ST PETER'S

PREPARATORY SCHOOL

Data Protection Policy

Updated on 3 April 2025
by Mr Dan Morris
(Director of Operations & Compliance)

Approved by Head: 

Date: 28 April 2025

Contents

General Data Protection Regulation

Rationale: From May 25 2018, all business registered as Data Controllers with the Information Commissioner's Office are required to process data ...in accordance with the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**, which together form the UK's primary data protection legislation.

Linked Policies - GDPR Privacy Notice, Taking, Storing and Using Images of Children Policy, Child Protection & Safeguarding Policy, CCTV Policy, Health and Safety Policy, IT Use Policy, Social Media Policy and e-Safety Policy.

Point of Contact: Director of Operations & Compliance

Aims

- To ensure that SPL Education Ltd trading as St Peter's Preparatory School's ("the School's") procedures and record keeping comply with current data protection legislation (EU General Data Protection Regulation)
- To provide guidelines to staff regarding the rights of individuals for whom the School processes data

General Data Protection Regulation

Schools hold information on both pupils and staff and, in doing so, must follow the requirements of this EU Legislation. GDPR covers the collection, storing, editing, retrieving, disclosure, archiving and destruction of personal data. The Act applies to data held on paper as well as electronically.

Personal data is defined as data (fact and opinion) that is held on a living individual who can be identified from the data itself. The school processes personal data regarding staff, pupils and their parents/guardians as well as contractors, volunteers and alumni. This involves obtaining, recording, holding, disclosing, destroying and using data.

It is important that all staff are very careful about the content of school information as the General Data Protection Regulation allows individuals to find out what data is held about themselves by the School and the rights that they hold regarding that data. This is documented within the School's Privacy Notice.

SPL Education Ltd is required to register with the Information Commissioner's Office as a 'data controller'. All those employees who handle data within the School are 'data processors'.

Under GDPR, the 'data protection principles' set out the main responsibilities of organisations regarding individuals' data:

GDPR requires that personal data shall be:

"a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) 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;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) 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;

e) 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 in the public interest, scientific or historical research 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; and

f) 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."

Article 5(2) requires that:

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

Responsibilities

The school is responsible for:

- ensuring that staff are provided with a copy of this policy and that it is explained at induction and during staff refresher courses;
- appointing a Privacy and Compliance Officer to ensure that all personal data is processed in compliance with this policy and the General Data protection Regulation
- ensuring information with regard to pupils, parents and staff and other individuals for whom the school legitimately holds data is not released without the written permission of the person(s) concerned.
- ensuring that the Privacy Notice and all its associated policies are published on the School website and are accessible to an individual who requests them.

  The School will carry out a **Data Protection Impact Assessment (DPIA)** before processing personal data that is likely to result in a high risk to individuals' rights and freedoms. Examples include the introduction of new technologies, large-scale surveillance, or processing special category data. The DPIA will assess the necessity, risks, and mitigation strategies for the proposed data processing activity.

Data Processing

Under GDPR, data processing may only be carried out if the individual has given his or her consent, and under 'legitimate use'

- the processing is necessary for the performance of a contract with the individual;
- the processing is required under a legal obligation;
- the processing is necessary to protect the vital interests of the individual;
- the process is necessary to carry out public functions;
- the processing is necessary in order to pursue the legitimate interests of the data controller or third parties.

The processing of sensitive data (racial or ethnic origin; political opinions; religious or other beliefs; trade union membership; health/medical; sex life; criminal proceedings or convictions) can only be processed if:

- the explicit consent, in writing, of the individual is obtained;
- the data are required by law for employment purposes or the administration of justice or legal proceedings;
- protection of the vital interests of the data subject or another.

The following data are exempt from the right of access under GDPR:

- information which identifies other individuals;
- information which the School believes is likely to cause damage or distress;
- information to which the legal profession has privileged rights.

