ST PAUL'S SCHOOL
Est. 1509

e-Safety Policy

Author/reviewer responsible:	DHA	ISI DOC CODE:	7
Reviewed by:	ICT Committee	Date of last review:	06/18
Authorised by resolution of:	EdExec	Date of authorisation:	07/19
Applicable:	**SPS & SPJ**	Date of next review:	06/20

This policy is available on the Handbook page of the School Intranet and policies page of the School website and can be made available in large print or other accessible format if required; such requests can be made by email to policyquery@stpaulsschool.org.uk

Contents

Development / Monitoring / Review of this Policy

This e-Safety Policy has been developed by the ICT Committee and sanctioned by the Operational Executive.

Schedule for Development / Monitoring / Review of this Policy

This e-Safety policy will be reviewed annually by the Governing Body:	Annually, usually at the June meeting
The implementation of this e-Safety policy will be monitored by:	The ICT Committee, responsible to the Safeguarding Committee
Monitoring will take place at regular intervals:	Termly – a standing item on the ICT Committee agenda
The Governing Body will receive a report on the implementation of the e-Safety policy generated by the monitoring group (which will include anonymous details of e-Safety incidents) at regular intervals:	Annually
The e-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-Safety or incidents that have taken place. The next anticipated review date will be:	June 2019

Should serious e-Safety incidents take place, either the High Master (SPS) or the Head (SPJ) or the e-Safety Governor (if the incident involves any one of the above) will be informed. They will determine what action to be taken. If the issue involves safeguarding concerns, then the Safeguarding and Child Protection Policy will be followed in order to determine whether to inform external persons / agencies.	

The school will monitor the impact of the policy using:

- *Logs of reported incidents*
- *Monitoring logs of internet activity (including sites visited)*

Scope of the Policy

3.1 This policy applies to all members of the school community (including staff, pupils, parents, visitors) who have access to and are users of school ICT systems, both in and out of the school.

3.2 The School will deal with e-Safety incidents in accordance with the procedures outlined in both this policy and in associated school policies, such as the safeguarding and child protection, behaviour and anti-bullying policies. It will, where known and appropriate, inform parents of incidents of inappropriate e-Safety behaviour that take place out of school.

Roles and Responsibilities

Governors

4.1.1 Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. This is carried out by the Health and Safety Committee receiving regular information about e-Safety incidents and monitoring reports. The e-Safety Governor is nominated by the Governing Body. The role of the e-Safety Governor includes:

- Receipt of the termly e-Safety report from the e-Safety Officers
- Regular monitoring of e-Safety incident logs
- Regular monitoring of changes to filtering
- Reporting to relevant Governors' meetings

High Master, Head Master and Senior Management Team

4.2.1 The High Master and Head have a duty of care for ensuring the safety (including e-Safety) of members of the school community, though the day to day responsibility for e-Safety will be delegated to the e-Safety Officers, reporting to the ICT Committee.

4.2.2 The High Master, Head, Designated Safeguarding Leads (DSLs) and deputy DSLs in both schools should be aware of the procedures to be followed in the event of a serious e-Safety allegation being made against a member of staff.

4.2.3 The Safeguarding Committee will receive a termly monitoring report from the e-Safety Officers.

E-Safety Officers: There are three e-Safety Officers: the Director of ICT at SPS, the Director of Computing at SPJ and the IT Manager. They:

4.3.1 Are members of the e-Safety Committee, which is the ICT Committee.

4.3.2 Take day to day responsibility for e-Safety issues and have a leading role in establishing and reviewing the school e-Safety policies and documents.

4.3.3 Email staff at the start of each year to remind them of the procedures that need to be followed in the event of an e-Safety incident taking place.

4.3.4 Arrange for the provision of training and advice for staff, parents and Governors (in liaison with the Head of PSCHE at SPJ and SPS).

4.3.5 Are responsible for e-Safety education for pupils.

4.3.6 Receive reports of e-Safety incidents and create a log of incidents to inform future e-Safety developments – details are in the section 'Responding to Incidents of Misuse' section of this policy.

4.3.7 Meet as necessary with the e-Safety Governor to discuss current issues, review incident logs and changes to filtering – see 4.1 above.

4.3.8 Report regularly to the Health and Safety Committee.

4.3.9 Report regularly to the Safeguarding Committee.

4.3.10 Deal with incidents in liaison with the DSLs.

The IT Manager: is responsible for ensuring the following:

4.4.1 That the school's technical infrastructure is secure and is not open to misuse or malicious attack.

4.4.2 That the School meets all e-Safety technical requirements as laid out in the Internet Security Information document.

4.4.3 That users may only access the school's networks and devices if properly authenticated and authorised.

4.4.4 The filtering policy is applied and updated on a regular basis.

4.4.5 That they keep up to date with e-Safety technical information in order to carry out their e-Safety role effectively and to inform and update others as relevant.

4.4.6 That the use of the school's networks and devices is regularly monitored to ensure compliance with the Acceptable Use Policies (AUPs) in order that any misuse or attempted misuse can be identified and reported to the appropriate person for investigation.

4.4.7 That monitoring software and systems are kept up to date.

Teaching and Support Staff: are responsible for ensuring that:

4.5.1 They have an up to date awareness of e-Safety matters and of the current e-Safety policy and practices.

4.5.2 They have read, understood and agreed to the Staff AUP agreement.

4.5.3 They report any suspected misuse or problem to the appropriate person for investigation.

4.5.4 All digital communications with other staff, pupils and parents are on a professional level.

4.5.5 They help pupils understand and follow the e-Safety and acceptable use policies.

4.5.6 They help pupils acquire a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

Designated Safeguarding Leads

4.6.1 Designated Safeguarding Leads are trained in e-Safety issues and made aware of the potential for serious child protection and safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying
- Prevent

The e-Safety Committee: Members of the e-Safety Committee (ICT Committee) will assist the e-Safety Officers with:

4.7.1 The production, review and monitoring of the school e-Safety policy and documents.

4.7.2 The production, review and monitoring of the school filtering arrangements as laid out in the Internet Security Information document, and requests for filtering changes.

4.7.3 Mapping and reviewing the e-Safety curricular provision – ensuring relevance, breadth and progression.

4.7.4 Monitoring incident logs.

4.7.5 Consulting stakeholders – including parents and pupils about the e-Safety provision.

4.7.6 Monitoring identified improvement actions.

Pupils

4.8.1 Are responsible for using the school digital technology systems in accordance with the Pupil AUP Agreements for St Paul's Juniors and St Paul's School.

4.8.2 Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

4.8.3 Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.

4.8.4 Should understand the importance of adopting good e-Safety practice when using digital technologies out of school and realise that the school's e-Safety Policy covers their actions.

Parents: play a crucial role in ensuring that their children understand the need to use the Internet / mobile devices in an appropriate way. Parents are asked to support the school in promoting good e-Safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events.
- Access to the Parent Portal.
- Their children's personal devices in the school.

Community Users: who access school systems as part of the wider school provision will be expected to sign a Visitors' AUP agreement before being provided with access to school systems.

