Personal Data Handling Policy

1 Scope

The School will do everything within their 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, which brings together the legal requirements contained in relevant data legislation and relevant regulations and guidance from the Local Authority.

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.

2 Requirements

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 the “Fair Processing Notice” and lawfully processed in accordance with the “Conditions for Processing”.

Personal Data

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 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, 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

The School's Senior Information Risk Officer (SIRO) is the School Manager. The SIRO 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
- Determine what information is held and for what purpose
- Determine 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.

Directors 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 Director.

The School is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

Information to Parents / Carers – The Fair Processing Notice

Under the "Fair Processing" requirements in the Data Protection Act, the School will inform parents / carers of all students of the data they hold on the students, the purposes for which the data is held and the third parties (e.g. LA, DCSF, QCA, Connexions etc) to whom it may be passed. The School Privacy Notice policy contains the fair processing notice and is part of the new student pack passed to parents / carers of students enrolling at the School.

Training and 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 SIRO

Secure Storage of and Access to Data

The School will ensure that IT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected 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.

All users will be given secure user names and strong passwords which must be changed regularly as defined in the Password Security Policy, 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 (even for very short periods) and set to auto lock if not used for ten minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on School provided equipment (computers, laptops and portable storage media). Private equipment (i.e. owned by the users) must not be used for the storage of personal data. When personal data is stored on any portable computer system, USB stick or any other removable media:

- The data must be encrypted and password protected
- The device must be password protected
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, once it has been transferred or its use is complete

The School has clear policy and procedures for the automatic backing up, accessing and restoring all data held on School systems, including alternative located backups.

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

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 to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. 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 recognizes that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or personal data from the School or authorized 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 computers or removable devices which contain personal data must not be accessed by other users e.g. family members, when out of school.
- When sensitive or personal data is required by an authorized user from outside the organisation's premises, e.g. by a member of staff to work on from home, they must use the secure remote access to the management information system or the learning platform.
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location.
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority in this event.

Disposal of Data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required. The The disposal of protected data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance, and other media must be shredded, incinerated or otherwise disintegrated for data.

Staff Responsibilities at the end of their Employments / Change of Duties

At the end of employment at the School staff must dispose of all protected data in a way that makes reconstruction highly unlikely. Staff changing duties and responsibilities within the School must ensure that any protected data no longer relevant to their new duties or responsibilities is disposed of in a way that makes reconstruction highly unlikely.

Audit Logging / Reporting / Incident Handling

It is good practice, as recommended in the "Data Handling Procedures in

Government" document that the activities of data users, in respect of electronically held personal information, will be logged and these logs will be monitored by responsible individuals.

The audit logs will be kept to provide evidence of accidental or deliberate security breaches – including loss of protected data or breaches of an acceptable use policy, for example.

The School has a policy for reporting, managing and recovering from information risk incidents, which establishes:

- A "responsible person" for each incident
- A communications plan, including escalation procedures
- and results in a plan of action for rapid resolution and
- A plan of action of non-recurrence and further awareness raising.

All significant data protection incidents must be reported through the SIRO to the Information Commissioner's Office based upon the local incident handling policy and communication plan.

3 Key Terms and Definitions

ACRONYM	TERM	DEFINITION
LA	Local Authority	
DCSF	Department for Children, Schools and Families	
SIRO	Senior Information Risk Officer	School Manager
QCA	Qualifications and Curriculum Authority	

Amendment Record

VERSION #	DATE	AMENDED BY	NATURE OF CHANGE
9.1	25.09.14	Ben Webber	Update to Academy policy format