Where data is processed under the lawful basis of **legitimate interest**, St Peter's Preparatory School will carry out a **Legitimate Interest Assessment (LIA)**. This is a structured three-part test:

1. **Purpose test** – is there a legitimate interest behind the processing?
2. **Necessity test** – is the processing necessary for that purpose?
3. **Balancing test** – is the legitimate interest overridden by the individual's rights, freedoms, or interests? The outcome of each LIA will be documented and reviewed periodically.

Use of Digital Images

For the purposes of this section, publication includes on websites, in the press, on TV, as web broadcasts or video/CD/DVD to be released into the public domain.

- Written permission from parents or carers will be obtained before photographs of pupils are published as outlined in the School's Taking and Storing of Images of Children Policy.
- When a parent does not agree to their child's photograph being used, the Head will inform staff and staff must make every effort to comply.
- As indicated in the Taking and Storing of Images of Children Policy, the naming of published images of pupils will be avoided wherever possible. This includes photographs, videos, TV presentations, web pages and the press. Where named images must be used then specific written permission from parent or guardian must be obtained.
- The School will monitor the use of cameras and anyone behaving inappropriately at extracurricular events. If there are concerns, the Head can require the person to cease using the camera or leave the premises.
- The Head or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The copyright of all material must be held by the School, or be attributed to the owner where permission to reproduce has been obtained.

Staff Use of Internet and Email

All internet activity should be conducted within the terms of the School's IT Use Policy; it should be appropriate to staff's professional activity or pupil education. Use for personal financial gain, gambling, political purposes or advertising is forbidden.

Access should only be made via the authorised account and password.

Unsuitable material (pornographic, racist, offensive) must not be deliberately accessed and downloaded. Should unsuitable material be accidentally accessed, the IT Support Officer, Director of Operations & Compliance and the Head must be immediately informed. As outlined in the Social Media policy, staff must not become 'friends' of pupils on social network sites.

Users are responsible for their email and must ensure that the content is professional and appropriate. Posting anonymous messages and forwarding chain letters is forbidden.

Email contacts must not be given without the permission of the person(s) concerned. BCC enables emails to be copied without disclosing the email address. The content of email must be strictly for the recipient(s) and a disclaimer used on all emails, see Annex 2.

The content of email must be polite and of the standard normally required by St Peter's. The following disclaimer may be used for confidential letters:

This letter is confidential and may not be read, copied, distributed, disclosed to or otherwise used by anyone other than the recipient.

Copyright of materials must be adhered to.

Breach of the above is a serious offence and will lead immediately to disciplinary action.

On leaving the school, school email accounts will be suspended and will not be accessible to the previous staff member.

Computer Security

The Director of Operation, supported by IT Support Officer & 3rd Party IT Support Company, CAPtech are responsible for ensuring that:

- procedures comply with GDPR;
- only licensed software is used;
- access controls are set with appropriate levels of security;
- passwords are used by only one person, changed regularly and not disclosed to another person;
- computer use is legitimate and that staff are aware of their responsibilities and security levels for data access;
- only authorised terminals are connected to the network system and that these are logged off immediately after use, or locked if being left unattended.
- access rights are cancelled as soon as staff leave;
- information is secured against loss or corruption;
- Staff ensure that waste computer output (printouts, CDs etc.) are immediately disposed of in a secure manner.

The security and confidentiality of information is extremely important. Some computer crimes are now criminal offences and prison sentences can be imposed. A manager may be charged as well as the person committing the crime. See Annex 1: Computer Security Legislation.

Computer data requires different levels of security and access, depending upon the degree of confidentiality. Some data are intended for easy use and access is not restricted. However, all data needs to be secured against loss or corruption.

Sensitive and confidential data e.g. pupil files, budgets should not, be saved onto portable storage devices such as USB memory sticks. The use of online cloud storage would be preferable for such tasks. If there is no alternative means of transferring the data, permission from SMT should be obtained. Data on the drives must be encrypted and the data deleted once it has been transferred to the appropriate and secure system. Care must be taken that the stick is not lost or carelessly mislaid.

