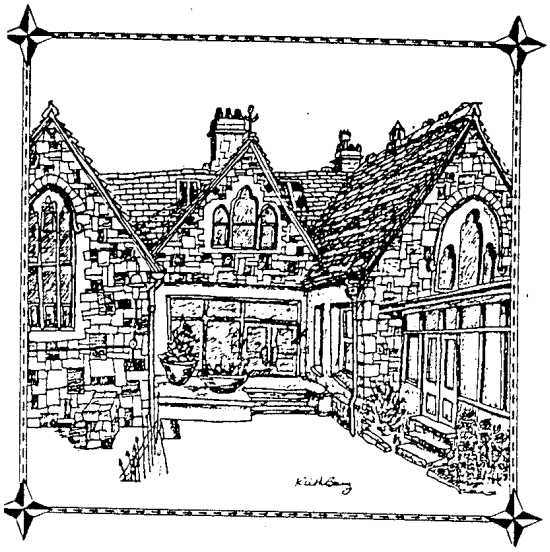
Dunster First School



Information Security Policy

May 2011

Introduction
Schools should 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.

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 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 and individual and provides specific information about them, their families or circumstances. This will include:

- personal information about members of the school community – including pupils, members of staff and parents and carers eg names, addresses, contact details, legal guardianship, health record, disciplinary records;
- curricular/academic data eg class lists, pupil progress records, reports, references
- professional records eg 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 Peter Hoyland who will keep up to date with current legislation and guidance and will determine and take responsibility for the school's information security policy and risk assessment.

The school has identified the School Business Manager, Admin Assistant and Class Teachers as Information Asset Owners (IAOs) for the various types of data being held (eg pupil 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 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 pupils of the data they hold on the pupils, the purposes for which the data is held and the third parties (eg LA, DfE and feeder schools) to whom it may be passed. The fair processing notice will be sent to parents/carers annually in September and is published on the school's website.

Training and Awareness
All staff will be made aware of their responsibilities with regard to data handling awareness and data protection through:

- induction training for new staff;
- staff meetings/briefings/INSET
- day to day support and guidance from the Information Asset Owners.

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

- recognising the risks that are present;
- judging the level of the risks (both the likelihood and consequences);
- prioritising the risks.

Secure Storage of and Access to Data

The school 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 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 have secure user names and strong passwords which must be changed regularly according to LA 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).

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 equipment (this includes computers and portable storage media). Private equipment (ie 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 of all data held on school systems.

All paper based sensitive 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 (detailed in the school's Publication Scheme) ie 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 recognises 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 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 (eg family members) when out of school;

- 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 preferably have secure remote access 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.

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

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.

Incident Handling
The school's has procedures for managing and recovering from information risk incidents which establish:

- 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 for 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.