DATA PROTECTION POLICY

INCORPORATING

\

Ratified by FGB 18 July 2018

Due for review July 2020

IT USER CREDENTIAL POLICY

DEFINITIONS

- School Network – the devices attached to the Network through Data cabling or Wifi.
- Users – the workforce and students who are given authorised to log on to the School Network.
- User Credentials – Usernames and associated Passwords.
- Third Party Systems – External Systems used by the School to assist in its management and to assist the Teaching and Learning as outlined in the Third Party System Policy.
- ICT Support Team – The staff employed by St. Peter's School to maintain the School's Network and associated systems.

INTRODUCTION

Users of the School Network are expected to adhere to the User Credential Policy so the data stored by the school remains secure, in accordance with the Data Protection Act and GDPR.

OBJECTIVES OF USER CREDENTIAL POLICY

- To maintain the security of the School Network and the Data it stores.
- To reduce the risk of cybercrime committed against the school.

STATEMENT OF INTENT

Users are NOT permitted to share their User Credentials (Username and Password) with anyone else. This includes all User Credentials for all platforms (e.g. Office 365, St Peter's School Network, and SIMS)

All school Network Passwords will consist of:

- At least 8 characters
- At least 1 Capital and 1 Numerical character
- Renew of passwords to occur every 6 months
- Renewed passwords cannot be the same as the previous 4 passwords.

User Credentials of Third Party Systems must meet their User Credential specification.

IT USE OF THIRD PARTY SYSTEMS POLICY

DEFINITIONS

- *The School* – St. Peter's School.
- *School's Information Risk Officer (SIRO)* – Mr Iain Scott-Brown.
- *School Network* – the devices attached to the Network through Data cabling or Wifi.
- *Users* – the workforce and students who are given authorised to log on to the School Network.
- *BYOD* – Bring your own Device (a device not owned by the School but used to access School digital resources (e.g. Email, Wifi, connect to a computer, remote gateway access,)
- *ICT Support Team* – The staff employed by St. Peter's School to maintain the School's Network and associated systems.
- *Staff* – the workforce of the School
- *User Credentials* – Usernames and associated Passwords.
- *Third Party Systems* – External Systems used by the School to assist in its management and to assist the Teaching and Learning as outlined in the Third Party System Policy.

INTRODUCTION

Staff wishing to use a Third Party System where there is a need to share and store personal data to support the school in its role, whether this is related to the management of the school and its resources or related to the Teaching and Learning of the students – must ensure that the system is fully GDPR compliant. This will be completed through an application process.

OBJECTIVES

- To ensure that the School is fully compliant with the Data Protection Act and the GDPR.
- To minimise the risk of a Data Breach.

STATEMENT OF INTENT

Staff may only use these systems once they have received written authorisation from the School's Information Risk Officer.

Authorisation will only occur once the School's Information Risk Officer has worked alongside the applicant to ensure the GDPR is fully complied with.

The member of Staff must complete the necessary form (appendix A) as part of this process. A review of the application should be agreed so that systematic checks may take place. Staff must also inform the School's Information Risk Officer of any changes to service. Any failure to comply with GDPR legislation will lead to the removal of the System.

ICT ACCEPTABLE USE POLICY

DEFINITIONS

- *The School* – St Peter's School.
- *School Network* – the devices attached to the Network through Data cabling or Wifi.
- *Users* – the workforce and students who are given authorised to log on to the School Network.
- *BYOD* – Bring your own Device (a device not owned by the School but used to access School digital resources (e.g. Email, Wifi, connect to a computer, remote gateway access,)
- *ICT Support Team* – The staff employed by St Peter's School to maintain the School's Network and associated systems.

INTRODUCTION

The School has a School Network that covers both sites and offers access for wireless devices and access from home. In order for Users to have access to these resources, the internet and other associated technologies to support teaching and learning, the workforce and students must agree to the following.

OBJECTIVES

- To ensure the safety of the Data stored on the School Network.
- To ensure the safety of all the Users on the School Network.
- To reduce the risk of cyber-attacks.