Staff passwords must be changed on a termly basis.

Computer Equipment

All computer equipment must be adequately protected against theft, malicious damage or unreasonable environmental surroundings. Access devices such as keys, card keys, passwords or codes must not be transferred to another person. Computer equipment is not insured if:

- Taken from an unattended vehicle that is not securely locked

- Left visible in a locked vehicle
- Taken abroad on a non-work based visit
- Not in the possession of a duly authorised representative of St Peter's.

The physical security of each piece of computer equipment in the School is the responsibility of DIrector of Operations alongside the Senior Management Team.

Wherever possible, administration terminals should be placed in positions that only allow the screen's display to be seen by authorised staff.

All confidential output must be stored securely when not in use.

Backups

With the use of Google Drive's Cloud Storage, fewer files are stored on the school network. However, copies of computer files that are still stored in this location are taken by the IT Network Manager regularly from the servers (the frequency to be determined for each application), users files are synchronised to the network each time that they logon to the network. For machines that are not connecting regularly or never to a network then an external backup device must be used for this purpose. Copies must be stored securely away from the computer. Recovery procedures for all important systems must be specified in the School's IT Disaster Recovery Plan. They should be reviewed and tested periodically to ensure that they are still workable.

Privacy

Through the use of network drives, every effort must be made to ensure that confidential information can only be accessed by persons who have permission to see it.

Software Viruses

St Peter's machines are protected by a current virus checking program. Personal machines must not be used on a school/office network system unless they have been passed as 'clean' by the IT network manager and all necessary links to the internet filtering system have been established.

Acquisitions

Purchase of non consumable IT equipment must is managed by the IT Network Manager. All purchases of ICT equipment must be entered into the asset register.

Intellectual Rights

Unauthorised copies of licensed software must not be made. St Peter's may fund and facilitate the development of software that enhances the professional standing and status of the company. In such instances, a contract will be drawn-up specifying remuneration and copyright.

Policies, planning and school documentation are the property of the School. When a member of staff leaves they must not copy these (electronically or on paper). See contract documentation for further details.

Personnel Policy

Any employee knowingly breaching this policy may be subject to disciplinary proceedings.

These breaches include:

- unauthorised use of passwords;
- unauthorised disclosure of information;
- deliberate and unauthorised access to, copying of, alteration to or interference with computer programs or data;
- loading of "pirate" or borrowed software.

- If a member of staff resigns or is suspended or dismissed, the security of computer equipment and data must be immediately addressed.

An employee may be subject to disciplinary procedures for:

- unauthorised use of passwords;
- deliberate and unauthorised access to, copying of, alteration to or interference with computer programs or data;
- unauthorised disclosure of information.

Access to Personal Data

Staff personal files are stored in a locked cabinet in the School Meeting room. Pupil files are stored in the locked marketing office. Access to staff files/records is restricted to the Head and Head's PA and others on St Peter's SMT, where appropriate.

Furlong's SchoolBase Management Information System is used to store pupil and staff data.

The Head is responsible for ensuring that files are checked annually to ensure that the information stored is accurate and relevant. No private written records are to be kept by a member of staff.

Any parent/guardian/member of staff (data subject) wishing to access any of their personal data should put the subject access request (SAR) in writing to the Privacy and Compliance Officer (Assistant Head, Operations.) The School must respond to any such written requests within 30 days. Before providing the information, the School will need to verify the identity of the person making the request using "reasonable means". This would be in the format of an accepted form of identification.

Where the Data Subject makes an SAR by electronic means and, unless otherwise requested by the Data Subject, the information will be provided in a commonly used electronic format.

In the case of paper personnel files, the Head or a member of the SMT must be present whilst the file is being examined. The person examining the file must sign and date any documents in the file

that s/he has examined. Copies may be provided if requested. Electronic data will be transferred by means agreed with the individual making the request.

