Data Protection Policy

Issue 1
September 2014

PURPOSE

To ensure that at Swaffham Campus personal information about individuals is handled correctly and in line with the Data Protection Act and the Information Commissioner's Office guidance.

SCOPE

This policy applies to all Trustees, Staff and Volunteers working at the school.

DEFINITIONS

ICO – Information Commissioners Office
DP – Data Protection
DPA – Data Protection Act

POLICY STATEMENT

Focus School Swaffham Campus aims to fulfil its obligations under the Data Protection Act (DPA) 1998 to the fullest extent.

This Policy and Procedure sets out our commitment to protecting personal data and how that commitment is implemented in respect of the collection and use of personal data.

When required reference to the ICO website will be made.

The ICO Newsletter will be sent to the CEO on a regular basis from Focus Regional Support Office.

PROCEDURES

Roles & Responsibilities

The Trust as the Employee has a duty to:

- Provide accurate personal information and ensure that is is kept up to date
- Follow procedures for preventing unauthorised access to, unauthorised use of, loss of or destruction of personal data
- Respect confidentiality of any sensitive information of which they are made aware
- Appoint a Trustee with responsibility for DP 'Data Controller' who has legal responsibility for processing personal data. These responsibilities cannot be delegated, but an employee such as the Senior Teacher School Administrator should have some devolved responsibility with regard to familiarity with the DP Policy and procedures on a day to day basis.

The Trustee responsible for registering with the ICO is: Gordon Fentiman

The employee with an overview of DP on a day to day basis is: Anne Lloyd

Duties include:

- Ensuring that the ICO registration / notification is renewed each year for the school and its associated Trusts
- Renewing the registration due on: 6th February 2015
- Ensuring that the school complies with all requirements of the eight principles of the DPA
- Making sure that the ICO is notified accurately of the purpose for the processing of personal data
- Recognising the need to handle personal information in line with the data protection principles
- Advising students, parents and staff what the school does with personal information recorded about them. Ensuring that the personal information is restricted to those who need it
- Keeping confidential information secure when storing it, using it and sharing it with others
- Ensuring that when disposing of records and items of equipment, personal information cannot be retrieved from them
- Monitoring the policy and procedure for DP in school including ensuring that particular information can be shared with others and is kept secure when shared
- Keeping a log and monitor when individuals request details of their personal data
- Controlling access to any restricted area of the school website, and checking before publishing any personal information (including images) on it
- If appropriate, following the ICO guidance on CCTV
- Ensuring that all staff and trustees are made aware of the basic importance of information governance, the law and good practice of DP.

At Swaffham Campus, the data protection legislation applies equally to students, parents and staff.

The eight principles set out in the DPA are followed in all cases:

1. Data must be processed fairly and lawfully
2. Data must only be obtained for specified and lawful purposes
3. Data must be adequate, relevant and not excessive
4. Data must be accurate and up to date
5. Data must not be kept for longer than necessary
6. Data must be processed in accordance with the “data subject’s” (the individual’s) rights
7. Data must be securely kept
8. Data must not be transferred to any other country without adequate protection in place.

The following procedures apply to information held about students:

- A student’s educational records will be disclosed to their parent or carer, and to the pupil in question, on submission of a written request. Requests will only be refused if it is obvious the requester does not understand what they are asking for, or if disclosure is likely to cause them or anyone else serious physical or mental harm.
- A student’s educational records will be made available without charge within 15 school days of receipt of the written request.
- When a student moves to a new school, a completed Common Transfer File together

with all educational records relating to the student will be sent to the new school. This includes copies of reports and any personal education plans, safeguarding information. To ensure security, this data will be sent electronically within 15 days of the student ceasing to be registered at the school, where possible. If the new school is not known, every effort will be made to contact the parents or carers by post, telephone or email.

The following procedures apply to information held about staff.

- A copy of their personal data is sent to each member of staff on one occasion (date tbc) each year. This applies to all data, whether held on computer or as hard copy.
- Members of staff are required to read this information carefully and inform the CEO at the earliest opportunity if they believe that anything is inaccurate or untrue, or if they are dissatisfied with the information in any way.
- Requests for additional access must be sent to the CEO. Each request will be judged in light of the nature of the information in question and the frequency with which it is updated. The member of staff will then be informed whether or not the request is granted. In the event of a disagreement, the matter will be taken up under the formal grievance procedure.
- If a request for additional access is granted, the information will be provided within 40 days of the date of the request.