STATEMENT OF INTENT

Acceptable Uses

- If Users move away from their device, they are expected to lock it (e.g. ⊞+L to lock a windows PC), so that other people are unable to access data held on it.
- The network has been set up to allow network (including internet) access to learning tools. This includes software activities/packages, e-mail, research tools and communication/collaboration tools.
- Network users have a limit to their storage space and must take responsibility for the management of their accounts. Users need to respect their space limits and delete files when necessary.
- Information which is copied/pasted from the internet must include an acknowledgment of the source.
- Material accessed and/or stored on the system is not guaranteed to be private. The network administrators may need to access material from time to time to make sure that the system is being used in accordance with **all** school policies.
- Users are expected to use school email appropriately and to be aware that the content of e-mails and other communications may be viewed by a third party.
- Network users are reminded that any work created or amended on the school network remains the intellectual property of the school.
- Network users are provided with user accounts and passwords. They must keep their passwords private. Usernames and/or passwords cannot be shared as outlined in the school's Password Policy.
- Users should also adhere to the following associated Policies:
    - Bring Your Own Device Policy
    - User Credential Policy
    - Social Media Policy

Unacceptable Uses

- [1]Users may not download, copy or store any software, shareware, freeware.
- The School's ICT facilities are for learning appropriately; e.g. it is therefore inappropriate to use them for playing games.
- The School Network should not be used for commercial purposes apart from school sanctioned ones (e.g. Young enterprise, charity etc.) Users should not buy or sell goods or services through the School Network.
- The School Network may not be used for any activity that would be considered breaking the law or promotes illegal actions.
- Users may not use profane, obscene or derogatory language in their communication with others.
- Personal attacks or inappropriate postings will be seen as cyber bullying and treated accordingly. This will include use of ICT in and out of school to bully any member of our school community.
- Users may not log on to another User's account or access their files. This will be seen as a breach of the Computer Misuse Act.
- The School's internet filters are there for a reason; accessing sites that allow the user to bypass these school filters and monitoring software is not appropriate.
- Newsgroups, chat lines, bulletin boards, social network sites, discussion groups etc. not set up, administered or sanctioned by the school are inappropriate for school use.

At times there may be material or uses of the school's ICT facilities that cannot be accounted for in this policy. The school has the final say in what it deems to be acceptable and what it deems to be unacceptable.

SAFETY GUIDELINES FOR STUDENTS

Your safety whilst using technology is very important to the school

- Never give out your last name, address or telephone number.
- Never agree to meet someone offline that you have only met online.
- Notify an adult in the event of any inappropriate communication or if you come across anything that works against the Acceptable Use Policy or that you simply feel uncomfortable with.
- Treat your personal data (including images) with respect and take care of it, once it is given away, it cannot be taken back!

I recognise that breaking parts of this acceptable use policy may lead to consequences depending on severity and repetition:

- Temporary loss of computer privileges
- Increased and more active monitoring of your computer usage
- Other sanctions as outlined in the school's Behaviour Policy

I have read and understand the guidelines above and realise that use of the school network and the internet is only possible on signing this form

Student's name	
Student's signature	
Parent's/Carer's signature	

Due for review July 2020

[1]Unless a member of the ICT support Team

CCTV POLICY

DEFINITIONS

- *The school* – St Peter's Catholic School
- *CCTV Controllers* – The school's CCTV Controller is Mr C Chastney and Mr M Slaughter
- *Site Manager*–The school's Site Manager is Mr C Chastney
- *CCTV Operator* – Employees of the school with the skills and permission to operate the CCTV and retrieve footage.

INTRODUCTION

The purpose of this policy is to regulate the management, operation and use of the closed-circuit television (CCTV) system at the school. The system comprises a number of static cameras located around the school site. The cameras can be monitored from various locations by CCTV Controllers. Cameras covering entrances and exits to the site, resources of high financial value and areas which have historically been identified by students where they feel most vulnerable. The CCTV system and data is owned by the school.

OBJECTIVES OF THE CCTV SYSTEM

- To protect the school buildings and assets of the school.
- To increase personal safety of students and the school's workforce and reduce the fear of crime.
- To support the Police in a bid to deter and detect crime.
- To assist in managing the school.

STATEMENT OF INTENT

The CCTV system will be registered with the Information Commissioner under the terms of the Data Protection Act 1998 and will seek to comply with the requirements both of the Data Protection Act and Commissioner's Code of Practice. The school will treat the system and all information, documents and recordings obtained and used, as data which are protected by the Data Protection Act. The system installed is compliant with the Data Protection Act, Human Rights Act and Regulatory Investigation Powers Act.