The rights under GDPR are the individual's to whom the data relates. The School will rely on parental/guardian consent to process data relating to pupils and will only grant pupils direct access to their personal data if they are aged 13 or in the School's reasonable belief, the pupil understands the nature of the request.

The School will not comply with requests by pupils that personal data are not disclosed to parents/guardians unless the school believes disclosure of the information is likely to put the pupil in danger or cause damage or distress. In such cases, the Head and Designated Safeguarding Lead must consult and, if necessary, seek advice from other safeguarding agencies

As outlined in the School's Privacy notice, the School takes reasonable steps to verify the identity and GDPR compliance of any third party before sharing any personal data

The School will not disclose or publish information at the request of a third party without the consent of the parent/guardian (individual).

The full names of individual pupils will not be published including publication on the school website.

Within the Taking, using and storing images of children policy, parental permission must be obtained prior to using photographs or information for publicity purposes, including newspapers.

Pupils or staff are not allowed to use mobile phones to take photographs or videos of pupils at any time. For more information on images of pupils please see the Taking, storing and using images of children as well as the Safeguarding Policy.

Personal Data Breach Management

In the event of a personal data breach (e.g. accidental loss, disclosure, or unauthorised access), the School will:

- Assess the scope, severity, and risk to data subjects.
- Document all details related to the breach and the School's response.
- Notify the Information Commissioner's Office (ICO) within 72 hours, if the breach is likely to result in a risk to the rights and freedoms of individuals.
- Notify affected individuals without undue delay, where there is a high risk to their rights or freedoms.

All staff must report any suspected data breach to the Privacy and Compliance Officer immediately.

Disclosure of Business Information

During and following employment employees must **not** use or disclose any confidential information relating to the business or financial affairs of SPL Education Ltd to any person, firm, company or other body so long as the information remains confidential.

Copyright and Licences

Operating manuals and handbooks, all notes, memoranda, records, correspondence, computer and other discs and tapes and all other documents and material whatsoever (whether made or created by the employee or otherwise) relating to the affairs of the Company or the School shall be and remain the property of the Company and shall be handed over by employees to the Company when they leave.

Copyright is an unregistered right (unlike patents, registered designs or trade marks). Therefore, there is no official action to take (no application to make, forms to fill in or fees to pay). Copyright comes into effect immediately, as soon as something that can be protected is created and "fixed" in some way, e.g. on paper, on film, via sound recording, as an electronic record on the internet, etc. Copyright work should be marked with the copyright symbol © followed by your name and the date, to warn others against copying it, but it is not legally necessary in the UK.

The Assistant Head, Complianceis responsible for ensuring that the necessary copyright licenses are obtained as follows:

	CLA	ERA	PPL	PRS	MCPS	CCLI
Reproducing of hymns and worship songs.						√
School play, concert, live or recorded music.			√	√		
Radio or television broadcast for educational purposes.		√				
Photocopying articles from journals, magazines or books.	√					
Playing radio/CD/tape in administration offices or staffroom.			√	√		
School disco, fete or fair outside school hours where music played.			√	√		
Overhead transparencies from journals, magazines or books.	√					
Hiring premises for keep fit/aerobics.			√	√		
After school film/video club.				√		
Music on hold on telephone system.			√	√	√	
Creating or storing school's computer system the school's own hymn book or carol sheets.						√

Video or audio recordings of school carol service or other religious/seasonal festival to circulate to parents.					√	√
Recording school concert, play other event containing music.					√	

Key

CLA – The Copyright Licensing Agency Ltd licenses the photocopying of extracts from books, journals and magazines.

ERA – The Educational Recording Agency Ltd licenses designated educational establishments to record radio and television broadcasts for non-commercial educational purposes.

PPL – represents the UK record industry, licensing the use of sound recording (CDs, tapes, discs etc.) on behalf of record companies and performers. Licences are issued for extra curricular use of copyright sound recordings on school premises.

