ST ANNE'S FULSHAW

Over 125 years of achievement

Data Handling Policy

St Anne’s Fulshaw CE Primary School Data Handling Policy

Introduction

1. The Data Protection Act

The Data Protection Act controls how your personal information is used by organisations, businesses or the government.

Everyone responsible for using data has to follow strict rules called ‘data protection principles’. They must make sure the information is:

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive
- accurate
- kept for no longer than is absolutely necessary
- handled according to people’s data protection rights
- kept safe and secure
- not transferred outside the European Economic Area without adequate protection

There is stronger legal protection for more sensitive information, such as:

- ethnic background
- political opinions
- religious beliefs
- health
- sexual health
- criminal records

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 can not 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.

NB - 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.

The Data Protection Act (1998) 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 security and requires users of data (data processors) to be open about how it is used and to follow “good information handling principles”.

Policy Statements

St Anne’s Fulshaw CE Primary 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 an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including children, members of staff and parents and carers eg names, addresses, contact details, legal guardianship / contact details, health records, disciplinary records
- Curricular / academic data eg class lists, children’s 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 the Headteacher.
She will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school’s data protection policy and procedures
- appoint the Information Asset Owners (IAOs)
- ensure all staff have initial data protection training

St Anne’s Fulshaw CE Primary School has identified Information Asset Owners (IAOs) for the various types of data being held:

- IAO for student and staff information is the school’s admin officer
- IAO for assessment data, children’s progress and any other information relating to children’s learning and behaviour is the headteacher
- IAO for data relating to children with additional needs is the school’s SENCO

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 children of the data they hold on the children, the purposes for which the data is held and the third parties (eg LA, DFE etc) to whom it may be passed. This fair processing notice will be passed to parents / carers when their children first join the school as part of the initial welcome literature.

A copy of the fair processing notice can be obtained on request from the school's admin officer.

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, who will be issued with appropriate guidelines (see Appendix 2)
- Staff meetings / briefings / Inset
- Day to day support and guidance from Information Asset Owners

Impact Levels and protective marking

The school uses the Government Protective Marking Scheme and has grouped data according to its subject. The Information Risks Action Form shows the main data held by school, its impact level and actions to minimise risk.

Government Protective Marking Scheme label	Impact Level (IL)
NOT PROTECTIVELY MARKED	0
PROTECT	1 or 2
RESTRICTED	3
CONFIDENTIAL	4
HIGHLY CONFIDENTIAL	5
TOP SECRET	6

Use of technologies and Protective Marking

The following (from Becta) provides a useful guide:

	The information	The technology	Notes on Protect Markings (Impact Level)
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 publically accessible technology such as school websites or portal, emailed newsletters, subscription text services	Most of this information will fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.
Learning and achievement	Individual learner's 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 learners 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 learners 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. Where parents are frequently accessing information online then systems e.g. Learning Platforms or portals, might be used to alert parents to issues via “dashboards” of information, or be used to provide further detail and context.	Most of this information will fall into the PROTECT (Impact Level 1) category. However, since it is not practical to encrypt email or text messages to parents, schools should not send detailed personally identifiable information. General, anonymous alerts about schools closures or transport arrangements would fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.

Risk Assessments
Information risk assessments will be carried out by Information Asset Owners (see example in appendix 1) 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

	Very unlikely	Unlikely	Possible	Likely	Frequent
PROTECT (Impact Level 1)	Low	Low	Low	Medium	Medium
PROTECT (Impact Level 2)	Low	Low	Medium	Medium	Medium
RESTRICTED (Impact Level 3)	Low	Medium	Medium	Medium	High

St Anne’s Fulshaw CE Community Primary School - Information Risk Actions Form - See Appendix 1

All documents relating to children and adults are impact level 2. Where the information is about vulnerable adults or children then impact level 3 is applied.

Occasionally, when data is aggregated or the situation changes, the subsequent impact level may be higher than the individual impact levels of the original data. This decision will be made by the ISA and/or head teacher and communicated to the relevant parties

In exceptional circumstances (impact level 4 and above), release and destruction markings should be shown in the footer eg. “Securely delete or shred this information when you have finished using it”.

Passwords
All adult users will be given secure user names and strong passwords which must be changed regularly. Passwords should be changed at the start of every year. Passwords must be a minimum of 8 characters long and must contain a mixture of letters, numbers and characters. User names and passwords must never be shared.

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.

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). 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 device must be encrypted and password protected
- the device must be checked for viruses
- 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

The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups. This is contained in the Manual of Internal Procedures.

All paper based Restricted (or higher) 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, an oral request to see part of the personal data and a written request to see all 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 removable devices which contain personal data must not be accessed by other users (eg family members) when out of school.
- Users must not transfer personal data from the encrypted and password protected device to home machines
- 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 use the 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
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.
- No data should be taken if data is to be taken or transferred to another country. Should exceptional circumstances arise where there is a need to do so, request must be granted from the Headteacher who may need approval from the Local Authority.

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 for data.

Reporting / Incident Handling
Breeches of security or inappropriate use of data by data users, in respect of electronically held personal information, will be logged and these logs will be monitored by the Headteacher, Deputy Headteacher and Admin Officer.

In response to an incident of mishandling data, the school must 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 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.

Appendix 1

Information Risk Assessment Form – St Anne's Fulshaw CE Primary School

Risk ID	Information Asset affected	Information Asset Owner	Protective Marking (Impact Level)	Likelihood	Overall risk level (low, medium, high)	Action(s) to minimise risk
	All personal information for staff and children	CD PT WC	2	Possible	Medium	Only necessary data to be take off site All data to be accessed remotely where possible All data backed up Back up data to be stored encrypted in the cloud
	All personal information relating to vulnerable children and adults	CD PT WC	3	Possible	Medium	Only available to identified people relevant to individual No data to be taken off site unless permission given by headteacher

Appendix 2

Guidelines for all data controllers

Your roles and responsibilities

As a member of St Anne’s Fulshaw CE Primary School, you have a shared responsibility to secure any sensitive or personal data you use in your day-to-day professional duties.

