Great Gaddesden C.E.(VA) Primary School

Data Protection Policy

Written: May 2015

Ratified: October 2015

Reviewed: October 2017

Reviewed

Introduction:

The purpose of the policy is to raise awareness on safe handling of data, data security, roles and responsibilities and where potential breaches of security could occur, identify the Records required to be retained by the school and to ensure confidentiality and manageable procedures in relation to access to such records by parents, staff and other stake holders.

Following these principles will help our staff prevent information from being lost or used in a way which may cause individuals harm or distress and/or prevent the loss of reputation our school might suffer if you lose sensitive information about individuals.

Rationale:

- A policy on data protection and record keeping is necessary to ensure that the school has proper procedures in place in relation to accountability and transparency
- It is good practice to record pupil progress so as to identify learning needs
- A policy must be put in place to ensure a school complies with legislation such as;
    - Education Act 1998
    - Education Welfare Act 2000
    - Data Protection Act 2003
    - Freedom of Information Act 1997
    - The National Strategy to improve Literacy and Numeracy among Children and Young People 2011 – 2020

Aims/Objectives:

- To ensure the school complies with legislative requirements
- To clarify the types of records maintained and the procedures relating to making them available to the relevant bodies
- To put in place a proper recording and reporting framework on the educational progress of pupils
- To establish clear guidelines on making these records available to parents and pupils over 18 years of age.
- To stipulate the length of time records and reports will be retained

2015 Policy on Data Protection:

Please read in conjunction with document “**Staff Guidance – Data Security in schools - Dos and Don’ts”.**

Responsibilities

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

The ICO's new powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.

The data protection powers of the Information Commissioner's Office are to:

- Conduct assessments to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern

Details of arrangements in place to ensure compliance with the eight rules of data protection

The policy will be implemented so as to ensure that all personal data records held by the school are obtained, processed, used and retained in accordance with the following eight rules of data protection (based on the Data Protection Acts):

1. Obtain and process information fairly
2. Keep it only for one or more specified, explicit and lawful purposes
3. Use and disclose it only in ways compatible with these purposes
4. Keep it safe and secure
5. Keep it accurate, complete and up-to-date
6. Ensure that it is adequate, relevant and not excessive
7. Retain it for no longer than is necessary for the purpose or purposes
8. Give a copy of his/her personal data to that individual or to their parent/carer on request.

Status of this Policy

This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the School from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings

The Data Controller and the Designated Data Controllers

The School as a body corporate is the Data Controller under the 1998 Act, and the Governors are therefore ultimately responsible for implementation. However, the Designated Data Controllers (SIRO and IAO) will deal with day to day matters.

The School has two Designated Data Controllers: The SIRO (Senior Information Risk Owner) is the Headteacher and IAO (Information Asset Owner) is the school secretary

Senior Information Risk Owner (SIRO)

The SIRO is a senior member of staff who is familiar with information risks and the school's response and has the following responsibilities:

- They own the information risk policy (strategies in place to identify and manage risks associated with information breaches) and risk assessment – see link below
- They appoint the Information Asset Owner(s) (IAOs)
- They act as an advocate for information risk management

The Office of Public Sector Information has produced Managing Information Risk, [http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf] to support SIROs in their role.

Information Asset Owner (IAO)

Any information that is sensitive needs to be protected. This will include the personal data of learners and staff; such as assessment records, medical information and special educational needs data. Schools should identify an Information Asset Owner. The school's Management Information System (MIS) is identified as an asset. Please refer to the appendix at the back of this document showing examples of assets a school may hold.

The ICT Subject Leader will:

- Ensure all staff are made aware of the guidance document "Staff Guidance – Data Security in schools – Dos and Don'ts" available on the grid. http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata

- Issue staff with School Policy for ICT Acceptable Use (eSafety, Data Security & Disposal of ICT Equipment) This contains significant guidance on esafety and data security http://www.thegrid.org.uk/eservices/safety/policies.shtml
- raise any security concerns & report any incidents – through the 'Audit logging and incident handling' - [http://schools.becta.org.uk/upload-dir/downloads/audit_logging.pdf]

Any member of staff, parent or other individual who considers that the Policy has not been followed in respect of personal data about himself or herself or their child should raise the matter with the appropriate Designated Data Controller, who would be: The Head teacher

.

Responsibilities of Staff

All staff are responsible for:

- Checking that any information that they provide to the School in connection with their employment is accurate and up to date.
- Informing the School of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently.
- The School cannot be held responsible for any errors unless the staff member has informed the School of such changes.
- If and when, as part of their responsibilities, staff collect information about other people (e.g. About a student's course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines for staff set out in the Schools Data Protection Code of Practise.

Data Security

All staff are responsible for ensuring that:

- Any personal data that they hold is kept securely.
- Personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.
- Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Personal information should:

- Be kept in a locked filing cabinet, drawer, or safe; or If it is computerised, be coded, encrypted or password protected and held on the school server.
- If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

Rights to Access Information

All staff, parents and other users are entitled to:

- Know what information the School holds and processes about them or their child and why.
- Know how to gain access to it.
- Know how to keep it up to date.
- Know what the School is doing to comply with its obligations under the 1998 Act.

This Policy document and the School's Data Protection Code of Practise address in particular the last three points above. To address the first point, the School will, upon request, provide all staff and parents and other relevant users with a statement regarding the personal data held about them. This will state all the types of data the School holds and processes about them, and the reasons for which they are processed.