PRS – is the copyright collection society for composers and publishers of music. It licenses the extra curricular use of copyright music on school premises, including PA events and use by hirers.

MCPS – represents its composer and publisher members, whenever a musical work is recorded on a CD, tape, video or DVD or when the recording is issued to the public. This applies to the recording of school concerts, plays or other events.

CCLI – Christian Copyright Licensing (Europe) Ltd. is the UK's major licensing body for the reproduction of hymns and songs used during assemblies. CCLE can license schools to reproduce the lyrics and music of many thousands of songs: written; stored on computer; photocopied; acetate sheets.

Retention of Records / Archiving Documents

The GDPR requires that personal data is only retained for as long as necessary – that is, necessary for the specific lawful purpose (or purposes) it was acquired.

Therefore at the end of each school year the School evaluates its storage of personal and special category data and, in line with its Privacy notice, will retain, archive or destroy data accordingly.

The following table indicates the current DfE guidance on record retention to which the School adheres:

Type of Record/Document	Suggested Retention Period
SCHOOL-SPECIFIC RECORDS Registration documents of School Attendance Register Minutes of Board of Reference meetings Annual curriculum	 Permanent (or until closure of the school) 6 years from last date of entry, then archive. 6 years from date of meeting From end of year: 3 years (or 1 year for other class records: eg marks / timetables / assignments)
INDIVIDUAL PUPIL RECORDS Admissions: application forms, assessments, records of decisions Examination results (external or internal) Pupil file including: ● Pupil reports ● Pupil performance records ● Pupil medical records ● Special educational needs records (to be risk assessed individually)	**NB – this will generally be personal data** 25 years from date of birth (or, if pupil not admitted, up to 7 years from that decision). 7 years from pupil leaving school ALL: 25 years from date of birth (subject to where relevant to safeguarding considerations: any material which may be relevant to potential claims should be kept for the lifetime of the pupil). Date of birth plus up to 35 years (allowing for special extensions to statutory limitation period)

SAFEGUARDING	NB – please read notice at the top of this note Keep a permanent record of historic policies
Policies and procedures	No longer than 6 months from decision on recruitment, unless DBS specifically consulted – but a record of the checks being made must be kept, if not the certificate itself.
DBS disclosure certificates (if held)	Keep on record for as long as any living victim may bring a claim (NB civil claim limitation periods can be set aside in cases of abuse). Ideally, files to be reviewed from time to time if resources allow and a suitably qualified person is available. [2]
Accident / Incident reporting	If a referral has been made / social care has been involved or child has been subject of a multi-agency plan – indefinitely.
Child Protection files	If low level concerns, with no multi-agency action – apply applicable school low-level concerns policy rationale (this may be 25 years from date of birth OR indefinitely).

Type of Record/Document	**Suggested[1] Retention Period**
CORPORATE RECORDS (where applicable)	e.g. where schools have trading arms
Certificates of Incorporation	Permanent (or until dissolution of the company)
Minutes, Notes and Resolutions of Boards or Management Meetings	Minimum – 10 years
Shareholder resolutions	Minimum – 10 years
Register of Members/Shareholders	Permanent (minimum 10 years for ex-members/shareholders)
Annual reports	Minimum – 6 years
ACCOUNTING RECORDS[3]	
Accounting records (normally taken to mean records which enable a company's accurate financial position to be ascertained & which give a true and fair view of the company's financial state) [NB specific ambit to be advised by an accountancy expert]	Minimum – 3 years for private UK companies (except where still necessary for tax returns) Minimum – 6 years for UK charities (and public companies) from the end of the financial year in which the transaction took place Internationally: can be up to 20 years depending on local legal/accountancy requirements
Tax returns	Minimum – 6 years

VAT returns	Minimum – 6 years
Budget and internal financial reports	Minimum – 3 years
CONTRACTS AND AGREEMENTS	
Signed or final/concluded agreements (plus any signed or final/concluded variations or amendments)	Minimum – 7 years from completion of contractual obligations or term of agreement, whichever is the later
Deeds (or contracts under seal)	Minimum – 13 years from completion of contractual obligation or term of agreement
INTELLECTUAL PROPERTY RECORDS	
Formal documents of title (trade mark or registered design certificates; patent or utility model certificates)	Permanent (in the case of any right which can be permanently extended, e.g. trade marks); otherwise expiry of right plus minimum of 7 years.
Assignments of intellectual property to or from the School	As above in relation to contracts (7 years) or, where applicable, deeds (13 years).

