Personal Data Protection Policy
2014-2016

Introduction
This school will do everything in its power to ensure the safety and security of any material of a personal or sensitive nature

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- have permission to access that data
- need to have access to that data

Any loss of personal data can have serious effects for individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action and / or criminal prosecution. All transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy.

The Data Protection Act (1998) lays down a set of rules for processing of personal data (both structured manual records and digital records). It provides individuals (data subjects) with rights of access and security and requires users of data (data processors) to be open about how it is used and to follow "good information handling principles".

Guidance for organisations on the DPA is available on the Information Commissioners Office website: http://www.ico.gov.uk/for_organisations/data_protection_guide.aspx

Policy Statements
The school will hold the minimum personal information necessary to enable it to perform its function and information will be erased once the need to hold it has passed.

Every effort will be made to ensure that information is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

All personal data will be fairly obtained in accordance with a "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".

The school and individuals will have access to a wide range of personal information and data. The data may be held in digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including *pupils / students*, members of staff and parents and carers e.g. names, addresses, contact details, legal guardianship / contact details, health records, disciplinary records
- Curricular / academic data e.g. class lists, pupil / student progress records, reports, references
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members

Responsibilities
The school's Senior Information Risk Officer (SIRO) is the Head teacher. They will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's information risk policy and risk assessment
- appoint the Information Asset Owners (IAOs)

The School will identify Information Asset Owners (IAOs) for the various types of data being held (e.g. pupil / student information / staff information / assessment data etc). The IAOs will manage and address risks to the information and will understand:

- what information is held and for what purpose?
- how information has been amended or added to over time
- who has access to protected data and why?

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

Registration
The school will maintain its registration as a Data Controller on the Data Protection Register (Registration number Z7244226) held by the Information Commissioner.

Information to Parents / Carers – the "Privacy Notice"
The school will inform parents / carers of all pupils of the data they hold on the pupils, the purposes for which the data is held and the third parties (e.g. LA, DfE, QCDA, etc) to whom it may be passed. This Privacy notice will be passed to parents / carers through the initial induction paperwork and prospectus. Parents / carers of young people who are new to the school will be provided with a Privacy notice through the same process as above.

Training & Awareness
All staff will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff
- Staff meetings / briefings / Inset
- Day to day support and guidance from Information Asset Owners

Risk Assessments
Information risk assessments will be carried out by Information Asset Owners to establish the security measures already in place and whether they are the most appropriate and cost effective.

Protective marking
All documents (manual or digital) will be labelled clearly according to their sensitivity.

Storage of and access to data

The school will ensure that ICT systems are set up so users will be assigned a clearance that will determine which files are accessible to them. Access to sensitive data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system or to every document store.

All users will be given secure user names and strong passwords which must be changed regularly. User names and passwords must never be shared.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left unattended.

All documents and storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or degradation according to the sensitivity of the data and the schools Retention Schedule.

Personal data can only be stored on school equipment. Private equipment (i.e. owned by the users) must not be used for the storage of personal data.

The school IT network is secure and staff are able to securely remotely access the system if required and permission has been given. There is therefore no need for any information to be removed from school on any electronic format. Staff are forbidden from using any personal device to transport data unless with specific advance approval of the Head teacher and this will only be in unusual situations where no other method is possible.

The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including any off-site backups.

All paper based Protected and Restricted (or higher) material must be held in lockable storage.

Data Subject Rights
The school recognises that under Section 7 of the Data Protection Act, data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place, following written requests to the Head teacher to see all or a part of the personal data held by the data controller in connection with the data subject, to deal with Subject Access Requests. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

Secure transfer of data and access out of school
The school recognises that personal data may be transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location.
- Users must take particular care that their personal computers must not be accessed by other users (e.g. family members) when logged into the school system.
- When sensitive or personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their

home), they should have secure remote access to the management information system or learning platform
- Particular care should be taken if data is taken or transferred to another country, particularly outside the European Economic Area, and advice is to be sought in this event. (N.B. to carry encrypted material is illegal in some countries)

Disposal of personal data
The school will comply with the requirements for the safe destruction of personal data when it is no longer required according to the retention Schedule.

Incident Handling
The school will introduce a policy for reporting, managing and recovering from information risk incidents.

Use of Cloud Services
The school has a Cloud Service run by Microsoft 365. Data for the school is hosted within the EU. The primary Microsoft data service centre host is in Dublin and the fail-over is in Amsterdam. Data is backed-up daily and multiple copies are kept across the two Microsoft data-centres. Microsoft has a clear process for recovering data. Individual users can recover data themselves up to 30 days after deletion. Administrators then have a further 30 days to recover this once the item is deleted from the deleted-items folder.
Microsoft protects privacy through, no advertising, no mixing of Office 365 data with consumer services (such as Hotmail) and full data-portability. Data remains the property of the school and not Microsoft. The school retains all rights, titles and interest in the data stored with Office 365. Downloaded copies of the school data can be downloaded at any time for any reason, by recognised users, without assistance from Microsoft. The data stored by the school can only be accessed by those with authorised usernames and log-ins. Microsoft employees who have completed appropriate background checks and have justified need can raise an escalation for time-limited access to Customer data. Access is regularly audited, logged and verified through the ISO 27001 Certification. As detailed in a recent accreditation submission to the UK Government, any organisation that specify "UK" as their country during tenant creation will be provisioned and data stored within the EU data-centres (Dublin and Amsterdam). Microsoft has been granted accreditation up to and including the UK government's "Impact Level 2" (IL2) assurance for Office 365. As of February 2013 Microsoft are the only major international public cloud service provider to have achieved this level of accreditation and, indeed, it is the highest level of accreditation possible with services hosted outside of the UK (but inside of the EEA).
Personal information stored on the Cloud Service is not shared with anyone else including third party advertisers. Microsoft uses 5 layers of security - data, application, host, network and physical and Microsoft offers a comprehensive standard Data Processing Agreement (DPA) to all customers. DPA addresses privacy, security and handling of customer data. Our standard Data Processing Agreement enables customers to comply with their local regulations.

The school requires a reliable service to ensure data protection and privacy. Microsoft Office 365 has a 99.9% reliability guarantee and the school has had 100% reliability with the provider in the past. Microsoft offer schools direct telephone support 24/7 for IT administrators and there is also a large range of online help services.