Cavendish Close Infant and Nursery School

Data and Information Security Policy

This Policy forms part of the Schools Information Governance Framework.

1 Data Protection

For the school to operate effectively, it must process information about its employees and students/pupils/learners – data subjects. It does this under the Data Protection Act 1998 and other related legislation.

The School acting as a holder – known as a custodian or data controller – of personal information recognises its moral duty to make sure that data is handled properly and confidentially at all times, whether it is held on paper or electronically. This covers the whole lifecycle, including:

- obtaining personal data
- storing and securing personal data
- using personal data
- disposing or destroying personal data.

The school also has a responsibility to make sure that data subjects have the appropriate access under the 1998 Act, to their personal information upon written request.

This policy applies to all permanent and temporary employees and those acting on behalf of the Governing Body/Head Teacher.

2 Data Protection Actions

By following and maintaining strict safeguards and controls, the school will:

- acknowledge the rights of individuals to whom personal data relates and make sure that they can use these rights in accordance with the 1998 Act
- make sure that the collecting and using of personal data is done in a way that recognises the Fair

Processing Code, which means that personal data is obtained fairly and lawfully – issuing privacy statements when appropriate

- only obtain and process personal data as specified in our notification
- collect and process personal data on a **need to know** basis making sure that it is accurate, not excessive and is disposed of at a time appropriate to its purpose
- make sure that for all personal data it takes the correct security measures – both technically and organisationally - to protect against loss, damage or misuse
- make sure that the movement of personal data is done in a lawful way, both inside and outside the school and that it has suitable safeguards at all times
- follow all the good practice advice and guidance issued by the Information Commissioner Office

3 Data Protection Enablers

To support these actions, the school will:

- have a designated **Data Protection co-ordinator** responsible for gathering and distributing information and issues relating to information security, the Data Protection Act and other related legislation
- The **Data Protection Co-ordinator** is The Head teacher
- make sure that all activities that relate to the processing of personal data have the correct safeguards and controls to make sure of information security and compliance with the 1998 Act
- make sure that all contracts and service level agreements – SLAs – between the school and external organisations, including contract staff – where personal data is processed - refers to the 1998 Act where necessary.

The school will also:

- make sure that all employees, including contract staff acting on the school's behalf, understand their responsibilities about information security under the 1998 Act.
- make sure they receive appropriate mandatory training, instruction and supervision so they can perform these duties effectively and consistently
- make sure they only have access to personal information that is necessary to their duties
- make sure that all others acting on the schools behalf are only given access to personal information that is necessary to the duties they perform and no more

The school will:

- handle any requests for access to personal data courteously, promptly and appropriately, making sure that either the data subject or their authorised representative have the proper right to access under the 1998 Act
- make sure that information provided is clear and explicit
- make sure Information Sharing Agreements are in place where necessary and appropriate, when sharing with partner agencies takes place.
- manage reported security breaches appropriately and in line with the security breach management framework issued by the Information Commissioners Office
- review this policy and the safeguards and controls that relate to it regularly, but in any case within 24 months from date of issue, to make sure that they are still relevant, efficient and effective

4. Information Security

The purpose of information security is to protect the highly valued information assets of the school. The objective is to reduce the risk of security incidents and be able to demonstrate to pupils/students, parents and employees that we collect, handle and store their information securely. It also shows a commitment by the school to process information in line with relevant legislation and e-Government requirements.

The policy applies to all school employees, including contractors and agency workers who have authorised access to school IT systems.

5. Information Security Definition

The International Standard ISO/IEC 27001:2005 standard specification for Information Security Management defines Information Security as protecting three aspects of information:

- ***confidentiality-*** making sure that information is accessible only to those authorised to have access
- ***integrity-*** safeguarding the accuracy and completeness of information and processing methods
- ***availability-*** making sure that authorised users have access to information and associated resources when required.

Information comes in many forms. It can be:

- stored on computers
- sent across networks
- printed out
- written
- spoken
- visual.

Information Security covers the safekeeping of all forms of information to protect its confidentiality, integrity and availability.

This is put into practice through appropriate controls, which will be a combination of policies, procedures, standards, guidelines, common sense and physical or hardware/software measures.