All staff, parents and other users have a right under the 1998 Act to access certain personal data being kept about them or their child either on computer or in certain files. Any person who wishes to exercise this right should complete the Subject Access Request Form and submit it to the Designated Data Controller.

The School will make a charge of £10 on each occasion that access is requested, although the School has discretion to waive this.

The School aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days, as required by the 1998 Act.

Subject Consent

In many cases, the School can only process personal data with the consent of the individual. In some cases, if the data is sensitive, as defined in the 1998 Act, express consent must be obtained. Agreement to the School processing some specified classes of personal data is a condition of acceptance of employment for staff. This includes information about previous criminal convictions. Jobs will bring the applicants into contact with children. The School has a duty under the Children Act 1989 and other enactments to ensure that staff are suitable for the job. The School has a duty of care to all staff and students and must therefore make sure that employees and those who use School facilities do not pose a threat or danger to other users.

The School may also ask for information about particular health needs, such as allergies to particular forms of medication, or any medical condition such as asthma or diabetes. The School will only use this information in the protection of the health and safety of the individual, but will need consent to process this data in the event of a medical emergency, for example.

Processing Sensitive Information

Sometimes it is necessary to process information about a person’s health, criminal convictions, or race. This may be to ensure that the School is a safe place for everyone, or to operate other School policies, such as the Equality Policy.

All sensitive information will be labelled, where practicable to keep it secure and to destroy it when it is no longer needed. This is especially important if sensitive information is combined into a report and printed.

The IAO will inform staff of the correct level of labelling for documents viewed by staff. There are different levels of labelling depending on just how sensitive the information is.

Further information can be found at ‘SIRO IAO Guidance for Schools on Data Security.doc’ available on the SITSS website. (The SIRO and IAO(s) should be aware of this document.) http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata

Because this information is considered sensitive under the 1998 Act, staff (and students or parents where appropriate) will be asked to give their express consent for the School to process this data. An offer of employment may be withdrawn if an individual refuses to consent to this without good reason.

Publication of School Information

Certain items of information relating to School staff will be made available via searchable directories on the public Web site, in order to meet the legitimate needs of researchers, visitors and enquirers seeking to make contact with the school.

School Retention of Data

The School has a duty to retain some staff and student personal data for a period of time following their departure from the School, mainly for legal reasons, but also for other purposes such as being able to provide references or academic transcripts. Different categories of data will be retained for different periods of time.

Conclusion

Compliance with the 1998 Act is the responsibility of all members of the School. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or even to a criminal prosecution.

Review

This policy will be reviewed every 3 years, or more frequently should regulations change

Data Protection Best Practice

- **Identify a SIRO and IAO(s) within our school.**
- **Staff Aware and follow of Esafety Policy including Acceptable Use of it Policy and ensure staff follow it.**
- **IT Equipment kept up to date with latest security updates**
- **IT Company are aware of this policy and importance of Data Security for the school**
- **The ICT subject leader, IT Services Provider and HGfL will monitor and record (log) the websites staff visit**
- **Only approved software installed on machines and files downloaded from trusted sources**
- **Avoid clicking on spam email links at school**
- **Only authorised staff are allowed to remove data from the school's premises**
- **Confidential electronic data is not removed from the school's premises without encryption**
- **Paper copies of personal data are correctly labelled**
- **Hard copies of sensitive data are securely stored and then disposed of when no longer required**
- **Zombie accounts (of leavers) are removed**

Third Party Relationships

When our school contracts a third party to provide a service on the schools behalf then we are covered under our Data Protection registration to supply the data to the contracted organisation. We shall ensure the method used to provide them with the data is secure and meets UK DP standards.

Full guidance can be found - Managing Information Risk, [http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf

Tips for Staff:

- **Staff should follow the school's password policy and do not disclose to unauthorised parties**
- **Shut down laptop or workstation using the 'Shut Down' or 'Turn Off' option**
- **Try to prevent people from watching the entering of passwords or view sensitive information**
- **Turn off and store all laptops and Ipads securely**
- **Secure the laptop via a password protected screensaver when you leave a computer.**
- **Don't leave your laptop unattended unless you trust the physical security in place**
- **Don't use public wireless hotspots as they are not secure**
- **Don't let unauthorised people use your laptop**
- **Be aware of who you are allowed to share information with.**
- **Ask third parties how they will protect sensitive information once it has been passed to them.**
- **Don't send sensitive information (even if encrypted) on removable media (USB memory drives, CDs, portable drives) if secure remote access is available**
- **Send sensitive information by email unless there is no alternative**
- **Don't let strangers or unauthorised people into staff areas**
- **Do position screens where they can be read from outside the room**
- **Only take information offsite as necessary and ensure that it is protected offsite**
- **Ensure that all staff are compliant with the guidelines referring to server security and data protection as recommended in the Network Manager's Guidance document http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata**
- **Ensure staff have read the email protocols and guidance on the grid http://www.intra.thegrid.org.uk/eservices/email/protocols/index.shtml**
- **Ensure staff have read or are aware of our school's policy on dealing with emails from all sources**
- **Ensure staff only use school email accounts, not personal ones such as Yahoo or Hotmail for work related items**
- **Ensure that staff with access to personal data on children or vulnerable adults have enhanced CRB clearance**
- **Put in place a policy for reporting, managing and recovering from information risk incidents.**
- **Make learners (and parents where applicable) aware of what data is being held about them and what it is being used for by issuing Privacy Notices**
- **Shred, pulp or incinerate paper containing personal data when no longer required.**