THE FOUNTAINS HIGH SCHOOL

SOUTH DERBYSHIRE SUPPORT CENTRE

DATA HANDLING POLICY

Policy Author – Gareth Allen –Headteacher

Review date: 01 December 2022
Created: January 2021
Ratified: 02 December 2021

part of the esteem Multi-Academy Trust

emat

Stronger Together...

BACKGROUND

Publicity about data breaches suffered by organisations and individuals has made the area of personal data protection compliance a current and high-profile issue for schools and other organisations. It is important that the Fountains High School (FHS) and South Derbyshire Support Centre (SDSC) have a clear and well understood personal data handling policy in order to avoid or at least minimise the risk of personal data breaches. A breach may arise from a theft, a deliberate attack on our systems, the unauthorised use of personal data by a member of staff, accidental loss, or equipment failure. In addition:

- The FHS and SDSC or individual would not want to be the cause of any data breach, particularly as the impact of data loss on individuals can be severe and cause extreme embarrassment, put individuals at risk and affect personal, professional or organisational reputation.
- The FHS and SDSC is "data rich" and the introduction of electronic storage and transmission of data has created additional potential for the loss of data
- The FHS and SDSC want to avoid the criticism and negative publicity that could be generated by any personal data breach.
- The FHS and SDSC is subject to a wide range of legislation related to data protection and data use, with significant penalties for failure to observe the relevant legislation.

It is a statutory requirement for all schools to have a Data Protection Policy.

The FHS and SDSC have always held personal data on the pupils in their care, and increasingly this data is held digitally and accessible not just in school but also from remote locations. Legislation covering the safe handling of this data is mainly the Data Protection Act 1998 ('the DPA'). Moreover, following a number of losses of sensitive data, a report was published by the Cabinet Office in June 2008, Data Handling Procedures in Government. The latter 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 schools, it is critical that they adopt these procedures too.

This Personal Data Handling Policy applies to all forms of personal data, regardless of whether it is held on paper or in electronic format. However, as it is part of an overall online safety policy, this document will place particular emphasis on data which is held or transferred digitally.

INTRODUCTION

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, and/or
- need to have access to that data.

Data breaches can have serious effects on individuals and The FHS and SDSC and can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office. for The FHS and SDSC and the individuals involved.

Particularly, 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 protection legislation and relevant regulations and guidance.

The DPA 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 correction. The DPA requires organisations to comply with eight data protection principles, which, among others require data controllers to be open about how the personal data they collect is used.

The DPA defines “Personal Data” as data which relate to a living individual who can be identified

- from those data, or
- from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

(http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions)

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Continued…

INTRODUCTION *Continued…* & POLICY STATEMENTS

It further defines "Sensitive Personal Data" as personal data consisting of information as to:

- the racial or ethnic origin of the data subject
- their political opinions
- their religious beliefs or other beliefs of a similar nature
- whether they are a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
- their physical or mental health or condition
- their sexual life
- the commission or alleged commission by them of any offence, or
- any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings

Guidance for organisations processing personal data is available on the Information Commissioner's Office website:
http://www.ico.gov.uk/for_organisations/data_protection_guide.aspx

Policy Statements

FHS and SDSC will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing". (see Privacy Notice section below)

RESPONSIBILITIES & REGISTRATION

The school's Data Protection Officer is ICT Technician. This person will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's information risk policy and risk assessment
- appoint the Information Asset Owners (IAOs)

All teachers and wider staff who handle pupil data are Information Asset Owners (IAOs), who handle a range of pupil and staff information. The IAOs will manage and address risks to the information and will understand:

- what information is held, for how long and for what purpose,
- how information has been amended or added to over time, and
- 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

Both Schools (FHS and SDSC are registered as a Data Controllers on the Data Protection Register held by the Information Commissioner).

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
- Risk Assessments

Information risk assessments will be carried out by 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) and
- Prioritising the risks.

Risk assessments are an ongoing process and should result in the completion of an Information Risk Actions Form (example below):

Risk ID	Information Asset affected	Information Asset Owner	Protective Marking (Impact Level)	Likelihood	Overall risk level (low, medium, high)	Action(s) to minimise risk

IMPACT LEVELS AND PROTECTIVE MARKING

Following incidents involving loss of data, the Government recommends that the Protective Marking Scheme should be used to indicate the sensitivity of data. The Protective Marking Scheme is mapped to Impact Levels as follows:

Government Protective Marking Scheme label	Impact Level (IL)	Applies to schools?
Not Protectively Marked	0	Will apply in schools
Protect	1 or 2	
Restricted	3	
Confidential	4	Will not apply in schools
Highly Confidential	5	
Top Secret	6	

Most student or staff personal data that is used within educational institutions will come under the PROTECT classification. FHS and SDSC will ensure that all school staff, independent contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher. Unmarked material is considered 'unclassified'. The term 'UNCLASSIFIED' or 'NON' or 'NOT PROTECTIVELY MARKED' may be used to indicate positively that a protective marking is not needed.

All documents (manual or digital) that contain protected or restricted data will be labelled clearly with the Impact Level shown in the header and the Release and Destruction classification in the footer.