CONTEXTUAL INFORMATION about Swaffham Campus relevant to the Data Protection Policy and its implementation in the Campus.

Personal data stored on students SIMS files is checked for accuracy by the parents once a year, by the signing of a Data Collection Sheet. A similar summary is used for staff to check their personal details on SIMS. Staff can request access to their (hard copy) personnel file via the HR trustee at any time.

ASSOCIATED DOCUMENTS

Appendix 1 – Detailed information on DP including ICO website links

Associated Focus Policies:

- Recruitment Policy
- ICT Policy
- Using Images Policy including Mobile Phones and electronic devices
- Safeguarding Policy
- Focus Enrolment Application Form
- Staff Handbook
- Admissions and Attendance Policies

LEGISLATION

List of Legislation:

- Data Protection Act 1998 & Data Protection Directives 95/96/EC
- Protection of Freedom Act 2012
- Freedom of Information Act 2000
- Telecommunications Regulations 2000
- Regulation of Investigatory Powers Act 2000
- Human Rights Act 1998
- Public Interest Disclosure Act 1998
- Employment Rights Act 1996
- Access to Medical Records Act 1988

ISSUED BY

Focus Learning Trust

Issue date: September 2014 Review date: September 2015

Version: 1

Signed by Chair of Board of Trustees: ._____

At a Trust Meeting on (date): 21/11/14_____

Appendix 1

ICO website:
www.ico.gov.uk

Data Protection 8 Principles ICO Link:
http://ico.org.uk/for_organisations/data_protection/the_guide/the_principles
You can then click on each link to obtain further information about each principle.

Topic Guides providing additional information on the ICO website links:
http://ico.org.uk/for_organisations/data_protection/topic_guides
Include: Anonymisation, CCTV, Data Sharing, Employment, Online and Computing
Privacy notices

CCTV Code of Practice:
http://ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Detailed_specialist_guides/ICO_CCTVFINAL_2301.pdf

Privacy Notices, Code of Practice:
http://ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Detailed_specialist_guides/PRIVACY_NOTICES_COP_FINAL.ashx

Education Links:
http://ico.org.uk/for_organisations/sector_guides/education
Include: Information held on students, meeting data protection obligations, employment, examination, taking photos in school,

Taking Photographs in School – Data Protection Good Practice Note:
http://ico.org.uk/for_organisations/sector_guides/~/media/documents/library/Data_Protection/Practical_application/TAKING_PHOTOS_V3.ashx

ICO Index Guide to Data Protection, privacy and electronic communication:
http://ico.org.uk/for_organisations/guidance_index/data_protection_and_privacy_and_electronic_communications#online

On-line and Computing including Bring your own device guidance, IT Asset Disposal.

In Detail :

- **Eight Principles**
- **Sensitive Data**
- **Personal Data**
- **Notification / Registration with ICO**
- **Educational Records and Reports**
- **Requests to Access Personal Data**
- **Retention of Records**
- **Employment**
- **Health and Safety Records**
- **Freedom of Information**
- **Data Loss and Portable Storage**
- **Penalties**

Eight Principles
Processing will be fair and lawful for the purposes of the first principle when one of the following conditions has been satisfied,:

- The individual has given consent.
- It is necessary for the performance of the contract with the individual, eg to make payments.
- There is a legal obligation on the employer, eg to comply with PAYE reporting or the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995.
- It is necessary to protect the vital interests of the individual.
- It is necessary to carry out public functions.
- It is necessary to pursue the legitimate interests of the data controller.
- It is necessary for the administration of justice.
- It is necessary for the exercise of any functions conferred by or under any enactment.

It is possible to infer consent from the circumstances in which the data is given, unless the data is “sensitive”, in which case explicit consent will be required.

To ensure fair processing:

- Data can only be provided by a person who is authorised or required by law to do so
- Personal data must not be obtained in a way that deceives or misleads the data subject as to it’s purpose
- The data controller must ensure, as far as practicable, that the data subject receives information about the intended use of any data and the consequence of its processing.

Sensitive Data can only be processed in certain circumstances, including where:

- the subject has given explicit consent
- it is necessary in order to comply with legal requirements
- it is necessary to protect the vital interest of an individual or another person
- the data has already been made public by the subject
- it is necessary for medical purposes and is carried out by someone with a duty of confidentiality
- it is necessary for equal opportunity monitoring and the data relates to racial or ethnic origin.

Schools and other educational bodies, such as Ofsted, should appoint a named data protection officer to decide how data is processed and to ensure that the processing complies with the law.