Cameras will be used to monitor activities within the school and its car parks and other public areas to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and wellbeing of the school and its workforce, students and visitors. Cameras are focussed in the school buildings and around entrances/exits.

Materials of knowledge secured as a result of CCTV will not be used for any commercial purpose. Information transferred to other appropriate media will only be used for the investigation of a specific crime or incident. Release to the media would only be allowed with the written authority of the police if this was required by them as part of a police investigation.

Warning signs, as required under the Data Protection Act, have been placed at key points around the site.

Updated: June 2018
Approved by TLA 4 July 2018
Ratified by Full Governing Body: 18 July 2018
Due for Review: July 2020

DATA HANDLING POLICY

Staff Link:	I Brown	**Date:**	May 2018
Governor Link:		**First Review:**	May 2020
		Subsequent Reviews:	Bi-annual

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 following 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.

System/Company	Reason	Information shared
Microsoft Office 365	To provide cloud services and emails for students.	Name, Year Group, Class Information, email address.
Redstore	School Backup services	All school related Data.
Capita SIMS – our Management Information System providers.	To provide login details For resolving issues.	Parent names and related student information are provided to create logins. Under normal circumstances they have no access to personal data but may be allowed access in the event of a problem with the Management Information system. In this case, this is carried out over an encrypted link and data is retained only so long as it is needed to resolve the issue.
Salamander	To provide login details	Name, Year Group, Class information.
Cambridge Elevate	To provide login details	Name, Year Group, Class information, Student's school email.
ParentPay	To provide login details	
Kerboodle	To provide login details	Name, Class Information, Student's school email.
Wonde		
Diagnostic Questions		
4Matrix		
Unifrog		
Parent Pay		Student fingerprints, Student PIN numbers, Parental Contact Information.

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: 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: 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:

- www.bournemouth.gov.uk (Our local authority)
- 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 record

System/Company	Reason	Information shared.
Dorset Payroll		
Capita SIMS	For troubleshooting and problem resolution	Personnel Record as held in sims
Kerboodle	For consultancy	
Office 365		
Unifrog		
4Matrix		
Parent Pay		

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

IAO	Type of Data	Why
Finance Staff	Financial	Job Function
Human Resources Officer	Personnel	Job Function
School Business Manager	Financial and Personnel	Job Function
Finance Manager	Financial and Personnel	Job Function (in the absence of the School Business Manager)
Pastoral and Attendance Officers	Student	Job Function
Heads of Year, Subject Leaders and Senior Leaders	Student	Job Function
Director of Communications	All	SIRO Job Function
Headteacher	All	Job Function
Deputy Headteacher	All	Job Function (in absence of Headteacher)
Assistant Headteacher	Student and Assessment	Job Function
General Office staff	Student	Job Function
Teacher	Student and Assessment	Job Function
Learning Support Assistants	Student	Job Function
Site Manager	Student	Job Function

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 or perform a contract with the data subject.	We cannot function as a school without basic information
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 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:

- Recognising the risks that are present
- Judging the level of the risks (both the likelihood and consequences)
- Prioritising the risks

Impact Levels and protective marking

The school will ensure that all school staff, contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher. Unmarked material is considered 'unclassified'. The term 'UNCLASSIFIED' or 'NON' or 'NOT PROTECTIVELY MARKED' may be used to indicate positively that a protective marking is not needed.

All documents (manual or digital) that contain protected or restricted data will be labelled clearly with the Impact Level shown in the header and the Release and Destruction classification in the footer.

Users must be aware that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data. Combining more and more individual data elements together in a report or data view increases the impact of a breach. A breach that puts a learner at serious risk of harm will have a higher impact than a risk that puts a learner at low risk of harm. Breaches may have an economic impact, the bigger this is the bigger the impact. Long-term significant damage to anyone's reputation has a higher impact than damage that might cause short-term embarrassment.

Release and destruction markings should be shown in the footer e.g. "Securely delete or shred this information when you have finished using it".

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 annually. Details are in the User Credential Policy. [2]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 be stored on encrypted media only
- 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.

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

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 to Senior Information Risk Officer, St Peter's School, St Catherine's Road, Bournemouth 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 email 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 confidential waste sacks 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.

GDPR RETENTION TIMES

Appendix A: St Peter's School Retention Periods

1 Child Protection

These retention periods should be used in conjunction with the document "Safeguarding Children and Safer Recruitment in Education" which can be downloaded from www.everychildmatters.gov.uk.