Users must be aware that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data. Combining more and more individual data elements together in a report or data view increases the impact of a breach. A breach that puts pupils at serious risk of harm will have a higher impact than a risk that puts them at low risk of harm. Long-term significant damage to anyone's reputation has a higher impact than damage that might cause short-term embarrassment.

Release and destruction markings should be shown in the footer e.g. "Securely delete or shred this information when you have finished using it".

SECURE STORAGE OF AND ACCESS TO DATA

FHS and SDSC will ensure that 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 use strong passwords which must be changed regularly (see Online Safety Policy) User 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) 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 school equipment (this includes computers and portable storage media (where allowed). 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,
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected),
- the device must offer approved virus and malware checking software (memory sticks will not provide this facility, most mobile devices will not offer malware protection), and
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

FHS and SDSC do not allow storage of personal data on removable devices that are not encrypted/ password protected.

FHS and SDSC has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups. (see Online Safety Policy)

The FHS and SDSC has clear policy and procedures for the use of “Cloud Based Storage Systems” (for example dropbox, Microsoft 365, google apps and google docs) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote / cloud-based data services providers to protect the data.

SECURE STORAGE OF AND ACCESS TO DATA *Continued…*

See appendix for further information and the ICO Guidance: http://www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/cloud_computing_guidance_for_organisations.ashx

As a Data Controller, The FHS and SDSC is responsible for the security of any data passed to a "third party". Data Protection clauses will be included in all contracts where data is likely to be passed to a third party.

All paper based Protected and Restricted (or higher) material must be held in lockable storage, whether on or off site.

The FHS and SDSC recognises that under Section 7 of the DPA, http://www.legislation.gov.uk/ukpga/1998/29/section/7 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 (where necessary) 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 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 FHS and SDSC 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 restricted or protected 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 which contain personal data must not be accessed by other users (e.g. family members) when out of school
- When restricted or protected 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 have secure remote access to the management information system and internal school drives.
- 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; and
- 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 (if relevant) in this event.

Disposal of data

The FHS and SDSC will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of personal 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 (see earlier section for reference to the Cabinet Office guidance), and other media must be shredded, incinerated or otherwise disintegrated for data.

AUDIT LOGGING / REPORTING / INCIDENT HANDLING

It is good practice, as recommended in the "Data Handling Procedures in Government" document that the activities of data users, in respect of electronically held personal data, will be logged and these logs will be monitored by responsible individuals who currently access Policy Central Data.

The audit logs will be kept to provide evidence of accidental or deliberate data security breaches – including loss of protected data or breaches of an acceptable use policy, for example.

The school has a policy for reporting, managing and recovering from information risk incidents, which establishes: (see Online Safety Policy)

- 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 of 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.

USE OF TECHNOLOGIES AND PROTECTIVE MARKING

The following provides a useful guide of the procedures in place at The FHS and SDSC:

	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 publicly accessible technology such as school websites or portal, emailed newsletters, subscription	School terms, holidays, training days, the curriculum, extra-curricular activities, events, displays of pupils' work, lunchtime menus, extended services, parent consultation events
Learning and achievement	Individual pupil academic, social and behavioural achievements, progress with learning, learning behaviour, how parents can support their child's learning, assessments, attainment, attendance, individual and personalised curriculum and educational needs.	Typically, schools will make information available by parents logging on to a system that provides them with appropriately secure access, such as a Learning Platform or portal, or by communication to a personal device or email account belonging to the parent.	Most of this information will fall into the PROTECT (Impact Level 2) category. There may be students/ pupils whose personal data requires a RESTRICTED marking (Impact Level 3) or higher. For example, the home address of a child at risk. In this case, the school may decide not to make this pupil / student record available in this way.
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.	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.

LEAVING THE EUROPEAN UNION & APPENDICES

As the UK transitional arrangements expired on 31 December 2020, there are some practical changes for Data Protection and the GDPR.

To comply with the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 please note that every policy, notice and procedural guide that refers to 'GDPR' shall now be read as 'UK GDPR'.

The rights, responsibilities and data protection that the Data Protection Act 2018 and the GDPR are not changed. Our procedures and arrangements will not change.

If you have any queries please contact Kath Linstead.

Appendices: Additional issues / documents related to Personal Data Handling in Schools:

Use of Cloud Services

The FHS and SDSC use cloud hosted services for email (Microsoft 365) and are exploring the wider options such as Google Apps for Education services:

http://www.google.com/apps/intl/en/terms/education_terms.html FHS and SDSC is ultimately responsible for the contract with the provider of the system.

The document found on the following link: http://www.swgfl.org.uk/products-services/education/Resources/Cloud-Hosted-Services focusses on Google Apps for Education and Microsoft 365 and states how they access and store data.

Parental permission for use of cloud hosted services

When the FHS and SDSC start using cloud hosting services (eg. Google Aps for Education) with pupils, parental permission will be sought through a specific 'Use of cloud systems permission form'.

Privacy and Electronic Communications

The FHS and SDSC is aware that we are subject to the Privacy and Electronic Communications Regulations in the operation of our websites.

Freedom of Information Act

The FHS and SDSC has a Freedom of Information Policy which sets out how we deal with FOI requests.