Personal Data

Personal data is any information in any media that relates to a living person who is or who has been involved in an organisation. Examples include:

- personnel records, including payroll records, whether stored under name or personnel number, CCTV which records the image of a person's face; a complaint where the person complained about is not specifically identified, but can be identified because of the circumstances; school admission and attendance registers; pupils' curricular and disciplinary records; children's learning and development records; family and home contact details; assessment data under the National Curriculum assessment arrangements; reports to parents on the achievements of their children; records in connection with pupils entered for prescribed public examinations; personal information for teaching purposes; records of contractors and suppliers.

Sensitive Personal Data

Sensitive personal data relates to:

- Ethnic or racial origin, political opinions, religious or other similar beliefs, trade union membership, physical or mental health, sexual life, the (alleged) commission of any offence and any related proceedings or sentence.

Notification / Registration with ICO

Notification is the process of registering with the Information Commissioner's Office (ICO). Unless they are exempt, every data controller that processes personal data must notify the ICO as to the nature and extent of the data being processed. Notification must be renewed annually and failure to notify is a criminal offence.

The current registration fee for a small organisation, ie one that has a turnover less than £25.9 million and no more than 250 staff, is £35.
Where a school holds personal data on a computer or some type of electronic retrieval system, or has CCTV, it will probably need to register.
Registration must be under the correct legal title of the individual or organisation.
Records held on a manual (paper-based) system are exempt from registration but must still adhere to the data protection principles.

Educational Records

All parents and carers are entitled to have their child's record disclosed to them on written request. Pupils can also request their own records. Requests can be refused if the disclosure is likely to result in physical or mental harm to someone.

When a pupil ceases to be registered at one school in England or Wales, and becomes registered at another, all maintained secondary, primary and nursery schools are required to send a Common Transfer File to the new school.

Requests to Access Personal Data

All workers, ex-workers and job applicants have the right to request access to any specified personal data held about them including details of:

- sickness, discipline, training, appraisals, emails, word-processed documents, email logs, audit trails, information on personnel files, interview notes.

Employees have the right to obtain access to personal data except where the information is:

- for management forecasting including succession planning or redundancy, about intentions in negotiations or bargaining, given in confidence in a reference, held for the prevention or detection of crime or for assessment or collection of tax, relating to any other individual.

Employers may charge up to £10 each time for access, and must respond within 40 calendar days of receiving the request.

Responding to employee requests for data should involve:

- checking who is seeking the information as the data can only be disclosed to the data subject and no-one else, telling the worker or job applicant what personal information is kept about him or her and for how long, describing the information, how it is used and whom it may be passed to, providing a copy of the information in an appropriate form, disclosing the information source, checking to ensure that the information doesn't identify or relate to another individual as well.

Retention of Records
The length of time for which records should be kept varies according to the type of data involved.

Educational records and reports
Under the Freedom of Information Act 2000, maintained schools and academies are required to maintain a schedule that lists:

- the records that are created in the school, how long they are to be retained, the action that should be taken when they are no longer of any administrative use.

We recommend that Focus Schools maintain a schedule as above as the procedure has a number of advantages:

- Information will be available when required as a result of a freedom of information request; staff cannot be accused of unauthorised tampering with files; information is not stored unnecessarily; sensitive material will be shredded at the appropriate time.

The retention time varies according to the record in question. For instance:

- child protection records should be retained until the child's 25th birthday, annual financial accounts should be kept for six years, pupils' personal files follow them as they progress through the school system and should normally be retained until the pupil's 25th birthday before secure disposal, attendance registers should be kept for three years before secure disposal, (see Focus Attendance Policy for further guidance); permission slips for school trips should be disposed of immediately after the visit, provided that it was completed without incident.

Employment
Although there is no statutory minimum or maximum time period for which to keep personnel and training records, it is recommended that they be kept for at least six years after termination of employment.

Records, such as those relating to recruitment, discipline and grievance or other documentation relating to an individual's performance, capability or conduct may be needed as evidence to be able to defend an employment tribunal claim. It is therefore recommended that these documents are not destroyed until at least six months after the time limit for the employment tribunal claim. This is because, although the time limit for the majority of employment tribunal claims is three months (eg an unfair dismissal claim), for some claims it can be extended to six months.