Policy Statements

Education – Pupils

e-Safety should be a focus in all areas of the curriculum and staff should reinforce e-Safety messages across the curriculum. The e-Safety curriculum should be broad, relevant and provide progression, and will be provided in the following ways:

- An e-Safety curriculum is provided as part of ICT, PSHE and other lessons and is regularly revisited
- Key e-Safety messages are reinforced as part of a planned programme of assemblies
- Pupils are taught to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information
- Pupils are helped to understand the need for the Pupil AUP agreement and encouraged to adopt safe and responsible use both within and outside school
- Pupils are helped to understand the benefits and risks associated with social media, online posting and messaging
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics that would normally result in internet searches being blocked. In such a situation, staff can request IT Support to remove those sites from the filtered list for those pupils. Any request to do so should be audited by the IT Manager, and clear reasons for the need must be established and recorded.

Education – Parents

5.2.1 Parents play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviour.

5.2.2 The School provides information and awareness to parents through seminars and other methods as appropriate.

Education & Training – Staff

It is essential that all staff who are granted access to the school network receive e-Safety training and understand their responsibilities, as outlined in this policy. Training will be arranged and overseen by the IT Manager, and recorded as having taken place, as follows:

- e-Safety training is made available to staff. This is regularly reinforced. The ICT Committee ensures that an audit of the e-Safety training needs of all staff with access to the network is carried out regularly.
- All new staff receive e-Safety training as part of their induction programme, ensuring that they fully understand the school e-Safety policy and Acceptable Use Policy. This training is overseen and recorded by the IT Manager.
- The e-Safety Officers will receive regular updates through attendance at external training events and/or by reviewing guidance documents released by relevant organisations.

Training – Governors

5.4.1 The e-Safety Governor takes part in e-Safety training / awareness sessions as necessary.

Technical – Infrastructure, Equipment, Filtering and Monitoring

5.5.1 School technical systems will be managed in ways that ensure that the school meets recommended technical requirements as laid out in the Internet Security Information document

5.5.2 The IT Manager continually reviews and audits the safety and security of school technical systems, and this audit is supplemented by an external audit and review every annually.

5.5.3 Servers, wireless systems and cabling must be securely located and physical access restricted.

5.5.4 All users are provided with a username and secure password by IT Support. Users are responsible for the security of their username and password.

5.5.5 Internet access is filtered for all users. The firewalls check for an updated filter list daily. If a URL is not on the filter list, the firewall checks the manufacturer's database directly. This database is updated constantly.

5.5.6 The school provides user-level filtering, allowing different filtering levels for different ages and different groups of users – staff, SPS pupils, and SPJ pupils.

5.5.7 All pupil web access is logged. Staff web access to restricted categories is also logged. Users are made aware of this in the AUP agreement. If a site is blocked by the filter as being inappropriate then access is not allowed. A report on such attempts is sent nightly to the IT Manager and Network Manager. These are viewed daily. Given the number of false positives in this logging, the threshold for action is

determined by the IT Manager or his deputy. Any causes for concern are passed on to the e-Safety officers. Logs are kept for three years.

5.5.8 A system is in place for users to report any actual or potential technical incident or security breach, pupils to the Director of ICT (SPS) or Director of Computing (SPJ); staff to the IT Manager.

5.5.9 Security measures are in place (Appendix: Internet Security Information) to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. The school infrastructure and individual workstations are protected by up to date anti-virus and anti-malware software.

Bring Your Own Device (BYOD)

5.6.1 Users who connect their own devices to the school's network are bound by the school's policies.

5.6.2 The school adheres to the principles and complies with the requirements of the Data Protection Act.

5.6.3 All users are provided with and accept the relevant AUP agreement.

5.6.4 All school network systems are secure and the wireless network is configured to require a pre shared key (PPSK). The key is emailed to the users school email address so that users can be identified and different policies by category can be applied, as on the cabled network.

5.6.5 Devices connected to the school's network are covered by the school's normal filtering systems.

5.6.6 Users accessing the School's wireless networks are authenticated using a pre shared key. Connection of a user's device to the School's network is recorded.

5.6.7 Pupils receive guidance on the appropriate use of personal devices.

Use of Digital and Video Images

5.7.1 See section 22 of the Codes of Conduct (SPS and SPJ).

5.7.2 When using digital images, staff should inform and educate pupils about the implications of the taking, use, sharing, publication and distribution of images. In particular, they should recognise the implications of publishing their own images on the internet e.g. on social networking sites.

5.7.3 In accordance with guidance from the Information Commissioner's Office, parents are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act, although this will be reviewed as part of the preparations for the introduction of the General Data Protection Regulations in 2018).

5.7.4 Staff are allowed to take digital / video images to support educational aims, but must follow school policy concerning 'Photography, Videos and other Creative Arts' in the Codes of Conduct.

5.7.5 Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

5.7.6 Pupils must not take, use, share, publish or distribute images of others without their agreement.

5.7.7 Pupils' full names may only be used on the intranet or website with parents' permission (or the pupil's if over 16).

5.7.8 Parents are requested to give their permission for the use of Pupils' photographs on the School's Intranet, Website or Social Media as part of their Registration for the School. Where permission is not granted, the School Office will inform all staff.

Data Protection

The school has a Data Protection Policy which includes electronic data, which has been revised to comply with the General Data Protection Regulations (GDPR) and Data Protection Act (DPA, 2018).

5.8.1 The School must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. This is in relation to data belonging to all members of the school community. As such, no member of staff is permitted to remove special category personal data from School premises, whether in paper or electronic form and wherever stored, without prior consent of the High Master, Head or Compliance Manager. Where a member of staff is permitted to download data off site it will need to be password protected.

5.8.2 There are two exceptions where prior approval is not required:

- iSAMS, the school's data management system, may be used on personal devices provided that the device used is secure and password protected.
- For pupils on residential trips, medical information and other relevant information (e.g. passport details) may be taken off site by the trip leader.

Communications

5.9.1 A wide range of rapidly developing communications technologies has the potential to enhance learning. The following describes how the school considers the benefit of using these technologies for education outweighs their risks / disadvantages.

5.9.2 These communication technologies are allowed for all adults, and pupils in both SPJ and SPS:

- Mobile phones may be brought to school (in SPJ they must remain switched off until after 4 p.m. unless permission has been given by a member of staff to make a call or send a text).
- Use of personal email addresses in school, or on the school network.
- Use of school email for personal emails.
- Use of messaging apps.

5.9.4 These communication technologies are allowed for all adults and for pupils in SPS only:

- Use of mobile phones in lessons.
- Use of mobile phones in social time.
- Taking photos on mobile phones / tablets/ cameras (may be used with explicit permission in SPJ).

- Use of other mobile devices e.g. tablets, gaming devices (may be used as e-readers only in lessons and library periods with explicit permission in SPJ).
- Use of social media.

5.9.5 Staff may not 'friend' current pupils at St Paul's Juniors.

5.9.6 When using communication technologies the school considers the following as good practice: '*The school email service may be regarded as safe and secure. Users should be aware that email leaving or entering the school is scanned for viruses, spam and bad language.*'

5.9.7 In accordance with the AUP agreement, users must immediately report the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Pupils report to an adult – usually their Form Tutor (SPJ), tutor or Undermaster (SPS). Staff report to a senior member of staff.

5.9.8 Any digital communication between staff and pupils or parents must be appropriate.

5.9.9 Pupils are provided with individual school email addresses for educational and administrative use.

5.9.10 Pupils are taught about e-Safety issues, such as the risks attached to the sharing of personal details. They are reminded of the need to communicate appropriately when using digital technologies.