6. Information Security responsibilities and accountabilities

The Governing Body has responsibility for defining and setting the school's information security policies, standards and procedures. Every IT system user who has access to school information is responsible and accountable for putting into practice these policies, standards and procedures.
Information Security is not an option. We are all required to keep a minimum level of security to meet our legal and contractual obligations.

7. Information Security Compliance with legal and contractual requirements

The school has an obligation to make sure that all information systems and processes meet the terms of all relevant legislation and contractual requirements, including the:

- Data Protection Act 1998
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Freedom of Information Act 2000

The Head teacher has specific responsibility for the Data Protection Act notification to the Office of the Information Commissioner.

8. Actions required to maintain confidentiality, integrity and availability

- Everyone has a responsibility to make sure that personal information is only collected, used, stored and shared for the purpose it was provided.
- Make sure any requests for personal information are handled in accordance with the Data Protection Act 1998. Information should only be disclosed on a need to know basis. Always make checks on the identity of callers.
- Make sure printed or hand written personal information is kept secure at all times.
- Make sure printed or hand written personal information is disposed of in a secure manner eg using the shredder

- Never dispose of personal information in general waste.

- Always use the computer screen lock facility where personal information may be held on the hard drive of a PC or laptop when the device is logged in and unattended.

- Never share user names and passwords. Never encourage others to anyone else's personal ID and password to log into a PC, the network, individual system or email.

- It is a criminal offence under the Computer Misuse Act 1990 to access a computer system without authority to do so.

- Be aware that emails are not usually a secure method of sharing personally identifiable information external to the school. EGRESS email system is used by the school for this.

- To avoid introducing viruses into the School network never open email attachments from unknown external sources.

- Make sure you set your password to the minimum standard required. Keep them secure and change them regularly.

9. Working Off Site

Information security is put into practice through appropriate controls which could be a combination of policies and procedures, guidelines and common sense. The definition of mobile computer equipment includes all portable equipment that has any data processing capability including but not limited to:

Laptops
ipads
Notebooks
Tablets
Personal Digital Assistants – PDA's and smart phones such as iPhones.

The definition of mobile storage device includes but is not limited to…

Universal Serial Bus – USB – port devices such as pen drives, flash drives and memory sticks
Hand held wireless devices such as Bluetooth
External hard drives

Occasionally it is necessary for employees to take work off school premises to work remotely, whether that be at home or to another location.
There are many additional risks to information security that result from this. Mobile computing devices are attractive, portable and easy targets for the opportunist thief. They are susceptible to loss, hacking and the distribution of malicious software – viruses. They are often used for storing personal and/or sensitive information, particularly about pupils/students that could be of more value that the device itself, and which if lost or stolen could have very serious financial and reputational implications to the school and its employees.

10. Security of mobile computing equipment, mobile devices and data

Mobile computing equipment and the data held on them must be protected by adequate security. They must be

- kept out of sight - for example in the locked boot of the car when being transported
- kept secure and guarded from theft and unauthorised access at all times - if you are working on information involving children at home make sure no other member of the family can access this information
- carried separately and concealed wherever possible by using an ordinary bag or rucksack rather than a laptop case
- protected from 'shoulder surfing' - when in public, make sure no-one can see your password or any other information
- backed up to a local server at the earliest opportunity or to an encrypted external hard drive. File and data housekeeping should be performed to make sure obsolete data is not kept any longer than necessary.
- locked away or put out of sight when not being used – this includes at home

- They must not be left unattended - for example do not leave them in your boot overnight even if kept in a locked garage
- School pupil/student information must not be loaded onto personal mobile devices

11. Other relevant policies, procedures and standards

- *Policy on the use of ICT and e-safety*

12. Compliance with the Data Protection Act Policy

The Head teacher is responsible for monitoring compliance with this Policy

If employees knowingly or recklessly fail to comply with this Policy, other school policies, procedures or guidelines the school may take appropriate action under the Disciplinary Procedure.

13. Contact Details

Please contact the Head teacher with any queries in relation to this Policy.

Or contact local authority information governance team on 640763 at information.governance@derby.gov.uk with enquires about this policy or any other referenced policy, procedure or law.

Policy Change History Sheet

Policy title: data and information security policy		
Review Date	Section	Summary of change
September 2015		Page numbers inserted