Payroll information must be kept as follows:

Type of payroll information	Length of time the information has to be kept
Tax and National Insurance returns	7 years
Payroll and wages records	6 years
Records of payments for statutory sick, maternity, paternity and adoption pay	3 years

HM Revenue and Customs will normally only go back six years in checking records unless fraud is suspected, in which case their limitation is 20 years.

Health and Safety Records
Records relating to any potential personal injury claims will need to be kept for a minimum of three years from the date it becomes apparent that the injury or damage was caused by a work-related incident.

However, in the case of industrial diseases such as mesothelioma, these may not develop until well after the employee has left. In any event, Employer Liability Insurance certificates should be kept for 40 years.

In addition, Health and Safety legislation requires accident books to be kept for a minimum of three years, and for 12 years in the case of an industrial accident.

In addition to abiding by the statutory minima for record keeping, employers should:

- establish policies for the retention of different types of information based on business needs, including who can access the information, make information anonymous wherever possible, delete any information about "spent" convictions at the appropriate time, regularly review any stored information to ensure that it is up-to-date, accurate and not excessive, dispose of information securely and effectively.

Freedom of Information
The Freedom of Information Act 2000 gives individuals the statutory right to access certain information held by public authorities. This includes maintained schools and academies, but not independent schools or the majority of early year provisions. Requests must be dealt with promptly, and within 20 school days or 60 working days if this is shorter.

The information should be sent by whatever means is most reasonable, although any preferred means of communication specified by the requestor should be complied with where possible.

Data Loss and Portable Storage
Also refer to the Focus ICT Policy. The use of portable devices such as laptops, mobile phones, USB sticks and portable hard drives to record data should be guided by clear protocols.

These devices must also be carefully protected.

- Train staff to be vigilant, aware of the dangers of data loss, and wary of any unexpected data requests
- Ensure that all systems, including remote e-mail access and mobile phones, have an adequate level of password or PIN protection
- Encrypt the data, so that it cannot be understood by anyone who doesn't have the right combination of decoding information and tools
- Question and review every use of a portable device to hold personal data. If the data no longer needs to be on such a device, erase it, the data should be properly and effectively erased from the device
- Educate staff about new and existing methods used to steal data
- Use computer security technology to block security attacks and hackers, where necessary obtaining specialist consultancy advice. Some malware programmes are designed to find and remove personal data from unprotected systems
- Train staff in the principles of data protection and information governance and ensure they are taking all the necessary precautions. They should be able to identify personal data and understand physical, technical and procedural security policies. They should be especially careful with e-mail and any attachments which contain executable files, or from unknown or unexpected sources

- Implement physical security systems to prevent the theft of portable devices, by preventing casual access to rooms where they are kept and always locking them away. Where possible, Kensington security slots should be used with laptops
- Train staff to avoid leaving devices unattended, to log- out or password protect data if they are momentarily absent, and to ensure that devices lock themselves after a short period of inactivity. Where workers regularly need to use devices on public transport, data security needs to be even higher in case of accidental loss
- Never dispose of old computer equipment or storage devices without checking that all personal data has been thoroughly and permanently removed. Physical destruction of the hard drive is the safest method, as data can still be recovered from the image left on a reformatted hard drive
- Ensure that the organisation has solid disaster recovery or critical system continuity procedures to ensure that any data loss is kept to an absolute minimum
- Encourage staff to report any security breaches immediately, even near-misses and conduct regular security audits of computer and data security. Respond to any security incidents or concerns and seek professional help if required. The Information Commissioner's Office often has greater sympathy where an organisation has self-reported a breach.

Penalties
Failure to process personal data in a fair and proper way can lead to a criminal offence or a claim for compensation.

The Information Commissioner's Office has powers to fine organisations up to £500,000 for serious breaches of the Data Protection Act 1998 (DPA). The Commissioner may instead issue an enforcement notice requiring systems or policies to be introduced or changed to comply with the DPA.

The Commissioner may impose a substantial monetary penalty notice for a contravention which is serious and is likely to cause "substantial damage or distress". In addition, either the contravention must be deliberate or the organisation must know, or ought to know, that there is a risk of breach which it has failed to take reasonable steps to prevent.

When considering the seriousness of the breach, the Commissioner will look at the policies and procedures in place to prevent any such breach, the general nature and attitude to data protection within the organisation, and whether a similar breach has occurred previously. Where the organisation has self-reported the breach and is already investigating and implementing appropriate remedial action and procedures, the Commissioner will usually exercise a degree of leniency.

When deciding on the size of a fine, the Commissioner will take into account the type and size of organisation as well as its financial and other resources.