation which comes into force on 25th May 2018. This policy reflects the current Data Protection Act and planning for the GDPR and may be updated to reflect advice and information released by the Information Commissioners Office.

Policy Statements

Article 5 of the GDPR requires that personal data shall be:

- *processed lawfully, fairly and in a transparent manner in relation to individuals;*
- *collected for specified, explicit and legitimate purposes and not 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;*
- *adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;*
- *accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;*
- *kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods*

insofar as the personal data will be processed solely for archiving purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

- *processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.*

As such the St. Peter's School undertakes to hold the minimum personal information necessary to enable it to perform its function and information will be erased once the need to hold it has passed for students this is when they reach the age of 25 (School leaving age +7 years). See Appendix A for the retention schedule.

Every effort will be made to ensure that information is accurate, up to date and that inaccuracies are corrected without unnecessary delay. We will send data checking forms annually but parents can make amendments as often as they like.

All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".

Information to Parents / Careers – the "Privacy Notice" Appendix

Under the "Fair Processing" requirements in the Data Protection Act, and the future terms of GDPR the school will inform parents/carers of all students of the data they hold on the pupils / students, the purposes for which the data is held and the third parties (e.g. LA, CES, DCSF, QCA, Connexions etc.) to whom it may be passed. This fair processing notice will be passed to parents / carers as part of a successful application to the school and be available on the school's website.

Information we hold and why we hold it.

Personal Data relating to Students

The school will have access to a wide range of personal information and data. The data may be held in digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. Access to data is restricted so that only members of the school community who need access will be able to access it.

We collect and process data relating to the students on roll (and formerly on roll). This information will include:

- Basic Students Details (Legal and known as names, Date of birth, gender, photograph,..)
- contact details for Students, Parents, Carers and Other People nominated by Parents,
- Examination results (EYFS, KS1, KS2, KS3, KS4, KS5),
- attendance information,
- behaviour log details,
- achievement log details,
- exclusion information,
- Destinations (where they go after they leave us)

and personal characteristics such as their

- ethnic group,
- additional educational needs,
- relevant medical information,
- Religion,

- Baptism records.

For students enrolling for post 14 qualifications, the Learning Records Service will give us the unique learner number (ULN) and may also give us details about their learning or qualifications.
Once our students reach the age of 14, the law requires us to pass on certain information to the Catholic Education Service, Borough of Bournemouth or the Youth Support Services in the area who have responsibilities in relation to the education or training of 14-19 year olds. We may also share certain personal data relating to young people aged 16 and over with post-16 education and training providers in order to secure appropriate services for them.

We share data with the third party companies as data processors. In principle the purposes of these systems are to support the core principles of the school and ultimately the progress and safety of the students in the school's care. *(Please refer to Third Party Systems Policy)*

Where possible, we will not give information about our pupils to anyone without your consent (as indicated via the Data Collection Form parents / guardians complete on entry to the school) unless the law and our policies allow us to do so.

If you want to receive a copy of the information about your child that we hold, please contact: info@st-peters.bournemouth.sch.uk in the first instance.

We are required, by law, to pass some information about our students to the Department for Education (DfE). This information will, in turn, then be made available for use by the Local Authority.
The DfE may also share student level personal data that we supply to them, with third parties. This will only take place where legislation allows it to do so and it is in compliance with the Data Protection Act 1998 (and GDPR from May 2018).
Decisions on whether DfE releases this personal data to third parties are subject to a robust approval process and are based on a detailed assessment of who is requesting the data, the purpose for which it is required, the level and sensitivity of data requested and the arrangements in place to store and handle the data. To be granted access to student level data, requestors must comply with strict terms and conditions covering the confidentiality and handling of data, security arrangements and retention of use of the data.
For more information on how this sharing process works please visit:
https://www.gov.uk/guidance/national-pupil-database-apply-for-a-data-extract.
For information on which third party organisations (and for which project) student level data has been provided to, please visit:
https://www.gov.uk/government/publications/national-pupil-database-requests-received.
If you need more information about how our local authority and/or DfE collect and use your information, please visit:

- https://bournemouth.gov.uk (Our local authority)
- https://www.gov.uk/data-protection-how-we-collect-and-share-research-data (DfE)

Personal Data relating to Staff

We collect and process data relating to staff on roll (and formerly on roll). This information will include:

For staff members we collect and process data which will include their:

- Personal details and characteristics such as
  - names,
  - addresses,
  - contact details,
  - bank account details,
  - ethnic group
  - religion
  - relevant medical information.

- Professional records e.g.
    - employment history,
    - Training
    - Qualifications
    - taxation and national insurance records,
    - appraisal records
    - Absence Information
    - References
    - disciplinary records

Data Protection Officers

Registration

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner. The registration number is **Z472096X** and the most up to date register entry can be seen at: https://ico.org.uk/esdwebpages/search.