	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
1.1	Child Protection files	Yes	Education Act 2002, s175, related guidance "Safeguarding Children in Education", September 2004	DOB + 25 years[3]	SHRED: Child Protection information must be copied and sent under separate cover to new school/college whilst the child is still under 18 (i.e. the information does not need to be sent to a university for example) Where a child is removed from roll to be educated at home, the file should be copied to the Local Education Authority.
1.2	Allegation of a child protection nature against a member of staff, including where the allegation is unfounded	Yes	Employment Practices Code: Supplementary Guidance 2.13.1 (Records of Disciplinary and Grievance) Education Act 2002 guidance "Dealing with Allegations of Abuse against Teachers and Other Staff" November 2005	Until the person's normal retirement age, or 10 years from the date of the allegation whichever is the longer	SHRED: The following is an extract from "Safeguarding Children and Safer Recruitment in Education" p60 "Record Keeping 5.10 It is important that a clear and comprehensive summary of any allegations made, details of how the allegation was followed up and resolved, and a note of any action taken and decisions reached, is kept on a person's confidential personnel file, and a copy provided to the person concerned. The purpose of the record is to enable accurate information to be given in response to any future request for a reference if the person has moved on. It will provide clarification in cases where a future CRB Disclosure reveals information from the police about an allegation that did not result in a criminal conviction. And it will help to prevent unnecessary reinvestigation if, as sometimes happens, an allegation re-surfaces after a period of time. The record should be retained at least until the person has reached normal retirement age or for a period of 10 years from the date of the allegation if that is longer."

[3] This amendment has been made in consultation with the Safeguarding Children Group.

2 Governors

	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
2.1	Minutes					
	Principal set (signed)	No		Permanent	Retain in school for 6 years from date of meeting	Transfer to Archives
	Inspection copies	No		Date of meeting + 3 years	SHRED	
2.2	Agendas	No		Date of meeting	SHRED	
2.3	Reports	No		Date of report + 6 years	Retain in school for 6 years from date of meeting	Transfer to Archives
2.4	Annual Parents' meeting papers	No		Date of meeting + 6 years	Retain in school for 6 years from date of meeting	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]
2.5	Instruments of Government	No		Permanent	Retain in school whilst school is open	Transfer to Archives when the school has closed
2.6	Trusts and Endowments	No		Permanent	Retain in school whilst operationally required	Transfer to Archives
2.7	Action Plans	No		Date of action plan + 3 years	SHRED	It may be appropriate to offer to the Archives for a sample to be taken if the school has been through a difficult period
2.8	Policy documents	No		Expiry of policy	Retain in school whilst policy is operational (this includes if the expired policy is part of a past decision making process)	Transfer to Archives
2.9	Complaints files	Yes		Date of resolution of complaint + 6 years	Retain in school for the first six years Review for further retention in the case of contentious disputes SHRED routine complaints	
2.10	Annual Reports required by the Department for Education and Skills	No		Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002.SI 2002 No 1171	Date of report + 10 years	Transfer to Archives
2.11	Proposals for schools to become, or be established as Specialist Status schools	No			Current year + 3 years	Transfer to Archives
2.12	Proposal and documentation relating to Academy conversion.	No			Current year + 3 years	Transfer to Archives

3 Management

	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
3.1	Log Books e.g. Racist, Homophobic, search etc.	Yes[4]		Current Year + 6 years	Log by Academic Year	Transfer to the Archives at end of Academic Year
3.2	Minutes of the Senior Management Team and other internal administrative bodies	Yes[1]		Current Year + 6 years	Retain in the school for 6 years from meeting	Transfer to Archives
3.3	Reports made by the Headteacher or SLT	Yes[1]		Current Year + 6 years	Retain in the school for 6 years from meeting	Transfer to Archives
3.4	Records created by Headteachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	Yes[1]		Current Year + 6 years	SHRED	
3.5	Correspondence created by Headteachers, Deputy Headteachers, Heads of Year and other members of staff with administrative responsibilities	No		Current Year + 6 years	SHRED	
3.6	Professional development plans	Yes		Current Year + 6 years	SHRED	
3.7	School development plans	No		Current Year + 6 years	Review	Offer to the Archives
3.8	Admissions – if the appeal admission is successful	Yes		Current Year + 1 year	SHRED	
3.9	Admissions – if the appeal is unsuccessful	Yes		Current Year + 1 year	SHRED	
3.10	Proofs of address supplied by parents as part of the admissions process	Yes		Current Year + 1 year	SHRED	