1.1 - Important ‘dos’

- make sure you and your colleagues are adequately trained
- follow guidance
- become more security aware
- raise any security concerns
- encourage your colleagues to follow good practice and guidance
- report incidents.

1.2 - Why protect information?

Organisations hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this data could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of personal data could result in adverse media coverage, and potentially damage the reputation of the school. This can make it more difficult for the school to use technology to benefit learners.

1.3 - What information do you need to protect?

You should secure any personal data you hold about individuals and any data that is deemed sensitive or valuable to our school. The school’s Headteacher, Deputy Headteacher and Admin Officer are responsible for working out exactly what information needs to be secured. These people are your Information Asset Owners. They understand what information you need to handle, how the information changes over time, who else is able to use it and why.

1.4 - Information impact levels

All information relating to children and adults in school has been graded as level 2 (unless the child/adult has been deemed vulnerable then level 3 will apply) It is the responsibility of all data users to ensure they have read, understood and take the necessary risk reduction steps as outlined in this policy.

1.5 - Steps you can take to help prevent security problems

There are plenty of things that you should do (or not do) that will greatly reduce the risks of sensitive information going missing or being obtained illegally. Many of these ‘dos and don’ts’ will apply to how you handle your own personal information. Using these practices will help you to protect your own privacy.

We have separated these points into different areas to make it easier for you to refer back to.

1.6 - Working online

Do...

- make sure that you follow your organisation’s policies on keeping your computers up to date with the latest security updates. Make sure that you keep any computers that you own up to date. Computers need regular updates to their operating systems, web browsers and security software (anti-virus and anti-spyware). Get advice from your IT technician if you need help.

- only visit websites that are allowed by Cheshire East LA while in school or using school equipment. Remember St Anne's Fulshaw CE Primary School may monitor and record (log) the websites you visit.
- turn on relevant security warnings in your web browser (for example, the automatic phishing filter available in Internet Explorer)
- be wary of links to websites in emails, especially if the email is unsolicited
- only download files or programs from sources you trust. If in doubt, talk to your IT technician.
- ensure you follow the Acceptable Use Policy.

1.7 - Email and messaging

1.7.1 - Do...

- report any spam or phishing emails to your Headteacher/ Deputy Headteacher that are not blocked or filtered
- report phishing emails to the organisation they are supposedly from

1.7.2 - Don't

- click on links in unsolicited emails. Be especially wary of emails requesting or asking you to confirm any personal information, such as passwords, bank details and so on.
- turn off any email security measures that your Headteacher/ Deputy Headteacher has put in place or recommended
- email sensitive information unless you know it is encrypted[1]. Talk to your IT technician for advice.
- try to bypass St Anne's Fulshaw CE Primary School security measures to access your email off-site (for example, forwarding email to a personal account)
- reply to chain emails.

1.8 - Passwords

1.8.1 - Do

- use a strong password (strong passwords are usually eight characters or more and contain upper and lower case letters, as well as numbers)
- make your password easy to remember, but hard to guess
- choose a password that is quick to type
- use a mnemonic (such as a rhyme, acronym or phrase) to help you remember your password. Change your password(s) if you think someone may have found out what they are.

1.8.2 - Don't

- share your passwords with anyone else
- write your passwords down
- use your work passwords for your own personal online accounts
- save passwords in web browsers if offered to do so
- use your username as a password
- use names as passwords
- email your password or share it in an instant message.

1.9 - Desktops

1.9.1 - Do

- shut down your desktop using the 'Shut Down' or 'Turn Off' option
- try to prevent people from watching you enter passwords or view sensitive information

[1] Encryption is a way of scrambling information. It helps stop anyone using the information if they do not have an electronic key or password to unscramble it.

- lock your desktop when leaving your laptop unattended

1.9.2 - Don’t

- leave your desktop unattended without locking it
- let unauthorised people use your desktop

1.10 - Sending and sharing

1.10.1 - Do

- be aware of who you are allowed to share information with. Check with your Information Asset Owner if you are not sure.
- ask third parties how they will protect sensitive information once it has been passed to them
- encrypt all removable media (USB pen drives, CDs, portable drives) taken outside the school building or sent by post or courier.

1.10.2 - Don’t

- send sensitive information (even if encrypted) on removable media (USB pen drives, CDs, portable drives) if secure remote access is available
- send sensitive information by email unless it is encrypted
- place protective labels on outside envelopes. Use an inner envelope if necessary. This means that people can’t see from the outside that the envelope contains sensitive information.
- assume that third-party organisations know how your information should be protected.

1.11 - Working on-site

1.11.1 - Do

- lock sensitive information away when left unattended
- lock laptops and notebooks to help prevent opportunistic theft.

1.11.2 - Don’t

- let strangers or unauthorised people into school without identification
- position screens where they can be read from outside the room.

1.12 - Working off-site

1.12.1 - Do

- only take offsite information you are authorised to and only when it is necessary. Ensure that it is protected offsite in the ways referred to above.
- wherever possible access data remotely instead of taking it off-site
- be aware of your location and take appropriate action to reduce the risk of theft
- make sure you sign out completely from any services you have used
- try to reduce the risk of people looking at what you are working with

Further help and support

St Anne’s Fulshaw CE Primary School has a legal obligation to protect personal information, under the Data Protection Act 1998. For more information, visit the website of the Information Commissioner’s Office [https://ico.org.uk/]

Reviewed: 17.05.16