Responsibilities

The school's Senior Information Risk Officer (SIRO) is *Iain Scott-Brown.* He will be responsible for keeping up to date with current legislation and guidance and will:

- determine and take responsibility for the school's information risk policy and risk assessment
- appoint the Information Asset Owners (IAOs)

The school has identified Information Asset Owners (IAOs) for the various types of data being held (e.g. student information / staff information / assessment data etc.). The IAOs will manage and address risks to the information and will understand:

- What information is held and for what purpose
- Who has access to protected data and why

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access with personal data, when engaged in their role as a Governor.

Lawful basis for processing personal data

We collect and hold personal information relating to our students and may also receive information about them from their previous school and / or local authority and / or Department for Education (DfE). We use this personal data to:

- support our students' learning;
- monitor and report on their progress;
- provide appropriate pastoral care; and
- assess the quality of our services.

The legal basis for our processing or personal data have been identified in 5 areas:

Contractual necessity	Personal data may be processed on the basis that such processing is necessary in order to enter into	We cannot function as a school without basic information

	or perform a contract with the data subject.	
Compliance with legal obligations	Personal data may be processed on the basis that the controller has a legal obligation to perform such processing.	We are required to keep certain records and submit them to government (e.g. School Census information)
Public interest	Personal data may be processed on the basis that such processing is necessary for the performance of tasks carried out by a public authority or private organisation acting in the public interest.	
Legitimate interests	Personal data may be processed on the basis that the controller has a legitimate interest in processing those data, provided that such legitimate interest is not overridden by the rights or freedoms of the affected data subjects.	It is in the interests of our students that we hold information and use it to track their performance, arrange rewards provide them with a most appropriate education.
Consent	Personal data may be processed on the basis that the data subject has consented to such processing. Parental permission is required to process the personal data of children (and note that a child is anyone under the age of 16). In some contexts (especially online) proving that parental permission has been obtained may be difficult.	We seek parental consent for processing of data and use this as a final basis. The parental consent will be used for example to allow or deny the use of photographs of students. We will still collect basic information and use it under the above criteria.

Consent

A consent form (Fair Processing Notice) is sent to parents of a student to sign as part of a successful application to the School.

A parent / guardian can request that **only** their child's name, address and date of birth be passed to the Catholic Education Service, Borough of Bournemouth or Youth Support Services by informing the school. This right is transferred to the young person once he reaches the age of 16. For more information about services for young people, please go to our local authority website at: www.bournemouth.gov.uk/childreneducation/YouthService/YouthService. This option is indicated on the data collection forms.

We will not give information about our students to anyone without your consent (as indicated via the Student Information Form parents / guardians complete on entry to the school) unless the law and our policies allow us to do so.

If you want to receive a copy of the information about your child that we hold, please complete the Subject Access Request Application Form found on the school website and email the school info@st-peters.bournemouth.sch.uk , or:

Send to the school clearly addressed: Senior Information Risk Officer
St Peter's School
St Catherine's Road
Bournemouth
Dorset
BH6 4AH

Training & awareness

All staff will receive data processing awareness / data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff
- Staff meetings / briefings / Inset
- Day to day support and guidance from Information Asset Owners

Risk Assessments

Information risk assessments will be carried out by Senior Information Risk Officer (SIRO) with support from Information Asset Owners (IAO) to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

- Recognizing the risks that are present
- Judging the level of the risks (both the likelihood and consequences)
- Prioritizing the risks

Secure Storage of and access to data

The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system. Permissions will be distributed as outlined above in the: *Responsibilities: IAO Table*.

All users will be given secure user names and strong passwords which must be changed as outlined in . the User Credential Policy. [1]Usernames and passwords must never be shared, this is classed as "unacceptable use" as outlined in the school's Acceptable Use Policy and will be a disciplinary matter.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked when left unattended (⊞+L) (even for very short periods).

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on school equipment (this includes computers and portable storage media). Private equipment (i.e. owned by the users) must not be used for the storage of personal data.
When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must stored on encrypted media only.

[1] Where staff have an ICT related problem their user credentials may be shared with the ICT support team.

- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Please refer to the School's Data Backup Policy, Bring Your Own Device (BYOD) Policy and Acceptable Use Policy.

All paper based Protected and Restricted (or higher) material must be held in lockable storage.

Right of Access

The school recognises that under Section 7 of the Data Protection Act (GDPR), data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests: Complete the Subject Access Request Application Form found on the school website and email the school info@st-peters.bournemouth.sch.uk , or:

Send to the school clearly addressed: Senior Information Risk Officer
St Peter's School
St Catherine's Road
Bournemouth
Dorset
BH6 4AH

Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

Right to withhold Data

St. Peter's School reserves the right to redact and/or withhold data if:

Information that might cause serious harm to physical or mental health of the student or another individual. *(Education Order 2000/414) e.g.*

- Information would reveal that the student was at risk of abuse.
- Where the disclosure would not be in the students' best interest.
- The information contained adoption and/or parental order records.
- Certain information given to a court in proceedings concerning the student.