4 Pupils

	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
4.1	Admission Registers	Yes		Current Year + 6 years	Log by Academic Year.	Transfer to the Archives at end of Academic Year
4.2	Attendance registers	Yes		Current Year + 6 years	SHRED [If these records are retained electronically any backup copies should be destroyed at the same time]	
4.4	Pupil files	Yes	Limitation Act 1980	DOB of the pupil + 25 years[5]	SHRED	
4.5	Special Educational Needs files, reviews and Individual Education Plans	Yes		DOB of the pupil + 25 years the review NOTE: This retention period is the minimum period that any pupil file should be kept. Some authorities choose to keep SEN files for a longer period of time to defend themselves in a "failure	SHRED	

[4] From January 1st 2005 subject access is permitted into unstructured filing systems and log books and other records created within the school containing details about the activities of individual pupils and members of staff will become subject to the Data Protection Act 1998.

[5] As above

				to provide a sufficient education" case. There is an element of business risk analysis involved in any decision to keep the records longer than the minimum retention period.		
4.6	Letters authorising absence	No		Current year + 6 years	SHRED	
4.7	Absence Records			Current year + 6 years	SHRED	
4.8	Examination results	Yes				
4.8a	*Public*	No		Year of examinations + 6 years	SHRED	Any certificates left unclaimed should be returned to the appropriate Examination Board
4.8b	*Internal examination results*	Yes		Current year + 6 years[6]	SHRED	
4.9	Any other records created in the course of contact with pupils	Yes/ No		Current year + 6 years	Review at the end of 3 years and either allocate a further retention period or SHRED	
4.10	Statement maintained under The Education Act 1996 - Section 324	Yes	Special Educational Needs and Disability Act 2001 Section 1	DOB + 30 years	SHRED unless legal action is pending	
4.11	Proposed statement or amended statement	Yes	Special Educational Needs and Disability Act 2001 Section 1	DOB + 30 years	SHRED unless legal action is pending	
4.12	Advice and information to parents regarding educational needs	Yes	Special Educational Needs and Disability Act 2001 Section 2	Closure + 12 years	SHRED unless legal action is pending	
4.13	Accessibility Strategy	Yes	Special Educational Needs and Disability Act 2001 Section 14	Closure + 12 years	SHRED unless legal action is pending	
4.14	Children's SEN Files	Yes		DOB of pupil + 25 years then review – it may be appropriate to add an additional retention period in certain cases	SHRED unless legal action is pending	
4.15	Parental permission slips for school trips – where there has been no major incident	Yes		Conclusion of the trip	SHRED	

[6] If these records are retained on the pupil file or in their National Record of Achievement they need only be kept for as long as operationally necessary.

4.16	Parental permission slips for school trips – where there has been a major incident	Yes	Limitation Act 1980	DOB of the pupil involved in the incident + 25 years The permission slips for all pupils on the trip need to be retained to show that the rules had been followed for all pupils	SHRED	
4.17	Records created by schools to obtain approval to run an Educational Visit outside the Classroom - Primary Schools	N	3 part supplement to the Health & Safety of Pupils on Educational Visits (HASPEV) (1998).	DOB of pupil + 25 years [7]	N	SHRED or delete securely

5 Curriculum

	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
5.1	Curriculum development	No		Current year + 1 year	SHRED
5.2	Curriculum returns	No		Current year + 1 year	SHRED
5.3	School syllabus	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SHRED
5.4	Schemes of work	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SHRED
5.5	Timetable	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SHRED
5.6	Class record books	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SHRED
5.7	Mark Books	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SHRED
5.8	Record of homework set	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SHRED
5.9	Pupils' work	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SHRED
5.10	Examination results	Yes		Current year + 6 years	SHRED
5.11	SATS records	Yes		Current year + 6 years	SHRED
5.12	PAN reports	Yes		Current year + 6 years	SHRED
5.13	Value added records	Yes		Current year + 6 years	SHRED

6 Personnel Records held in Schools

	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
6.1	Timesheets, sick pay	Yes	Financial Regulations	Current year + 6 years	SHRED
6.2	Staff Personal files	Yes		Termination + 7 years	SHRED
6.3	Interview notes and recruitment records	Yes		Termination + 7 years	SHRED

