INFORMATION SECURITY POLICY

Prepared:  Sept 2016
Reviewed:
Approved by Governing Body: 

Author:  Lisa Hughes
Next Review:  Dec 2019
Date:  08/11/16
Introduction
Schools collect and process personal information to deliver educational services. This information is held about a variety of people and it is essential that the availability and confidentiality of accurate relevant information is maintained in a secure and legal environment. Longford Park School is committed to full compliance with its responsibilities under the Data Protection Act 1998. To actively demonstrate this, the School has issued a policy commitment which provides assurance to pupils, parents, governors and staff that sound and secure measures are in place to protect the confidentiality, integrity and availability of their information.

Objective
The information security objective is to ensure that the school’s information base is protected against identified risks so that it may continue to deliver its services and obligations to the community. It also seeks to ensure that any security incidents have a minimal effect on its business and academic operations.

Policy
The purpose of this policy is to protect the school’s information assets from all threats, whether internal or external, deliberate or accidental. The key aims of the policy are to ensure that:

• Information is protected from unauthorised access.
• Confidentiality of personal or sensitive information is assured.
• Integrity of information is maintained.
• Information is disposed of in a timely, appropriate and secure manner.
• Legislative requirements and school policy and practices are observed.
• Business continuity plans are produced, maintained and tested.
• Data protection/ information security training is available to all school staff.
• Appropriate monitoring and reporting processes are put in place to identify and act upon breaches of information security

Supporting Framework
Examples of measures to achieve the above are physical security, virus control and the use of passwords for access control.

Responsibilities to Ensure Security of Personal Data
The school’s Head Teacher has direct responsibility for maintaining this policy and providing advice and guidance on its implementation.

All staff are responsible for policy implementation and for ensuring that they manage and adhere to the standards. All staff are aware of the action that can be taken by the ICO and the penalties that can be issued if the school is found to breach data protection (See Appendix 1). The school has a “Data Breach Management Policy” that gives guidance to staff on the appropriate course of action should a security breach present itself.
Managing and Reducing the Risk of a Security Breach

- The School will ensure that appropriate security measures are in place and enforced to keep paper and electronic personal data secure.
- The School will regularly review the physical security of the School buildings and storage systems.
- The School will ensure that only authorised individuals have access to personal data.
- The School does not allow for portable electronic devices to be used for the storing of personal data.
- No personal data will be left unattended in any vehicles and staff will ensure that if it is necessary to take personal data from School premises, for example to complete work from home, the data is suitably secured.
- Staff are encouraged to log with the school administrator any pupil files taken from the filing cabinets, thus creating an audit trail and ability to locate the file if needed.
- Staff are encouraged to adopt a clear desk policy. This is the best way to avoid unauthorised access to physical records which contain sensitive or personal information.
- Staff are aware that they only need access to the minimum amount of data needed to do their job.
- Staff are aware of the importance of ensuring that personal information is only disclosed to people who are entitled to receive it.

Photographs and Electronic Images
The School has developed a number of policies in relation to the use of photographs/videos that contain images of pupils. (See eSafety Policy & Acceptable Use Policies). These policies provide the School's position regarding the use of images of pupils by the School in any School publicity material, its website, in newspapers and in outside agency publications.

Parents are informed at events that photography and filming is permitted, they are advised to focus on their own child and that they are not permitted to reproduce, upload to social media or share with anyone other than immediate family.

Biometric Data
Should the school use biometric data (such as fingerprint technology) a separate, detailed notice would be sent to all pupils and parents explaining the intended use and providing parents with options for alternative systems if they wish their child to opt out.

The School would obtain the written consent of at least one parent before taking and using and biometric data from a pupil.
CCTV
Images and audio recordings of identifiable individuals captured by Closed Circuit Television amount to personal data relating to that individual and will be subject to the same provisions and safeguards afforded by the Data Protection Act as other types of recorded information.

The School may use CCTV for the following purposes:
- To protect the school buildings and assets
- To increase personal safety of staff, pupils and visitors
- To reduce the fear of crime
- To support the Police in order to deter and detect and to apprehend and prosecute offenders
- To help protect members of the public and private property.