5.9.11 On the school website, only school email addresses should be published.

5.9.12 Staff should use school email for school business.

5.9.13 Regarding the use of mobile numbers:
- SPS: The sharing and storage of pupil phone numbers on personal phones is justified where the context makes it professionally appropriate – for example, between tutors and tutees, or for those on school trips – and must be done openly and transparently.
- SPJ: staff must not have pupil numbers on personal phones.

Social Media

5.10.1 The school encourages and supports staff in their use of digital technologies, sites and apps in the course of their work (teaching, extracurricular, pastoral) with pupils but requires that any such use is informed and fully consistent with our standards and policies. All staff must read and make sure they understand §23 of the Codes of Conduct before engaging in any such activity.

5.10.2 For pupils in St Paul's Juniors:
- there should be no 'friending' between staff and pupils on social media.
- on social sites and apps, closed groups should be used where possible.
- staff should seek the permission of the e-Safety Officer before using social sites or apps.

5.10.3 For pupils is St Paul's School:
- staff should seek the permission of the e-Safety Officer before using social sites or apps.
- on social sites where direct messaging is available, there should be two staff admins.

Unsuitable / Inappropriate Images

The School believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. Whilst this list is not exhaustive, the school policy restricts usage as follows:

User Actions		Acceptable for adults	Acceptable for SPJ pupils	Acceptable for SPS pupils	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child sexual abuse images – The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**				X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.				X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008				X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) – contrary to the Public Order Act 1986				X
	Statements or images that are intended to radicalise people or in any other way endorse, condone or incite extremist or terrorist activity	No	No	No	
	Pornography & adult material	No	No	No	
	Promotion of any kind of discrimination	No	No	No	
	Threatening behaviour, including promotion of physical violence or mental harm	No	No	No	
	Any other information which breaches the integrity of the ethos of the school or brings the school into disrepute	No	No	No	
Using school systems to run a private business (*SPS boys may do this with permission of the Director of ICT)		No	No	No*	
Using systems, applications, websites or other mechanisms that bypass deliberately the filtering or other safeguards employed by the school		No	No	No	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)		No	No	No	
Creating or propagating computer viruses or other harmful files		No	No	No	
On-line gaming (educational)		Yes	Yes	Yes	
On-line gaming (non educational, unless blocked by the system)		Yes	Y es	Yes	
On-line gambling		No	No	No	
On-line shopping / commerce		Yes	No	Yes	
File sharing (peer-to-peer)		No	No	No	
Use of social media		Yes	No	Yes	

Use of messaging apps	Yes	No	Yes	
Creating and uploading of video broadcasts	Yes	No	Yes	

Responding to Incidents of Misuse: reports of misuse of IT equipment and services may originate from these sources and by these means:

5.12.1 The IT Support Centre:

- From daily filter log reports.
- Through routine examination of firewall and other service logs.
- By alerts raised from desktop monitoring software.
- From materials discovered during routine or other maintenance of School-owned IT equipment – including servers, desktop and laptop computers and mobile devices.
- As a result of observations of unusual patterns of network and storage use.

5.12.2 Through complaints concerning IT related activity made to the School from:

- Pupils
- Parents
- Staff
- Others outside the community

5.12.3 Line managers (in the case of staff) – or tutors (in the case of pupils):

- Suspicions of IT misuse by staff or pupils.
- Evidence handed to managers or tutors by other parties.

5.12.4 Individuals

- Staff members or pupils who wish to confess to some wrong-doing.

5.12.5 However the incident is reported or discovered there are two broad courses of action that can be taken - depending entirely on whether there is any suspicion of illegality involved or not.

Illegal Incidents

5.13.1 Anyone suspecting that:

- accesses have been attempted to any website containing child abuse images
- accesses have been attempted to any website containing material that breaches the Obscene Publications Act
- accesses have been attempted to any website containing criminally racist material
- accesses have been attempted to any website which contains statements or images that are intended to radicalise people or in any other way endorse, condone or incite extremist or terrorist activity
- any such materials are themselves to be found on any electronic device - whether owned by the School or not
- there has been any incident by electronic means of 'grooming' behaviour

must report all allegations, complaints, concerns or suspicions directly to the High Master or Head (as appropriate), or, in his absence, to the Chairman of Governors, unless that person is the subject of the concern; those about the High Master should be reported to the Chairman of Governors (or in his absence, the Vice Chairman). All allegations, complaints, concerns or suspicions about the Chairman of Governors should be reported to the LADO without the Chairman of Governors being informed. The LADO may choose to appoint a 'case manager'.

5.13.2 Action from this point will be dictated by the Safeguarding and Child Protection Procedures - Appendix 2 **Procedure to be followed in the event of an allegation against a member of staff or volunteer of abuse** - including the involvement of the DSL, LADO, Police, Charity Commission, DBS, NCTL or other external agencies, as appropriate.

5.13.3 Concerns, suspicions or allegations of other IT related illegal activity (such as fraud, copyright theft or unlicensed use of software) by a member of staff should also be reported according to the reporting hierarchy outlined above. Such concerns will be managed in accordance with the School's whistleblowing code.

5.13.4 Concerns that relate to the illegal behaviour or actions of pupils or parents (and not staff) should be reported to the DSL or on his absence, the Deputy DSL. The DSL (or Deputy) will follow the Safeguarding and Child Protection Policy and Procedures in reporting any such behaviour to Children's Social Care and/or the Police.

5.13.5 Suspicions of other IT related illegal activity (such as fraud, copyright theft or unlicensed use of software) should be reported directly to the Surmaster (SPS) or Deputy Head (SPJ) for pupils, and the High Master or Head for members of staff.

Safeguarding Incidents

5.14.1 Substantive safeguarding concerns should be reported to High Master or Head (if concerns relate to activity of a member of staff) or to the DSL (if about pupils) as per the Safeguarding and Child Protection Policy and Procedures.

Other Incidents

5.15.1 Reports of misuse of IT equipment and services originating from:

- pupils, parents or staff
- line managers or tutors
- individuals

which do not raise safeguarding concerns, or appear to suggest any other kind of illegal activity, should be made directly to the appropriate Line Manager (usually the Head of Department) who will take action as appropriate, consulting the IT Support Centre and/or e-Safety Officer as necessary to establish, capture and preserve any relevant data or other evidence.

5.15.2 Misuse of IT equipment and services by pupils or visitors should be referred first to an e-Safety Officer who may refer to a senior member of staff as appropriate.

5.15.3 Misuse detected by the IT Support Centre will first be investigated by the IT Manager or Network Manager and evidence gathered. This evidence will then be forwarded to a senior member of staff.

E-Safety Officer Responsibilities

5.16.1 In the case of a reported incident the e-Safety Officers will take the following actions:

- Evaluate the reports to determine appropriate response.
- If required, to ask the IT Support Centre to investigate further and to provide more evidence.
- To initiate a response to the incident according to normal disciplinary procedures for both staff and pupils.
- To log the incident in the e-Safety Incident Log.
- Following the conclusion of any incident the e-Safety Officers will log the incident in the e-Safety Incident Log; review the incident to determine if any modification to policy or practice is required; and brief the e-Safety Committee on all incidents at its next meeting.