[7] This retention period has been set in agreement with the Safeguarding Children's Officer

6.4	Pre-employment vetting information (including CRB checks)	No	CRB guidelines	Date of check + 6 months	SHRED [by the designated member of staff]
6.5	Disciplinary proceedings:	Yes	**Where the warning relates to child protection issues see 1.2. If the disciplinary proceedings relate to a child protection matter please contact your safeguarding children officer for further advice.**		
6.5a	Oral warning			Date of warning + 6 months	SHRED[8]
6.5b	Written warning – level one			Date of warning + 6 months	SHRED
6.5c	Written warning – level two			Date of warning + 12 months	SHRED
6.5d	Final warning			Date of warning + 18 months	SHRED
6.5e	Case not found			If child protection related please see 1.2 otherwise shred immediately at the conclusion of the case	SHRED
6.6	Records relating to accident/injury at work	Yes		Date of incident + 12 years In the case of serious accidents a further retention period will need to be applied	SHRED
6.7	Annual appraisal/assessment records	No		Current year + 5 years	SHRED
6.8	Salary cards	Yes		Last date of employment + 85 years	SHRED
6.9	Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960), revised 1999 (SI 1999/567)	Current year, +3yrs	SHRED
6.10	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes		Current year + 6 years	SHRED
6.11	Proofs of identity collected as part of the process of checking "portable" enhanced CRB disclosure	Yes		Where possible these should be checked, and a note kept of what was seen and what has been checked. If it is felt necessary to keep copy documentation, then this should be placed on the member of staff's personal file.	

7 Health and Safety

	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
7.1	Accessibility Plans		Disability Discrimination Act	Current year + 6 years	SHRED
7.2	Accident Reporting		Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980		
7.2a	Adults	Yes		Date of incident + 7 years	SHRED

[8] If this is placed on a personal file it must be weeded from the file.

7.2b	Children	Yes		DOB of child + 25 years[9]	SHRED
7.3	COSHH			Current year + 10 years [where appropriate an additional retention period may be allocated]	SHRED
7.4	Incident reports	Yes		Current year + 20 years	SHRED
7.5	Policy Statements			Date of expiry + 1 year	SHRED
7.6	Risk Assessments			Current year + 3 years	SHRED
7.7	Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos			Last action + 40 years	SHRED
7.8	Process of monitoring of areas where employees and persons are likely to have come in contact with radiation			Last action + 50 years	SHRED
7.9	Fire Precautions log books			Current year + 6 years	SHRED

8 Administrative

	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
8.1	Employer's Liability certificate			Closure of the school + 40 years	SHRED	
8.2	Inventories of equipment and furniture			Current year + 6 years	SHRED	
8.3	General file series			Current year + 6 years	Review to see whether a further retention period is required	Transfer to Archives
8.4	School brochure or prospectus			Current year + 3 years		Transfer to Archives
8.5	Circulars (staff/parents/pupils)			Current year + 1 year	SHRED	
8.6	Newsletters			Current year + 1 year	Review to see whether a further retention period is required	Transfer to Archives
8.7	Visitors book			Last Date + 10 years	Review to see whether a further retention period is required	Transfer to Archives
8.8	PTA/Old Pupils Associations			Current year + 6 years	Review to see whether a further retention period is required	Transfer to Archives

[9] A child may make a claim for negligence for 7 years from their 18th birthday. To ensure that all records are kept until the pupil reaches the age of 25 this retention period has been applied.

