THE HOLY SPIRIT CATHOLIC MULTI-ACADEMY COMPANY

Schools: Our Lady of the Angels Infant School and Nursery, St. Anne's Catholic Primary School, St. Benedict's Catholic Primary School, St. Francis Catholic Primary School, St. Joseph Junior School, St. Thomas More School and Sixth Form College.

Data Protection Policy

Ratified at Directors Meeting on:……..

Signed ……Chair of Directors

Date…….

To be reviewed annually in the Summer term.

Introduction

All member schools have always held personal data on the pupils in our care, and increasingly this data is held digitally and accessible not just in member schools but also from remote locations. Legislation covering the safe handling of this data is addressed by the UK Data Protection Act 1998 and following a number of losses of sensitive data, a report was published by the Cabinet Office in June 2008, Data Handling Procedures in Government. This stipulates the procedures that all departmental and public bodies should follow in order to maintain security of data.

Given the personal and sensitive nature of much of the data held in our Member schools, it is critical that we adopt these procedures too.

It is important to stress that the Personal Data Policy applies to all forms of personal data, regardless of whether it is held on paper or in electronic format.

All member schools will do everything within 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 each school community to take care when handling, using or transferring personal data that it can not 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 schools 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”. Guidance on the DPA is available on the Information Commissioners Office website : http://www.ico.org.uk

Policy Statements

All member schools 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 member school's Privacy Notices which are distributed to all students and staff. Data will be lawfully processed in accordance with the "Conditions for Processing".

Personal Data

All member schools 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 schools' 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 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

Each member school will have a named Data Protection Officer who will keep up to date with current legislation and guidance. Guidance for Managing Information Risk is available at

http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf

The Member schools will identify Information Asset Owners (IAOs) who will manage sensitive 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 schools have 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.

Information to Parents / Carers – the "Privacy Notice"

Under the "Fair Processing" requirements in the Data Protection Act, each member schools will inform parents / carers of all students of the type of data they hold on the students, the purposes for which the data is held and the third parties (eg LA, DCSF, QCA, etc) to whom it may be passed.

This privacy processing notice will be distributed to all parents / people with parental responsibility. Parents / carers of young people who are new to the school will be provided

with the privacy notice and the privacy notice supplementary information which details 3rd parties with whom we are required to share information.

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

Secure Storage of and access to data
The College will ensure that ICT 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 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 whole management information systems.
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 five 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 schools equipment (this includes computers 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 and
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus checking software (memory sticks will not provide this facility)
- the data must be securely deleted from the device, once it has been transferred or its use is complete

Member schools have clear policies and procedures for the automatic backing up, accessing and restoring of all data held on schools systems, including off-site backups (see ICT Security Policy).

All paper based sensitive material must be held in lockable storage.

The Member schools recognise 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 protection officers in connection with the data subject. Data subjects have the right to know: if the data

protection officer 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 member schools

Member schools recognise 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 schools 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 computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of schools.
- When sensitive or personal data is required by an authorised user from outside schools premises (for example, by a member of staff to work from their home), they should only access it via a secure remote connection to the management information system or 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

Member schools will comply with the requirements for the safe destruction of personal data when it is no longer required. The disposal of sensitive data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely.

The following provides a useful guide:

	The Information	**The Technology**	**Notes on Protect Markings**
School life and events	School terms, holidays, training days, the curriculum, extra-curricular activities, events, displays of pupils work, lunchtime menus, extended services, parent consultation events	Common practice is to use publically accessible technology such as school websites or portal, emailed newsletters, subscription text services	Most of this information will fall into the NOT PROTECTIVELY MARKED category.
Learning and achievement	Individual learner's academic, social and behavioural achievements, progress with learning, learning behaviour, how parents can support their child's learning,	Typically Colleges will make information available by parents logging on to a system that provides them with appropriately secure access, such as a	Most of this information will fall into the PROTECT category. There may be learners whose personal data requires a RESTRICTED marking or higher. For example, the home address of

	assessments, attainment, attendance, individual and personalised curriculum and educational needs.	Learning Platform or portal, or by communication to a personal device or email account belonging to the parent.	a child at risk
Messages and alerts	Attendance, behavioural, achievement, sickness, school closure, transport arrangements, and other information that it may be important to inform or contact a parent about as soon as possible. This may be particularly important when it is necessary to contact a parent concerning information that may be considered too sensitive to make available using other online means.	Email and text messaging are commonly used by schools to contact and keep parents informed. Where parents are frequently accessing information online then systems e.g. Learning Platforms or portals, might be used to alert parents to issues or be used to provide further detail and context.	Most of this information will fall into the PROTECT category. However, since it is not practical to encrypt email or text messages to parents, schools should not send detailed personally identifiable information. General, anonymous alerts about schools closures or transport arrangements would fall into the NOT PROTECTIVELY MARKED category.