IT Support Centre Investigations

5.17.1 Where directed by the High Master, Head, Chair of Governors or Vice Chair of Governors, DSL or Deputy DSL, or by an external agency such as the Police, the IT Support Centre will undertake further investigative actions. These may include:

- Detailed examination of firewall, filter, mail relay and other security logs - and the extraction therefrom of references to activity associated with the incident in questions
- Examination of materials stored on the School's storage networks - taking copies of any items associated with the incident in question.
- Remote examination of School desktop and laptop computers - and the gathering of relevant evidence therefrom, including the copying of materials or the taking of screen-captures as required.
- Examination of the contents of School email mailboxes, including sent and deleted items - and the extraction of messages and materials relevant to the incident in question.
- The requiring of staff to return School-owned mobile devices to the IT Support Centre for investigation.

5.17.2 These investigations will be carried out by the IT Manager and Network Manager using machines in the IT Support Centre.

5.17.3 Unsuitable materials will be copied and may then – under the direction of an appropriate authority - be deleted from storage, mailboxes or computers.

5.17.4 At the culmination of the investigation a report on all materials and references found - detailing the processes followed - will be passed on to the e-Safety Officers; names will be redacted as appropriate from all such reports in accordance with confidentiality requirements.

5.17.5 Should any of these investigations uncover materials or accesses for which there is any suspicion of illegality the IT Support Centre staff will immediately suspend any further inspection, reporting the matter in accordance with the procedure above (illegal incidents) or to the Police (if already involved) and awaiting direction from them. IT Support Centre staff will also assist with the recovery of School-owned

equipment such as desktop and laptop computers and mobile devices as required by the relevant authorities.

5.17.6 The IT Support Centre will only examine the contents of devices not owned by the School with the prior agreement of the pupil and/or his parents.

Appendices

1. SPJ pupils' AUP agreement
2. SPS pupils' AUP agreement
3. Staff AUP agreement
4. Visitors' AUP agreement
5. Internet Security Information
6. Protocols for monitoring and reporting
7. Information sent to parents
   a. SPJ photograph and images letter
   b. SPS photographic permission

ICT Acceptable Use Policy for Pupils

Applicable: St Paul's Juniors

This agreement is intended to encourage imaginative, responsible and safe use of digital technologies. By acting with care and thought pupils should be putting into practice much of this policy.

The School provides both networked, desktop computers and wireless access to the internet through its own filtered connection. Wireless access is available everywhere in the school for pupils to use if given permission to do so.

Personal safety and responsibility

- I understand that the School will log and monitor my use of computers, devices and my digital communications;
- I will keep my school username and password safe and secure. I will not share it, nor will I try to use another pupil's or staff member's username and password. I understand that I should not write down or store passwords where it is possible that someone may steal them;
- I will not leave any school device, or device connected to the school network, logged on for others to use;
- I will not give out personal information about myself or others that could be used to identify me, my family or my friends (e.g. addresses, email addresses, phone numbers, information about the school or my age or the age of another pupil) unless a trusted adult has given me permission;
- I will never arrange to meet someone I have only ever previously met online unless I take a trusted adult with me;
- I will only use school computers and devices as directed. I will not use school devices for on-line gaming, on-line gambling or internet shopping and I will not visit sites I know to be unsuitable;?
- I understand that some websites and social networks have age restrictions and I will respect this;
- I understand that once something is posted online or written in an email it has a permanence that is not like something that is said. It can be repeated, is searchable and can be copied out of context. I understand that I have to take responsibility for my actions online and I should consider my reputation, the reputation of others and the reputation of the School.
- If I see anything unpleasant or inappropriate or I receive a message I do not like, I will not respond but I will save it and talk to a trusted adult as soon as possible;
- I will be polite and responsible when I communicate with others. I will not use strong, aggressive or inappropriate language. I will not send messages either anonymously or pretending to be someone else and I will not send group messages needlessly;
- I will not take or distribute images of anyone without their permission;
- I will edit or delete my own files only and not view, or change other people's files without their permission.

Device security

- I will only use my personal devices (mobile phone, USB device, laptop , iPad etc.) in school only if I have been authorized by a member of staff and explicit permission has been granted to bring in the device to facilitate teaching and learning. I understand that if I do use my own devices in school I will follow the rules set out in this agreement, in the same way as if I were using school equipment;
- I will not try to upload, download or access any materials which are illegal, or encourage illegal, extremist or terrorist activity, or which may cause harm or upset to others, nor will I try to use any programs or software that might allow me to bypass the filtering systems in place to prevent access to such materials;
- I will report immediately any damage or faults involving school equipment or software, however this may have happened;
- I will report any actual or potential technical incident or security breach to the Director of Computing;? Member of staff
- I will not open a hyperlink in any email or attachment to an email if I have any concerns about it or think it may contain a virus or other harmful program;
- I will not install, attempt to install or store programs or software on any school device, nor will I try to alter the computer settings.

Sanctions

- I understand that if I fail to comply with this Acceptable Use Policy Agreement I will be subject to disciplinary action. This would include involvement in incidents of cyber-bullying or any inappropriate behaviour that is covered in this agreement, when I am in or out of the School and where it involves my membership of the school community.

I agree to comply with the rules and regulations set out in the St Paul's Juniors ICT Acceptable Use Policy Agreement.

ICT Acceptable Use Policy for Pupils

Applicable: St Paul's School

This agreement is intended to encourage imaginative, responsible and safe use of digital technologies. By acting with care and thought pupils should be putting into practice much of this policy.

The school provides both networked, desktop computers and wireless access to the internet through the school's own filtered connection. Wireless access is available for use via your own devices.

It is standard practice in organisations to audit users' internet activity and all staff and pupils are audited in this way. Audit trails are examined when necessary. Should you find yourself looking at or opening material you consider the school would think inappropriate (or material you find disturbing), simply inform a member of staff so we can work with you to address the matter.

- I understand that the school will log and monitor my use of computers, devices and my digital communications

Identity and responsibility (online and digital)

This section applies to all your use of digital technologies, whether school-owned or personal.

In the digital realm, once something is posted online it has a persistence that is not like something that is said. It is also replicable and searchable (directly and through its metadata), and you cannot be sure who your audience is or will be. Once something is posted online, its effects are often magnified and can be mirrored out of context. All of this requires experience to understand. Remember: when you post, you have not only your own reputation to consider but also that of others and that of the school. Every member of the community has to take responsibility for his or her actions online. If you are in doubt, it is best not to post, send an email, etc.

- I will respect and maintain the integrity of my own and others' digital identities
  - I will log on only as myself
  - I will keep my login details private and make them secure
  - I will not leave any device logged in and accessible to others
  - I will exercise informed judgement about disclosing my personal details and will not give out another person's details without their clear consent
  - I will be polite and responsible when I communicate with others.
- I will not make, post or send images and video footage of others except with the agreement and understanding of those involved. Agreement must extend to the finished, edited product
- I understand that financial transactions are permitted provided that I act within the constraints of the school's rules and with my parents' approval.
- I understand that the school's computers and systems are not to be used to upload, download or access any materials which are illegal, or which endorse, condone, or incite illegal, extremist or terrorist activity or which are in any other way inappropriate for school, or likely to cause harm or distress to others, or bring the

school's name into disrepute. I understand that I may not use any program or software to access such materials by bypassing the school's filters.