9 Finance

	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
9.1	Annual Accounts		Financial Regulations	Current year + 6 years		Offer to the Archives
9.2	Loans and grants		Financial Regulations	Date of last payment on loan + 12 years	Review to see whether a further retention period is required	Transfer to Archives
9.3	Contracts					
9.3a	under seal			Contract completion date + 12 years	SHRED	
9.3b	under signature			Contract completion date + 6 years	SHRED	
9.3c	monitoring records			Current year + 2 years	SHRED	
9.4	Copy orders			Current year + 2 years	SHRED	
9.5	Budget reports, budget monitoring etc.			Current year + 3 years	SHRED	
9.6	Invoice, receipts and other records covered by the Financial Regulations		Financial Regulations	Current year + 6 years	SHRED	
9.7	Annual Budget and background papers			Current year + 6 years	SHRED	
9.8	Order books and requisitions			Current year + 6 years	SHRED	
9.9	Delivery Documentation			Current year + 6 years	SHRED	
9.10	Debtors' Records		Limitation Act 1980	Current year + 6 years	SHRED	
9.11	School Fund – Cheque books			Current year + 3 years	SHRED	
9.12	School Fund – Paying in books			Current year + 6 years then review	SHRED	
9.13	School Fund – Ledger			Current year + 6 years then review	SHRED	
9.14	School Fund – Invoices			Current year + 6 years then review	SHRED	
9.15	School Fund – Receipts			Current year + 6 years	SHRED	
9.16	School Fund – Bank statements			Current year + 6 years then review	SHRED	
9.17	School Fund – School Journey books			Current year + 6 years then review	SHRED	
9.18	Applications for free school meals, travel, uniforms etc.			Whilst child at school	SHRED	
9.19	Student grant applications			Current year + 3 years	SHRED	
9.20	Free school meals registers	Yes	Financial Regulations	Current year + 6 years	SHRED	
9.21	Petty cash books		Financial Regulations	Current year + 6 years	SHRED	

10 Property

	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
10.1	Title Deeds			Permanent	Permanent these should follow the property unless the property has been registered at the Land Registry	Offer to Archives if the deeds are no longer needed
10.2	Plans			Permanent	Retain in school whilst operational	Offer to Archives[10]

[10] If the property has been sold for private housing, then the archives service will embargo these records for an appropriate period of time to prevent them being used to plan or carry out a crime.

10.3	Maintenance and contractors		Financial Regulations	Current year + 6 years	SHRED	
10.4	Leases			Expiry of lease + 6 years	SHRED	
10.5	Lettings			Current year + 3 years	SHRED	
10.6	Burglary, theft and vandalism report forms			Current year + 6 years	SHRED	
10.7	Maintenance log books			Last entry + 10 years	SHRED	
10.8	Contractors' Reports			Current year + 6 years	SHRED	

11 Local Education Authority

	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
11.1	Secondary transfer sheets (Primary)	Yes		Current year + 2 years	SHRED	
11.2	Attendance returns	Yes		Current year + 1 year	SHRED	
11.3	Circulars from LEA			Whilst required operationally	Review to see whether a further retention period is required	Transfer to Archives

12 Catholic Education Service

	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
12.1	Returns	Yes		Current year + 1 year	SHRED	
12.2	Circulars from CES			Whilst required operationally	Review to see whether a further retention period is required	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]

13 Department for Children, Schools and Families

	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative Life of the record	
13.1	HMI reports			These do not need to be kept any longer		Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]
13.2	OFSTED reports and papers			Replace former report with any new inspection report	Review to see whether a further retention period is required	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]
13.3	Returns			Current year + 6 years	SHRED	
13.4	Circulars from Department for Children, Schools and Families			Whilst operationally required	Review to see whether a further retention period is required	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]

14 Connexions

	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
14.1	Service level agreements			Until superseded	SHRED
14.2	Work Experience agreement			DOB of child + 18 years	SHRED

15 Parent Pay

	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
15.1	Dinner Register			Current year + 3 years	SHRED
15.2	School Meals Summary Sheets			Current year + 3 years	SHRED

16 Family Liaison Officers and Parent Support Assistants

	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
16.1	Day Books	Y		Current year + 10 years then review	SHRED
16.2	Reports for outside agencies – where the report has been included on the case file created by the outside agency	Y		Whilst the child is attending the school then destroy	SHRED
16.3	Referral forms	Y		While the referral is current then destroy	SHRED
16.4	Contact data sheets	Y		Current year then review, if contact is no longer active then destroy	SHRED
16.5	Contact database entries	Y		Current year then review, if contact is no longer active then destroy	DELETE
16.6	Group Registers	Y		Current year + 2 years	SHRED

17 Other Records - Administration

	Basic file description	DP Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
Financial Records					
17.1	Financial records – accounts, statements, invoices, petty cash etc.	N		Current year + 6 years	
Insurance					
17.2	Insurance policies – Employers Liability	N	Employers Liability Financial Regulations	The policies are kept for a minimum of 6 years and a maximum of 40 years depending on the type of policy	
17.3	Claims made against insurance policies – damage to property	Y		Case concluded + 3 years	
17.4	Claims made against insurance policies – personal injury	Y		Case concluded + 6 years	