Data breaches

The School will monitor its Data Handling Policy and Practice by completing annual Data Audits. Data Audit Reviews will also take place after data breaches to identify ways to improve the security of the Data held by School. If a Data Breach occurs:
The Data Protection Officer will be informed of the Breach as soon as it is noticed.
The Data Protection Officer will judge whether the ICO need to be notified.
The Data Protection will then assign a member of the School's workforce to investigate the breach.
The Data Subjects relating to the breach will receive notification within 48 Hrs.
After the investigation, the Data Subjects will receive a written report pertaining to the breach and efforts to minimise the risk in future.

Other Data Processing issues

Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location.
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school.
- When sensitive or personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should make use of the secure remote access to the management information system.
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software. This includes devices own by them (please refer to the school's Bring Your Own Device Policy)
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority in this event.

Retention & Disposal of data

St. Peter's School undertakes to hold the minimum personal information necessary to enable it to perform its function and information will be erased once the need to hold it has passed for students this is when they reach the age of 25 (School leaving age +7 years). See Appendix A for the retention schedule.

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of protected data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance, and other media must be shredded, incinerated or otherwise disintegrated for data.

A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

Audit Logging / Reporting / Incident Handling

It is good practice, as recommended in the "Data Handling Procedures in Government" document that the activities of data users, in respect of electronically held personal information, will be logged and these logs will be monitored by SIRO, SLT and School governors.

The audit logs will be kept to provide evidence of accidental or deliberate security breaches – including loss of protected data or breaches of an Acceptable Use policy.

The school has a policy for reporting, managing and recovering from information risk incidents, which establishes:

- a "responsible person" for each incident
- a communications plan, including escalation procedures
- and results in a plan of action for rapid resolution and

- a plan of action of non-recurrence and further awareness raising.

All significant data protection incidents must be reported through the SIRO to the Information Commissioner's Office within 48 hours of the breach occurring.

Use of technologies and Protective Marking

	The information	The technology	Notes on Protect Markings (Impact Level)
School life and events	School terms, holidays, training days, the curriculum, extra-curricular activities, events, displays of pupils work, lunchtime menus, extended services, parent consultation events	Common practice is to use publically accessible technology such as school websites or portal, emailed newsletters, subscription text services.	Most of this information will fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.
Learning and achievement	Individual learner's academic, social and behavioural achievements, progress with learning, learning behaviour, how parents can support their child's learning, assessments, attainment, attendance, individual and personalised curriculum and additional educational needs.	St. Peter's School will make information available by parents logging on to a system that provides them with appropriately secure access, such as a SIMS Parent App or SLG, and by communication to a personal device or email account belonging to the parent.	Most of this information will fall into the PROTECT (Impact Level 2) category. There may be learners whose personal data requires a RESTRICTED marking (Impact Level 3) or higher. For example, the home address of a child at risk. In this case, the school may decide not to make this learners record available in this way.
Messages and alerts	Attendance, behavioural, achievement, sickness, school closure, transport arrangements, and other information that it may be important to inform or contact a parent about as soon as possible. This may be particularly important when it is necessary to contact a parent concerning information that may be considered too sensitive to make available using other online means.	Email and text messaging are commonly used by schools to contact and keep parents informed. Where parents are frequently accessing information online then systems e.g. SIMS Parent App and SLG, might be used to alert parents to issues or be used to provide further detail and context.	Most of this information will fall into the PROTECT (Impact Level 1) category. However, since it is not practical to encrypt all emails or text messages to parents, schools should not send detailed personally identifiable information. General, anonymous alerts about schools closures or transport arrangements would fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.

Notes for Staff

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- have permission to access that data
- need to have access to that data.

This might, for example mean ensuring that your school's email account is not accessible on a home computer by virtue of a saved password. It could equally mean not leaving papers containing personal data unsupervised in a classroom or on a table at home.

Any loss of personal data can have serious effects for individuals and / or institutions concerned, and can bring the school into disrepute and may well result in disciplinary action and / or criminal prosecution. All transfer of data is subject to risk of loss or contamination.

Staff must therefore take all possible precautions to ensure the security and integrity of the data that the school holds.
This includes, but is not limited to:

- Locking all computers which may have access to personal data when leaving them.
- Only having copies of personal data required.
- Storing electronic copies primarily on the school's Resources Drive secure or if this is not feasible on encrypted devices.
- Disposing of paper copies of personal data in the secure confidential waste bins which will then be disposed of securely when full.
- Changing their passwords regularly as per the School's User Credential Policy
- Never sharing their usernames and passwords.
- Restricting the storage of personal information to school devices (e.g. not transferring data to a personal computer.
- Paper based records must be stored securely during their lifetime.

It is also important to note that any records relating to somebody's personal data must be disclosed under freedom of subject access requests. It is important therefore to record everything is a proper manner and remember that any record may be viewed at a later date. In particular, when entering data relating to a named student the names of other students should never be included.