Network and hardware integrity

I will respect and maintain the network and the computers the school provides:

- I will not open unexpected or suspicious files.
- I understand the need to exercise judgement when connecting a device to the school's network or to a computer. Those with non-executable files on them are clearly fine, but those with executables (e.g. a browser designed to run safely from a USB stick) can be harder to assess. I will not store or seek to install any executable file on the school network.
- I will not link devices that are themselves computers (in whatever form) to the wired network without first consulting either the Director of ICT or the IT Manager.
- I understand the need to exercise judgement when downloading files and am aware that viruses can be hidden in documents and images (for example) and not just in executable files. I will always seek advice if in doubt.
- I will respect the network's integrity when sending messages. I will not spam people or send needless messages. I will not attempt to send messages anonymously or pseudonymously for malicious purposes.
- I will report any actual or potential technical incident or security breach to the Director of ICT.
- I understand that if I fail to observe this agreement I will be subject to disciplinary action.

I agree to comply with the rules and regulations set out in the St Paul's School ICT Acceptable Use Policy Agreement for pupils.

ICT Acceptable Use Policy for Staff

Applicable: St Paul's School and St Paul's Juniors

This agreement is intended to encourage imaginative, responsible and safe use of digital technologies. By acting with care and thought you should be putting into practice much of this policy.

In the digital realm, once something is posted online it has a persistence that is not like something that is said. It is also replicable and searchable (directly and through its metadata), and you cannot be sure who your audience is or will be. Once something is posted online, its effects are often magnified and can be mirrored out of context. All of this requires experience to understand. Remember: when you post, you have not only your own reputation to consider but also that of others and that of the school. Every member of the community has to take responsibility for his or her actions online. If you are in doubt, it is best not to post, send an email, etc.

This Acceptable Use Policy is intended to ensure:

- that staff will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use when in school, when using school systems and equipment and when connected to the school network
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- that staff are protected from potential risk in their use of ICT in their everyday work

Access to ICT is made available to staff to enhance their work and to enhance opportunities for pupils' learning, and the school expects staff to be responsible users.

Acceptable Use Policy Agreement

- I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.
- I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT.? Support Staff
- In any interactions with pupils I will ensure appropriate use of ICT.
- I confirm that I have read and understood the St Paul's School e-Safety Policy.? Not all staff have access to the e-Safety policy before their employment. Should say I have read or will read at the earliest opportunity

For my professional and personal safety:

- I understand the school will monitor my use of its ICT systems and networks.
- I understand that the rules set out in this agreement also apply to use of school ICT systems out of school, and to the transfer of personal data out of school.

- I understand that the security of my account is my responsibility and that I should
  - Logon only as myself;
  - Keep my login details private and make them secure;? How to make secure
  - Not leave any device logged in and accessible to others.
- I will report any actual or potential technical incident or security breach to the IT Manager.? Any eSafety breach
- I will immediately report any illegal, inappropriate or harmful material I become aware of when in school or connected to the school network:
  - Material that appears to originate from sources external to the School should be reported to IT Support;
  - Material that appears to have been sent or circulated by a pupil or parent should be reported to the Designated Safeguarding Lead (DSL) (or in his absence the deputy DSL);? eSaftey officer
  - Material that appears to have been sent or circulated by a member of staff (including a temporary member of staff or volunteer) should be reported to the High Master or Head.

I will be professional in my communications and actions when using school ICT systems at school, when using school ICT systems and equipment or when connected to the school network:

- I will ensure that when I take and / or publish images of others I will do so in accordance with the school's policy on the use of digital / video images.
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- Any use that I make of chat and social networking sites will be in accordance with the guidance given in the SPS and SPJ Codes of Conduct.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- I understand that the school ICT systems are primarily intended for educational use.

The school has the responsibility to provide safe and secure access to ICT:

- I will not open any hyperlinks in emails, or any attachments to emails, unless the source is known and trusted.
- I will not try to upload, download, or access any materials which are illegal (for example child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or which endorse, condone, or incite illegal, extremist or terrorist activity or which are in any other way inappropriate for school, or may cause harm or distress to others. I will not try to use any programs or software to bypass the school's filtering and security systems in order to access such materials.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school's Data Protection Policy.? Greg
- I understand that data protection requires that any staff or pupil data to which I have access must be kept private and confidential.? Greg
- I will immediately report any damage, loss or faults involving school equipment or software to IT Support.

When using the internet in my professional capacity or for school-sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this AUP Agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises
- I am aware that emails may be disclosed as evidence in court and that, even if deleted, copies may exist on a back-up system
- I understand that if I fail to comply with this AUP Agreement, I could be subject to disciplinary action.

I agree to comply with the rules and regulations set out in the St Paul's School & St Paul's Juniors ICT Acceptable Use Policy Agreement for staff.

ICT Acceptable Use Policy for Visitors

Applicable: St Paul's School and St Paul's Juniors

I understand that I must use the school's systems and devices, including its wireless network, in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users.

- I understand that my use of the school's systems and devices and digital communications will be monitored.
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- Whilst in the school, I will not try to upload, download or access any materials which are illegal (for example child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or which endorse, condone, or incite illegal, extremist or terrorist activity or which are in any other way inappropriate for school, or may cause harm or distress to others. I will not try to use any programs or software to bypass the school's filtering and security systems in order to access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the IT Manager or his deputy.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I will not access, copy, remove, add to or otherwise alter any other user's files, without permission.
- I will not install or attempt to install programs of any type on a school device, nor will I try to alter school computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened, to the IT Manager or his deputy.

I understand that if I fail to comply with this agreement the school has the right to remove my access to school systems and devices.

I agree to comply with the rules and regulations set out in the St Paul's School & St Paul's Juniors ICT Acceptable Use Policy Agreement for visitors.

Signed:

Name:

Date:

Appendix 6

Internet Security Information

Internet security is a branch of computer security specifically related to the Internet. The Internet represents an insecure channel for the exchange of information and for access to online services. By its nature it carries a high risk of intrusion or fraud, as well as the possibility of inadvertent or malicious abuse by those accessing it. The objective of the schools' security approach is to establish rules and measures to protect against attacks from the Internet and to prevent abuse from within the School, whilst at the same time balancing these risks against the requirement to ensure that members of the community have the widest possible access to internet resources in order to enhance teaching and learning, or for administrative use.

Aim. The aim of this appendix is to highlight the risks associated with internet usage at St Paul's School and St Paul's Juniors and identify the methods used to mitigate these risks. As will be seen from the technical details below, the security tools in use at the School are extremely flexible.

Policy Control. Security policy is ultimately determined by the Governors and the SMT for each part of the School. The e-Safety Committee, which includes the three e-Safety Officers, has responsibility for oversight of Internet Security policy. The IT Manager and his staff are responsible for implementation and monitoring of the policy, and for reporting breaches thereof.

Incident Reporting. Substantive safeguarding concerns should be reported to the High Master or Head (if concerns relate to activity of a member of staff) or to the DSL (if about pupils) as per the Safeguarding and Child Protection Policy and Procedures. Concerns which are not of a safeguarding nature should be reported in the first instance to the appropriate line manager (staff) or Undermaster (SPS pupils), or Deputy Head (SPJ pupils).