Human Resources					
17.5	Personal Files - records relating to an individual's employment history	Y[11]		Termination + 6 years then review	
17.6	Pre-employment vetting information (including CRB checks)	N	CRB guidelines	Date of check + 6 months	
17.7	Staff training records – general	Y		Current year + 2 years	
17.8	Training (proof of completion such as certificates, awards, exam results)	Y		Last action + 7 years	
	Premises and Health and Safety				
17.9	Premises files (relating to maintenance)	N		Cessation of use of building + 7 years then review	
17.10	Risk Assessments	N		Current year + 3 years	

Created June 2018

[11] For Data Protection purposes the following information should be kept on the file for the following periods:

- all documentation on the personal file. Duration of employment
- pre-employment and vetting information Start date + 6 months
- records relating to accident or injury at work (Minimum of 12 years)
- annual appraisal/assessment records (Minimum of 5 years)
- records relating to disciplinary matters (kept on personal files)
    - oral warning (6 months)
    - first level warning (6 months)
    - second level warning (12 months)
    - final warning (18 months)

PART G

DATA BACKUP POLICY

1. Definitions

- School Network – the devices attached to the Network through Data cabling or Wifi.
- Users – the workforce and students who are given authorised to log on to the School Network.

2. Introduction

St Peter's will back up all of its data and IT systems on a regular basis to ensure ease of recovery in the event of loss (malicious or accidental) or contamination.

3. Objectives of Data Backup Policy

- To maintain the integrity of the School's Data.
- To reduce the risk of cybercrime committed against the school.
- To reduce the impact and recovery time of the School in response to an IT system failure.

4. Statement of Intent

- **Fileserver:** All the Data pertaining to the Users of the School network are backed-up daily, at an incremental level, over a 30 day period and held offsite in accordance with the Data Protection Act and GDPR. Current Maximum retention period is 6 months (any changes made before this period will not be able to be recovered).
- **SIMS:** All the Data contained as part of the School's Information Management System is backed-up daily, at an incremental level, over a 30 day period and held offsite in accordance with the Data Protection Act and GDPR. Current Maximum retention period is 6 months (any changes made before this period will not be able to be recovered).
- **VSphere:** All the server infrastructure (Server Farm) is backed-up weekly at an incremental level and held offsite in accordance with the Data Protection Act and GDPR. Current Maximum retention period is 6 months (any changes made before this period will not be able to be recovered).

Created: June 2018
Due for review July 2020

BRING YOUR OWN DEVICE (BYOD) POLICY

1. Definitions:

- The School – St Peter's School.
- School Network – the devices attached to the Network through Data cabling or Wifi.
- Users – the workforce and students who are given authorised to log on to the School Network.
- BYOD – Bring your own Device (a device not owned by the School but used to access School digital resources (e.g. Email, Wifi, connect to a computer, remote gateway access,)
- School Community – The workforce and students of the St Peter's School.
- ICT Support Team – The staff employed by St Peter's School to maintain the School's Network and associated systems.

2. Introduction:

The School recognises that members of the School Community may have need to use BOYD whilst at school. In addition, they may also use BYOD to access school systems from home or while mobile (e.g. the remote gateway and Office 365). The School accepts NO responsibility for any loss or damage to the device. Furthermore, the ICT Support Team will not be responsible for any maintenance of a BYOD.

3. Objectives:

- To minimise the risk of Personal Data breaches.
- To minimise the risk of a cyber-attack.

4. Statement of Intent:

BYOD are allowed to connect to the school's Wifi (JOIN) network as long as the device is registered using the Users School Network Credentials.

In the first instance, BYOD should only use the remote gateway to access/view personal data. However, it there may be a need to store personal in a file and where this is the case it MUST be encrypted (This includes using Storage Media e.g. USB drives). Please note, the preferred storage place for files containing personal information is the School Network or on Office 365 OneDrive and SharePoint, as these are automatically encrypted.

Where BYOD are used to access Personal Data via Third Party Systems (e.g. Office 365) they should also have an extra level of encryption (e.g. a pin code or password to access).

With all BYODs, passwords for school resources and Third Party Systems should not be stored so that other users of the device can access without affirming the associated password.

Updated: June 2018
Approved by TLA 4 July 2018
Ratified by Full Governing Body: 18 July 2018
Due for review July 2020