The School will ensure that any use of CCTV is necessary and proportionate to achieve the aims stated above and will ensure that regular reviews of the use of CCTV within the School take place.

The School will ensure that any use of CCTV is included in its notification to the ICO.


The School will ensure that clear notices are in place identifying when an individual is entering an area that is monitored by CCTV. The notice will identify the School as the responsible data controller and will state the purpose for which the recording is taking place.

The School will not operate audio recording as part of the CCTV.

The School will not operate CCTV in any areas of the premises where individuals would have a legitimate expectation of personal privacy, such as toilets or changing rooms.

The School does not presently record CCTV coverage. However, if it did it would keep recordings securely and ensure access to recordings was restricted to those staff who operate the system or to make decisions relating to how the images should be used.

Implementation
This policy will be made available to all pupils, parents, guardians, staff (whether permanent or temporary) and governors.

Relationship with existing policies
This policy has been drawn up within the context of:
• Freedom of Information Policy
• Data Protection Policy
• Records Management Policy
• Data Breach Management Policy
• eSafety Policy
• Acceptable Use Policy & Acceptable use Policy Staff iPad
• and with other legislation or regulations (including audit, equal opportunities and ethics) affecting the school.
Appendix 1 - Action that can be taken by the ICO and the penalties that can be issued if the school is found to breach data protection


Taking Action – Data Protection

There are a number of tools available to the Information Commissioner’s Office for taking action to change the behaviour of organisations and individuals that collect, use and keep personal information. They include criminal prosecution, non-criminal enforcement and audit. The Information Commissioner also has the power to serve a monetary penalty notice on a data controller.

The tools are not mutually exclusive. We will use them in combination where justified by the circumstances.

The main options are:

- serve information notices requiring organisations to provide the Information Commissioner’s Office with specified information within a certain time period;
- issue undertakings committing an organisation to a particular course of action in order to improve its compliance;
- serve enforcement notices and ‘stop now’ orders where there has been a breach, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- conduct consensual assessments (audits) to check organisations are complying;
- serve assessment notices to conduct compulsory audits to assess whether organisations processing of personal data follows good practice;
- issue monetary penalty notices, requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act occurring on or after 6 April 2010;
- prosecute those who commit criminal offences under the Act; and
- report to Parliament on issues of concern.


Taking action – Privacy and Electronic Communications Regulations

There are a number of tools available to the Information Commissioner’s Office for taking action to change the behaviour of anyone who breaches the Privacy and Electronic Communications Regulations (PECR). They include criminal prosecution, non-criminal enforcement and audit. The Information Commissioner also has the power to serve a monetary penalty notice imposing a fine of up to £500,000.

These powers are not mutually exclusive. We will use them in combination where justified by the circumstances.

We can:

- issue an undertaking committing an organisation to a particular course of action in order to improve its compliance;
- conduct an audit to check a service provider is complying with its security obligations, and make recommendations;
- serve an enforcement notice or ‘stop now’ order where there has been a breach, requiring an organisation to take specified steps to comply with the law. Failure to comply is a criminal offence;
- issue a Monetary Penalty Notice, requiring an organisation to pay up to £500,000 for serious breaches;
- impose a fixed penalty of £1,000 on a service provider who fails to notify us of a security breach;
- apply to the court for an order under section 213 of the Enterprise Act 2002 requiring a person to cease conduct harmful to consumers;
- prosecute if the breach also involves a criminal offence under the Data Protection Act, or if an organisation fails to comply with an Enforcement Notice (except in Scotland, where the Procurator Fiscal brings prosecutions); and
- report to Parliament on issues of concern.

On 6 April 2015 the threshold for issuing monetary penalties under PECR changed. An amendment to the Regulations removed the requirement for the ICO to consider whether the contravention is likely to have caused substantial damage or substantial distress. The ICO will be able to issue a penalty for any serious contraventions of regulations 19 to 24 in PECR (these provisions cover automated calling and direct marketing). We are in process of updating the monetary penalties guidance issued under section 55C (1) of the Data Protection Act 1998, this will be published once the Secretary of State has been consulted and the guidance has been laid in Parliament. We will highlight the update in our e-newsletter and on the website.