The following risks and mitigations have been identified:

Risks related to Internet Use	Details	e-Safety implications	Mitigation
Access			
Unauthorised access - by those within and outside the School	Use of School systems without permission	yes	The School's network and systems can only be accessed by use of a network account - identified by a username and password. Network account details are only handed over in person after an induction.
Security of network accounts	Insecure passwords - sharing of accounts - revealing account details - attempting to use another's account	yes	Strong passwords arenforced and staff and pupil inductions reinforce the importance of network account security - and the users' responsibilities therefore. Forgotten passwords will only be reset by a visit to the ITSC in person or by substantial proof of identity
Accountability - monitoring	Attempts to avoid account monitoring		Role based or shared network accounts are deprecated unless tied to an accountable individual. All logons are recorded in multiple event logs and databases
Accountability - AUPs	Non-compliance with School policies	yes	The School's Acceptable Use Policies are signed electronically annually
Attacks on infrastructure			
Viral attacks	Viruses, worms, trojans		The School runs an application layer firewall by Palo Alto Networks. The firewall provides antivirus, threat protection and URL filtering services. All of the School's servers and desktop systems run additional endpoint antivirus software
Malware	Malware, spyware, adware, ransomware		Covered by the Palo Alto threat protection and Wildfire service
Denial of service attacks	Attempts to interfere with legitimate traffic by flooding the network		The Palo Alto firewalls prevent all currently known DoS attacks. The configuration of the School's networks and of the security rules on the firewalls further mitigates this and other attacks
Exploitation of software vulnerabilities	Exploitation of known vulnerabilities in operating systems and applications		Covered by the Palo Alto threat protection service. Inside the School systems are protected by group policies such that users cannot access system components

Attempts to access infrastructure equipment and services	Attempts to log on to or otherwise interfere with infrastructure equipment such as firewalls, switches and routers		The School's network is configured such that management access to infrastructure items is only possible by IT staff
Installation or use of unauthorised software on School systems			School systems are locked against the installation or re-configuration of software by users. The desktop machines available to boys are protected further by the Impero software suite that monitors usage by recording and tracking users' Internet and networked computer activity
Connection of poorly configured personal devices	Connection of devices not owned by the School that may be infected with virus or worms, or have badly configured network connections		Personal devices may not be connected to the wired network without permission of the ITSC. The wireless network is configured as a 'sandbox'. All other School systems are protected from it
Hacking, cyber espionage from outside the School			Covered by the Palo Alto threat protection service
Use of hacking tools within the School	Keyloggers, password crackers, promiscuous packet capture		The Impero software protects publicly accessible machines
Antisocial Use			
Bandwidth hogging	Use of applications the consume unreasonable amounts of bandwidth		The Palo Alto firewalls are configured to prevent the use of heavy bandwidth applications such as peer to peer files sharing. Network bandwidth use is constantly monitored to identify abuses
Running unauthorised services	Connection of a device to the School network that advertises unauthorised websites or other services		The firewalls are configured in such a way that only authorised sites and services can be publicised from the School's network to the Internet. A variety of network scanning tools are used to identify other rogue services
Storage			
Security of user files and resources held on School systems	Attempts to access to user's files and resources without permission	yes	Access to the School's storage networks is tightly controlled by permissioning based on the users' network accounts. This gives direct accountability and security

Integrity of user files and resources	Attempts to alter or delete others users' files and resources		File security makes it most unlikely that a user could maliciously damage another user's files, but in the event of such happening the ITSC can restore from routine backups. The backup regimen covers all School storage systems on a nightly basis and there are additional mechanisms to allow users to recover their own files should they become lost or damaged
Security of system and administrative resources	Attempts to access the system or School administration resources without permission		Access to the School's storage networks is tightly controlled by permissioning based on the users' network accounts. This gives direct accountability and security
Integrity of system and administrative resources	Attempts to alter or delete system or School administration files and resources		In addition to the mechanisms defined above all School databases are backed up to multiple locations to provide increased resilience
Unacceptable or inappropriate storage of personal data	Use of the School's storage networks in an unauthorised or insecure manner for personal data		ITSC staff have access to all file systems and monitor broad patterns of use constantly. Suspicious traffic patterns are investigated in depth
Access to copyright materials	Making accessible materials in breach of copyright - eg - outside the School		The School's streaming media servers are configured to prevent access to materials thereon that might breach copyright. The staff AUP states that work protected by copyright will not be downloaded or distributed for any school work, and use of any original work by others requires their permission. Pupils receive instruction in the use of copyright and otherwise licensed material.
Introduction of inappropriate or illegal materials onto School systems ● Across the network ● From other public networks ● From personal devices ● From removable media	The copying or downloading of inappropriate or illegal materials onto School computers or network storage solutions		The Palo Alto URL filters are configured to prevent access to and the downloading from Internet sites that have been categorised by the filter manufacturer. Attempts to access blocked sites are recorded and daily reports sent to the IT Manager and his deputy.
Email			

Unacceptable/inappropriate use of email	Unprofessional conduct - use of unacceptable language - inappropriate email targeting - use of School systems for commercial purposes	yes	The ITSC operates a pair of mail relays equipped with Mailmarshal filtering software. This software is used to prevent use of offensive language in emails
Antisocial use of email	Sending of inappropriate or unauthorised bulk emails		Pupils' mailboxes are configured such that they cannot send emails to more than 15 recipients. All mailboxes are limited as to the size of message that can be sent
Email attacks	Spam, mail-bombing and phishing attacks, use of botnets		The Mailmarshal software includes antivirus and antispam filters and can protect against a wide variety of mail based attacks
Relaying - anonymous and otherwise	The use of School email system to forward messages to other external mail systems	yes	The mail relays are configured to prevent the relaying of emails by any system on the School's network other than authorised mail servers
Bullying		yes	The Mailmarshal software maintains a log of messages sent and received that can be used for diagnostic and forensic purposes. Impero software is used to flag up immediately to the IT Manager any situation where a school computer is used to type or display any word on a specified trigger words list, which includes words associated with bullying and trolling.
Accidental exposure of data	Careless use of email resulting in data being send to the wrong recipient		Internal emails can be recalled by the user, and they can be deleted from mailboxes en masse by IT. Staff induction includes advice on the careful use of email
World Wide Web			
Access to unsuitable materials	Accessing materials and websites that are inappropriate in a school environment	yes	The Palo Alto URL filters are configured to prevent access to and the downloading from Internet sites that have been categorised by the filter manufacturer. Attempts to access blocked sites are recorded and daily reports sent to the IT Manager and his deputy. Substantive safeguarding concerns would be reported to the High Master or Head (if concerns relate to activity of a member of staff) or to the

			DSL (if about pupils) as per the Safeguarding and Child Protection Policy and Procedures. Concerns which are not of a safeguarding nature would be reported in the first instance to the appropriate line manager (staff) or Undermaster (SPS pupils) or Deputy Head (SPJ pupils).
Access to terrorist or extremist propaganda	Accessing or generating statements or images which endorse, condone, or incite illegal, extremist or terrorist activity	yes	As above, plus Impero software is used to flag up immediately to the IT Manager any situation where a school computer is used to type or display any word on a specified trigger words list, which includes words associated with extremism or radicalisation.
Access to illegal materials and services	Accessing child abuse materials - race or hate crime materials - materials that breach the Obscene Publications Act - fraudulent or copyright materials - unlicensed software or services	yes	See above; in addition Netclean software is used to detect, track and block illicit material
Access to unwanted materials	Inadvertent viewing of unsuitable materials	yes	The Palo Alto URL filters are configured to prompt staff before allowing access to a range of subject categories that - whilst not deemed unsuitable - are considered to require caution
Gaming and gambling		yes	See above
Excessive use of the Internet		yes	This is a pastoral issue
Running unauthorised websites	The publicising within or outside the School of websites purporting to have official backing without permission	yes	The firewalls are configured in such a way that only authorised sites and services can be publicised from the School's network to the Internet. If unacceptable sites outside the School are reported the Directors of ICT deal with those responsible
Social Networking			
Inappropriate or unsafe use of social media	Inappropriate communications between adults and children - exposure to grooming - awareness of audience - control	yes	The School's policies and guidance on the safe use of social media are foregrounded in safeguarding training. Pupils are given extensive guidance through the ICT curriculum regarding the safe use of social media. Impero software is used to flag up immediately to the IT