Type of Record/Document	Suggested Retention Period
IP / IT agreements (including software licences and ancillary agreements e.g. maintenance; storage; development; coexistence agreements; consents)	Minimum – 7 years from completion of contractual obligation concerned or term of agreement
EMPLOYEE / PERSONNEL RECORDS Single Central Record of employees Contracts of employment Employee appraisals or reviews Staff personnel file Payroll, salary, maternity pay records Pension or other benefit schedule records Job application and interview/rejection records (unsuccessful applicants) Immigration records Health records relating to employees	NB this will contain personal data Keep a permanent record of all mandatory checks that have been undertaken (but not DBS certificate itself: 6 months as above) 7 years from effective date of end of contract Duration of employment plus minimum of 7 years As above, but do not delete any information which may be relevant to historic safeguarding claims. Minimum – 6 years Possibly permanent, depending on nature of scheme Minimum 3 months but no more than 1 year Minimum – 4 years 7 years from end of contract of employment
INSURANCE RECORDS Insurance policies (will vary – private, public, professional indemnity) Correspondence related to claims/ renewals/ notification re: insurance	Duration of policy (or as required by policy) plus a period for any run-off arrangement and coverage of insured risks: ideally, until it is possible to calculate that no living person could make a claim. Minimum – 7 years
ENVIRONMENTAL, HEALTH & DATA Maintenance logs Accidents to children Accident at work records (staff) Staff use of hazardous substances	10 years from date of last entry 25 years from birth (longer for safeguarding) Minimum – 4 years from date of accident, but review case-by-case where possible

	Minimum – 7 years from end of date of use
Risk assessments (carried out in respect of above) [4] Data protection records documenting processing activity, data breaches	7 years from completion of relevant project, incident, event or activity No limit: as long as up-to-date and relevant (as long as no personal data held)
Emails on Server ● Pupil Email Accounts ● Staff Emails	● Delete upon leaving the school. ● Rescind Staff Access upon leaving employment, emails accessible by school admin for up to 3 years.

EXPLANATORY NOTES:

1. Some of these periods are mandatory legal requirements (e.g. under the Companies Act 2006 or the Charities Act 2011), but others are based on practical considerations for retention such as limitation periods for legal claims, and guidance from Courts, weighed against whether there is a reasonable argument in respect of data protection.

2. The High Court has found that a retention period of 35 years was within the bracket of legitimate approaches. It also found that it would be disproportionate for most organisations to conduct regular reviews, but at the time of writing the ICO (Information Commissioner's Office) still expects to see a responsible assessment policy (e.g. every 6 years) in place.

3. Retention period for tax purposes should <u>always</u> be made by reference to specific legal or accountancy advice.

4. As latent injuries can take years to manifest, the limitation period for claims reflects this: so records of procedures as they were at the time are also kept alongside relevant insurance documents.

Archive

Archived documentation is kept in the school secure archive store. Data is boxed, labelled and secured within the store.

Data to be destroyed

For confidential, sensitive or personal information to be considered securely disposed of, it must be in a condition where it cannot either be read or reconstructed. Therefore paper records are burned or shredded using a cross-cutting shredder; CDs / DVDs / diskettes should be cut into pieces. Hard-copy images, AV recordings and hard disks are dismantled and destroyed.

Where third party disposal experts are used, they are supervised wherever possible.

