DATA PROTECTION POLICY

This policy was agreed by the Governing Body in February 2012 and implemented in February 2012. It will be reviewed in March 2018.

Signed …….. Chair of Governors

Signed …….. Headteacher

All school employees have a right to know what information is being kept on them by the school and/or the LEA.

The legal right for individuals to gain access to personal files containing information about them was first introduced in the **1984 Data Protection Act**. At that time the legislation only covered information held on computer and the misuse of that information.

The Data Protection Act 1998 extended the right to manual records.

Since October 2001 all workers have full right of access to their personal files whether held manually or on computer. These are known as 'relevant filing systems', i.e. they are kept in such a way that particular information is readily accessible e.g. a card index or files kept in a filing cabinet or filed away on computer files.

Personal Data

Personal data means the data relating to a living individual who can be identified from the information in the file or information which is likely to come into the possession of the 'data controller'.

For school staff the Head is likely to be the 'data controller' along with, in most cases, the LEA. It can include sensitive data. Therefore, any expressions of opinion about a teacher or any recorded intentions by the Head towards the teacher, count as data for the purposes of the Act.

Principles

The data protection principles to which all schools should adhere were set out in the 1984 Act, and repeated in 1998. These are that personal data -

- **should be processes lawfully and fairly**
- **should be held for one or more specified purposes**
- **should not be disclosed in any manner incompatible with the purposes for which it is held**
- **should be held in such a way that is adequate, relevant and not excessive for the purposes for which held**
- **should be accurate and up-to-date**
- **should not be held longer than necessary**

In addition, a member of staff should be informed regularly and without undue delay or expense whether any information about him/her is being kept. They should also be given access to the information, and are entitled, where appropriate, to have any data corrected or erased.

Finally the principles say that security measures should be taken to guard against unauthorised access to or alteration to, disclosure or destruction of personal data and against accidental loss or destruction of such personal data.

Handling the Information

If the school holds records on a computer or on computer disks, the school is designated as a 'data user' under the Act. The individual member of staff does not have to give consent to the information being held, unless it is 'sensitive' material. In this case the member of staff must give permission.

The member of staff also has a right to be informed whether any personal data, sensitive or otherwise, is being kept, and to be supplied with a copy of it, if a request is made in writing and an appropriate fee is paid (current maximum of £10)

The governing body, through the Head as the immediate data controller, owes a duty to all staff members whose details are held on file to allow access to the file when a request is received, which must be in writing. A reasonable fee could be charged, and if inaccuracies are pointed out the Head must ensure that they are corrected or removed.

The member of staff has a right to know whether the information is being kept by 'automatic' means, and if so, whether this information is likely to constitute the sole basis for any decisions affecting him/her, and what logic is involved in the decision-making process.

If the school failed to comply with a request for details of the information held the individual could seek a court order requiring the school to do so.

Damage and Distress

A member of staff could at any time require the school to cease, or not begin, processing personal details about him/her, on the grounds that it is likely to cause substantial unwarranted damage or distress to him/her or another person. The school would have to reply within 21 days stating whether it had complied, and if not, what the reasons were. This does not apply if the processing of the data is necessary to protect the colleague's own interests, or to comply with legal requirements.

The school, as the data user, could be forced to pay compensation for damages or distress if the data was lost, destroyed or inaccurate. It is, therefore, important for governing bodies to ensure that their school records systems are efficient and secure. Periodic checks should be part of the governors' annual checklist.

Confidential References

Heads can still write confidential references for specified purposes, such as for training or employment. Staff cannot demand access to these. However, the material on which the reference is based if kept on file can be accessed by the member of staff.

In addition, the data controller at the receiving end, say the Head to whom a confidential reference for a job is sent, must give access to the information if requested to by the applicant. In effect this means that Heads should consider carefully whether to write confidential references. It may be wiser to discuss the contents with the colleague who is applying for a new post, and to send an open reference.

Pupil Records

Pupils are entitled to the same protection as anyone else, and the same care should be taken with their files.

However, pupils have no right of access to personal data recorded when they were sitting an examination.

As far as examination marks are concerned pupils do have the right of access to examination marks no later than 5 months from the date of their request or 40 days from the announcement of the results, whichever is shorter.

The practice of returning candidates' examination papers has clearly added to the whole move towards transparency of personal information.

The Commissioner

Under the **1984 Data protection Act** a Registrar was responsible for the registration of all data users and for enforcement of the legislation. The 1998 Act replaced the Registrar with a Data Protection Commissioner (eventually to be known as the **Information Commissioner**) with wider enforcement powers and also a new duty to promote good practice. The existing registration process is simplified and is now called ' notification'.

Each school or LEA, as data users, has to nominate a named person who is responsible for compliance with the provisions. The filing system containing either computerised information or manual records must be managed by a 'data controller'.

Since the 1998 Act schools and LEAs have had to notify the Commissioner of their processing of personal data. LEAs usually do this for their schools. LEAs and schools which were previously registered with the Registrar have to notify the new Commissioner when their current registration runs out.

Criminal Offence

If the Commissioner has grounds for suspecting a breach of the law, or where someone has lodged a complaint the Commissioner has the power to issue a notice requiring the data controller to respond.

And if any of the data protection principles have been contravened the Commissioner can issue an enforcement notice. If a school or LEA failed to comply with the order they could be prosecuted for a criminal offence!

However, most disputes will normally be brought to the Information Tribunal which has superseded the Data Protection Tribunal.

Code of Practice

A Code of Practice has been instigated by the Commissioner and has been issued piecemeal from 2000. The Code is divided into five sections:

- Background
- The Code
- Further Information
- Frequently asked questions
- Checklists

It does not have the force of law. Schools must comply with the Act itself. But the benchmarks are the Commissioner's own recommendations and therefore strongly persuasive. For further information see Appendix A

Compiled by: Stuart Rogers, Business and Facilties Manager	Revision Number: 6
Approved by: SMT, Governing Body	Revision date: March 2018 Person Responsible for Revision: S Rogers