	of permissions - sensitivity regarding personal data - regard for reputation (school and personal)		Manager any situation where a school computer is used to type or display any word on a specified trigger words list, which includes words associated with grooming, bullying, trolling and radicalisation
Antisocial use of social media	Trolling, abusive messaging	yes	See above. The School's anti-bullying policy also applies
Inadequate privacy settings	Allowing public access to personal information through inadequate knowledge of security settings	yes	See above
Bullying		yes	See above. The School's anti-bullying policy also applies
Exposure to social network based attacks	Social engineering, fake offers, manual sharing scams, 'like' jacking, fake plugins, fake apps	yes	See above
Intranets and external websites			
Publishing of unsuitable materials	The publishing on School websites and intranets of unsuitable, inflammatory or otherwise unauthorised materials		The School's content management solution - Firefly - logs the creators and editors of content, who are identifiable through their network accounts. The webmasters for these sites have control over permissioning
Bringing the School into disrepute	The publishing on websites or social media outside the School of materials or comments that damage the reputation of the School		
Personal and Mobile Devices			
Dangerous or careless use of resources personal or mobile devices	Use of personal or mobile devices in a manner that could cause a breach of the School's AUPs - inadvertent access to personal data or resources through lack of understanding	yes	For School owned devices, safeguarding training is given as part of the device induction. A Conditions for Loan form must be signed by the recipient of the device which covers safeguarding requirements

Theft or loss of personal devices	Loss of School owned devices - loss of personal data contained thereon	yes	School devices are covered by a signed agreement as to the user's responsibilities for the device
Digital Literacy			
Abuses resulting from ignorance	Breaches of School policies through lack of knowledge of IT systems	yes	Staff training and INSET aims to raise staff awareness of the Internet and its uses. The ICT curriculum does the same for pupils
Unsafe practices caused by lack of knowledge	Lack of understanding of how Internet services such as synchronisation of cloud storage and social networks operate can result in unsafe use of the Internet	yes	See above
Circumvention of the School's security mechanisms			
Anonymous proxies	Attempts to access websites and services otherwise prohibited from the School's network by bypassing the School's security systems	yes	Known anonymous proxies are blocked by the Palo Alto firewalls
Http tunnelling	Attempts to bypass security systems by tunnelling through secure connections	yes	We implement SSL decryption for pupils with one or two exceptions in selected categories, such as banking and shopping.
Masquerading	Attempting to use another person's identity on the Internet - eg - as email sending address	yes	Extensive logs are maintained on all of the School's platforms that can be used forensically to trace such wrongdoing
IT Service Issues			
Incorrectly or poorly configured systems	Security loopholes in School networks and systems as a result of poor design or configuration		The ITSC has a considerable range of experience in the design and maintenance of secure networks and systems. This is augmented by ongoing training and research. In addition, internal and external penetration tests

			are carried out on an annual basis. IT support also carry out weekly tests on systems and infrastructure.
Out of date software versions	Updates and security hotfixes not applied in a timely fashion		All School systems are updated at the earliest possible point - depending on the urgency of the hotfix. Central management solutions roll out most updates automatically - except in circumstance where so to do might compromise the service provision
Out of date threat databases	Antivirus, threat and URL filtering databases not being updates on a regular basis		Antivirus, threat protection and URL filtering databases are updated automatically on a nightly basis
Inadequate IT staffing	Insufficient or poorly trained IT staff resulting in poor systems design and maintenance		The ITSC is well staffed, well-resourced and has an appropriate annual training budget
Future Threats			
As yet unknown Internet threats			The ITSC is charged with ongoing research into new and evolving Internet and other security related issues

e-Safety Protocols for Monitoring and Reporting
St Paul's School and St Paul's Juniors

1. These monitoring and reporting protocols are to be read in conjunction with the St Paul's School and St Paul's Juniors e-Safety Policy.

Responsibility	Policy Reference	Requirement	Frequency	Dates	Remarks
ICT Committee	-Schedule for Development /Monitoring/ Review -e-Safety Group (ICT Committee) Roles and Responsibilities	Report on e-Safety for Executive Group	Termly	Summary of preceding term's e-Safety issues presented early each term to ICT Committee	- Standing item at each ICT Committee To include: -Summary of e-Safety incidents -e-Safety Staff Training report
Executive Group	-Schedule for Development /Monitoring/ Review	Review Report on e-Safety from the ICT Committee	Termly	Early each term after ICT Committee has approved the report	
ICT Committee	e-Safety Group (ICT Committee) Roles and Responsibilities	Report on e-Safety for Governing Body	Annually	Last Governors' Meeting of the Summer Term	
Governing Body (led by e-Safety Governor)	-Governors' Roles and Responsibilities -e-Safety Group (ICT Committee) Roles and Responsibilities	Review Report from e-Safety Committee	Annually	Last Governors' Meeting of the Summer Term	
Governing Body (led by e-Safety Governor)	-Governors' Roles and Responsibilities	Report to Governing Body	Annually	Last Governors' Meeting of the Summer Term	

Governing Body (led by e-Safety Governor)	Schedule for Development /Monitoring/ Review	Review e-Safety Policy	Annually	Last Governors' Meeting of the Summer Term	May be reviewed more regularly in the light of any significant new developments
e-Safety Governor/e-Safety Officers	- Governors' Roles and Responsibilities - e-Safety Officers' Roles and Responsibilities	Termly Meeting	Termly	Alongside H&S meeting	
e-Safety Officers	- e-Safety Officers' Roles and Responsibilities	Termly Meeting	Termly meeting	2nd week of each term	To include a review of e-Safety policy plus training and curriculum for staff and pupils
IT Manager/Deputy Manager	- IT Manager's Roles and Responsibilities	Check Filtering Log Reports	Daily	Includes holidays	- To check for unusual activity - Log automatically generated at 1am daily - Can be checked remotely
IT Manager/Deputy Manager	- IT Manager's Roles and Responsibilities	Monitor: - Traffic Flow Logs - Security Logs - Event Logs	Weekly	Includes holidays	- To check for unusual activity - Can be checked remotely
IT Manager/Deputy Manager	- IT Manager's Roles and Responsibilities	Monitor: - Website Access Logs - Back up Website Access Logs	As required / prompted by a specific incident	Includes holidays	- Provides information on who has accessed which websites. - Data can be held indefinitely
Teaching and Support Staff, Volunteers and Governors	- Teaching and Support Staff Roles and Responsibilities - Governors' Roles and	e-Safety Training	- On induction - whole school INSET repeated every	Rolling programme	- To be understood as part of safeguarding and child protection work

	Responsibilities - e-Safety Officers' Roles and Responsibilities - Education & Training – Staff/Volunteers		three years		
Pupils	- Pupils' roles and Responsibilities - e-Safety Officers' Roles and Responsibilities - Education - pupils	e-Safety Training	- On induction - Throughout the year	- When joining - In assemblies and PSCHE and (as needed) tutor meetings	4th form ICT course; PSCHE; assemblies
All school IT users (including pupils)	- IT Manager's Roles and Responsibilities - Teaching and Support Staff Roles and Responsibilities - Pupils' roles and Responsibilities	- Brief on and sign up to Acceptable Use Policy (AUP) - All users required to sign anew	- On induction - Yearly	First log in of the new Academic Year	- Signed electronically
Parents	- Parent AUP	Sign up to Parent Agreement on use of IT	On induction and annually thereafter	On registration	
Community User	- IT Manager's Roles and Responsibilities - Teaching and Support Staff Roles and Responsibilities	Community User AUP	Registration as required, up to a maximum of a week	On registration, from September 2014	- Username and password to be collected from IT Department. - Wi-Fi to be password protected (therefore identity of all Bring Your Own

					Devices will be known.
IT Manager	- IT Manager's Roles and Responsibilities	External audit of school technical systems	Every 3 years	2015	

ST PAUL'S SCHOOL
Juniors

Dear Parents,

I am writing to explain the School's policy regarding the use of the sharing, distribution and publication of images of pupils. I hope that you will feel able to endorse the same level of trust in this area that you afford to us in all other areas of our care for your child at St Paul's Juniors.