……

Acceptance

Please indicated with your name and signature below that you have read, understood and agree to comply with this data protection policy during and after your employment with SPL Education Ltd trading as "St Peter's Preparatory School"

Name (please print) ……

Position……

Signature …… Date ……..

Revision History		
Date Revised	**Changes**	**Reviewed By**
03 Apr 2025	Added Personal Breach Management and clarity around Legitimate Interests.	Dan Morris (Dir. of Operations)

Annex 1: Computer Security Legislation

Copyright, Designs & Patents Act 1988

This Act makes it a criminal offence carrying a maximum sentence of two years imprisonment for managers to distribute, or let staff distribute, illegal copies of software within their organisation.

All software being used within departments must have adequate software licences. Packages run on hard disc machines must have their own individual copy. Sufficient copies of floppy discs/CD ROMS must be purchased so that copies are used on only one machine at any given time. However, one disc/CD ROM can be licensed for multiple users.

Copyright in a work is infringed by a person who without licence of the copyright owner does, or authorises another to do, any of the acts restricted by the copyright.

If any person fails to comply with any direction given under this Act or makes or causes to be made an application for the registration of a design in contravention of that section, s/he shall be guilty of an offence and liable to conviction and imprisonment.

The Computer Misuse Act, 1990

This act details three new offences:

- unauthorised access including "hacking" or eavesdropping where the contents of computer files are modified;
- ulterior intent whereby legal power includes both the use of a computer to commit an offence and also, where it aids the committing of another offence;
- unauthorised modification whereby an offence is committed if any action by the offender causes unauthorised modification of the contents of a computer with the intention of disrupting or damaging its contents.

Unauthorised Access (Hacking)

Examples of offences:

- deliberately attempting to access a computer knowing that you are not allowed such access, this applies to just switching on a computer without authority to use it;
- trying out a list of passwords – an offence is committed as soon as the computer shows an error message;
- using telephone networks to search computer lines.

Ulterior Intent (Hacking with intent to commit a serious crime)

This is deliberately attempting to access a computer without authority but with the intention to commit a serious crime. This offence is much more serious than unauthorised access, and to be proved it is necessary to show:

- there was a deliberate access to a computer;
- they had no authority to do so;
- they knew they were not authorised;

- there was an intention of using the information to commit a further offence.

The penalties are severe – five years' imprisonment (or more) and an unlimited fine.

Unauthorised Modification (Destruction or alteration of programs or data)

This is intentionally and without authorisation destroying or altering data or programs. This covers viruses, worms, logic bombs, Trojan horses etc. A person is guilty of this offence if:

- s/he does any act which causes an unauthorised modification of the contents of any computer;
- at the time he does the act he has the requisite intent and the requisite knowledge.

The requisite intent is an intent to cause modification to the contents of any computer and by so doing:

- impair the operation of any computer;
- prevent or hinder access to any program or data on any computer;
- impair the operation of any such program or the reliability of such data.

The penalties for this are an unlimited fine and up to five years' imprisonment.

In all of the above the burden of proof will fall on an organisation's electronic records of access and, consequently, security procedures will be open to scrutiny.

Annex 2: Email Footer/Disclaimer

[Name]
[Position]
St. Peter's Preparatory School
Harefield, Lympstone, Devon
EX8 5AU
Tel: 01395 272148

THE GOOD SCHOOLS GUIDE

Read our review here [link to Good School's Guide review]

This email and any attachments are confidential and may also be privileged. If you have received this message in error, please (a) notify the sender immediately, (b) destroy this email and any attachments, and (c) do not use, copy, store and/or disclose to any person this email and any attachments. In the event of any technical difficulty with this email and any attachments, please contact the Director of Operations on 01395 272148.

St Peter's Preparatory School is a part of SPL Education Ltd. SPL Education Ltd is a Limited Company registered in England and Wales. Company Number 01788139 with registered offices at St Peter's Preparatory School, Harefield, Lympstone, Devon, EX8 5AU