Information Security Policy

St Paul's School for Girls aims in our mission to "promote the good of society". Our mission statement reminds us "that all persons are sacred because each is made in the image and likeness of God and is therefore deserving of respect". One of the ways in which we live out that belief is by respecting the data processed and held on each individual to thereby "treat others with a spirit of respect and responsible love."

Introduction

The Governing Body have adopted this policy to ensure we are compliant with Information Security regulations.

The Governing Body and Senior Leadership Team of St Paul's School for Girls, located at Vernon Road, Edgbaston, B16 9SL, are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout their organisation in order to preserve its legal, regulatory and contractual compliance and professional image. Information and information security requirements will continue to be aligned with St Paul's School for Girls's goals and our information security management systems are intended to be an enabling mechanism for information sharing, for electronic operations, and for reducing information-related risks to acceptable levels.

St Paul's School for Girls's current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information-related risks.

Fundamental to this policy are business continuity and contingency plans, data back-up procedures, avoidance of viruses and hacks, access control to systems and information security incident reporting are fundamental to this policy.

St Paul's School for Girls aims to achieve specific, defined information security objectives, which are developed in accordance with the business objectives, the context of the organisation, the results of risk assessments and associated risk reduction plans.

All governors, employees and volunteers of St Paul's School for Girls and any associated data processors are expected to comply with this policy. All governors, employees and volunteers will receive appropriate training. Data processors will be required to provide training of a similar nature. The consequences of breaching the information security policy are set out in the disciplinary policy and in contracts and agreements with third parties.

This policy will be reviewed at least annually, to respond to any changes in the risk assessment or risk treatment plan and at least annually.

In this policy, 'information security' is defined as:

Preserving

This means that governors, all full-time or part-time employees, volunteers, sub-contractors, project consultants and any external parties have, and will be made aware of, their responsibilities to preserve information security, to report security breaches and to act in accordance with the requirements of the law. All governors, employees and volunteers will receive information security awareness training and more specialised employees will receive appropriately specialised information security training.

the availability,

This means that information and associated assets should be accessible to authorised users when required and therefore physically secure. The computer network must be resilient and St Paul's School for Girls must be able to detect and respond rapidly to incidents such as viruses and other malware that threaten the continued availability of assets, systems and information. There must be appropriate business continuity plans.

confidentiality

This involves ensuring that information is only accessible to those authorised to access it and therefore to preventing both deliberate and accidental unauthorised access to St Paul's School for Girls information and its systems, including its network and website.

and integrity

This involves safeguarding the accuracy and completeness of information and processing methods, and therefore requires preventing deliberate or accidental, partial or complete, destruction or unauthorised modification, of either physical assets or electronic data. There must be appropriate contingency, including for the network and website, and data back-up plans and security incident reporting. St Paul's School for Girls must comply with all relevant data-related legislation in those jurisdictions within which it operates.

of the physical (assets)

The physical assets of St Paul's School for Girls including, but not limited to, computer hardware, data cabling, telephone systems, filing systems and physical data files.

and information assets

The information assets include information printed or written on paper, transmitted by post or shown in films, or spoken in conversation, as well as information stored electronically on servers, website(s), extranet(s), intranet(s), PCs, laptops, mobile phones and PDAs, as well as on CD ROMs, floppy disks, USB memory sticks, back-up tapes and any other digital or magnetic media, and information transmitted electronically by any means. In this context, 'data' also includes the sets of instructions that tell the system(s) how to manipulate information (i.e. the software: operating systems, applications, utilities, etc).

St Paul's School for Girls and such partners that are part of our integrated network and have signed up to our security policy.

A **SECURITY BREACH** is any incident or activity that causes, or may cause, a break down in the availability, confidentiality or integrity of the physical or electronic information assets of St Paul's School for Girls.

This policy was approved by the Governing Body on 01/05/2018 and is issued on a version controlled basis by the Governing Body.