We like to use photographs or videos to celebrate the achievements of our boys and to allow pupils, staff and parents to enjoy memories of past events. We believe that by taking proper precautions any risk to individuals can be made very small and that using images of pupils should continue in line with the policy set out below.

Photographs, digital images or videos of boys may be taken either at the School or when pupils are involved in organized activities off site. We use some of the images in school publications, such as *The Grapevine* or *the annual school magazine*, on the intranet, or on the website or on School social media. From time to time professional photographers are invited into the School to take group photographs or pictures of significant events. These photographs are available for parents to purchase and can be accessed by password via the school's Parent Portal. CCTV is located around the School but is not installed in classrooms, changing rooms or toilet areas. All surveillance within the School is overseen by a data controller registered with the Information Commissioner's Office.

Parents and family members are welcome to take photographs or videos of school events which may include images of other pupils. To respect the privacy of others and in some cases for protection purposes, these images should not be made publicly available. Parents should not take photographs of their son or fellow pupils in the swimming pool or changing rooms. Copyright issues may prevent the School from permitting the filming or recording of some plays or concerts. A reminder will be printed in the programme of events where issues apply. Flash photography can disturb others in the audience or even cause distress for those with medical conditions; we therefore ask that it is not used at indoor events.

The School's Policy

We comply with the Data Protection Act and the requirements of the Information Commissioner's Office and we follow the advice given by the Department for Education which states: "If the pupil is named, avoid using the photograph. If the photograph is used, avoid naming the pupil". Where it is deemed necessary or desirable to deviate from the above policy (for example, in an article celebrating a particular boy's achievements) we will always seek specific parental consent before publication.

We would also seek parental consent before publishing any images in the newspaper or on television.

If you have any concerns regarding the information in this letter, please do not hesitate to get in touch. If I do not hear from you I will assume that you are happy for the School to use static or video images of your child, unidentified by his name, in school publications (e.g. newsletter, magazine, website, intranet, social media).

With best wishes,

Head

Parental Consent Form – Use of photographic images

Name of Parent or Guardian _____

Child's name _____

May we take static or video images of your child and use them, unidentified by his name, in school publications (prospectus, magazines, website, intranet etc)?

Please circle your answer: **Yes / No**

I understand that if it is deemed necessary or desirable to use the name of my son alongside his photograph, my permission will be sought before publication. The School will also seek my consent before any images of my son are published in newspapers or appear in other news media.

Declaration

I have read and understood the School's policy regarding the use of photographs of pupils. My decision on whether to give consent will remain valid throughout my child's time at St Paul's Juniors unless I notify the School to the contrary in writing. If I or members of my family take photographs or video recordings at a school event, I promise that these will be kept for family use only.

Signed: _____

Date: _____

Maxine Shaw
Head

ST PAUL'S SCHOOL
Est. 1509

Dear Parent or Guardian,

This letter accompanies a consent form (overleaf) covering the use of images and recordings that may be made of your son during his time at the School. When you have read it, please complete and return the form. We hope you will feel able to provide consent for the use of images and recordings in line with the policy below. Pupils over 16 years old are asked to complete the form themselves.

If we do not receive a signed consent from you, we will assume that we can make images and recordings of your child and use them, unidentified by his full name, in school-published media.

*****

St Paul's recognises that children growing up now have never known a world without the web and digital technology. During their time at St Paul's, all boys will participate in digital projects which will help them to develop important skills and to learn to manage their own online identities. In addition, the School uses media of all kinds to celebrate and record its pupils' work and success.

Fears have been voiced in the media about the possibility of a child being identified by an image or recording and the likelihood of this creating a risk of abuse. Having taken advice from the Metropolitan Police and Richmond Borough Council, we believe the risk of a child being identified by a stranger in a way that puts the child at risk is small when images and recordings are made and used in line with the policy set out below:

Policy for the use of images and recordings

1/ Academic work and school publications (all media)

This area encompasses both publishing by your son in the course of his work at school and school publications.

For such work, children's full names will only be used alongside their images or recordings if parental permission has first been obtained. Group pictures are not subject to this condition, provided that names cannot be linked to individual boys. Other personal details (beyond year group) are not used.

2/ Authorised, external publications involving St Paul's (all media)

The School will allow media to take images and make recordings of children, when appropriate, provided that parental consent has been given. We normally give the children's full names, but not addresses, to external media. A clear statement of your agreement or disagreement to this is essential. If you do have an objection, the School will not allow external media-organisations to take or use images or recordings of your child.

Please now complete, sign and return the form overleaf. If you would like to discuss these matters in more detail, please talk to your child's tutor. In the future, should you wish to change your decision on whether to give consent, you can do so in writing at any time.

Richard Girvan
Surmaster May 2016

Consent Form for Use of Images and Recordings

We would like to seek your permission to use images (photographs or video) or recordings (video or audio) of your child. Published images or recordings may form part of or appear in: i) his academic work, ii) the school's own publications (all media), iii) authorised, external publications (all media).

Please complete and return this form. If you want a copy of the consent form to keep, please write a note to this effect on this form and one will be sent to you.

1a) I agree to allow my son's images or recordings to appear in his academic work and in the school's own publications (all media) and understand that, as a result, these images or recordings may be shared in print and/or digitally.

Yes / No

If your answer to 1a) is 'Yes', please answer 1b).

1b) I agree to the use of my son's full name alongside his images or in association with recordings.

Yes / No

2) I agree to allow images or recordings of my son to be made by and/or appear in external media and for his full name to be given to the organisations publishing the material. I understand that such images or recordings may be shared in print and/or digitally.

Yes/No

Declaration: I have read and understood the school's policy overleaf and the notes below. My decision on whether to give consent will remain valid throughout my child's time at the school, unless I notify the school to the contrary in writing.

Signed:_____ (Parent/Guardian) Print: _____

Date:_____ Name of child: _____

Please note:

- Websites can be viewed throughout the world, not just in the UK where UK Law applies.
- Material appearing online can be republished elsewhere in ways beyond the School's control.
- The school cannot be held liable for any images or recordings which find their way on to the web or into media in ways the school could neither have foreseen nor be held responsible for.

If we do not receive a signed consent from you, we will assume that we can make images and recordings of your child and use them, unidentified by his full name, in school-published media.

Please return this form in the enclosed envelope addressed to Natasha Thompson