CONSETT JUNIOR SCHOOL

Data Protection Policy

Document control

Document reference:	Data Protection Policy	**Date implemented:**	March 2019
Version:	21.1	**Date modified:**	March 2021
Revision due date:	March 2023	**Publication:**	March 2021
Reviewed by:	P. Dixon R. Waters	**Sign and date:**	
Authorised by:	Chair – A. Fraser	**Sign and date:**	

Version	Date	Description
19.1	March 2019	Initial Policy
21.1	March 2021	Review in line with updated guidance

Contents

1. Purpose and Aims

Our school aims to ensure that all data collected about staff, pupils, parents and visitors is collected, stored and processed in accordance with the Data Protection Act 2018.

The aim of this policy is to provide a framework to enable staff, parents and pupils to understand:

- The law regarding personal data
- How personal data should be processed, stored, archived and deleted/destroyed
- How staff, parents and pupils can access personal data
- This policy applies to all data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the Data Protection Act 2018, and is based on guidance published by the Information Commissioner's Office and model policies published by the Local Authority and Department for Education.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

Term	Definition
Personal Data	Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identified
Sensitive personal data	Data such as: • Contact details • Racial or ethnic origin • Political opinions • Religious beliefs, or beliefs of a similar nature • Where a person is a member of a trade union • Physical and mental health • Sexual orientation • Whether a person has committed, or is alleged to have committed, an offence • Criminal convictions
Processing	Obtaining, recording or holding data
Data subject	The person whose personal data is held or processed
Data controller	A person or organisation that determines the purposes for which, and the manner in which, personal data is processed
Data processor	A person, other than an employee of the data controller, who processes the data on behalf of the data controller

4. The data controller

Our school processes personal information relating to pupils, staff and visitors, and, therefore, is a data controller. Our school delegates the responsibility of data protection officer to Miss Waters.

The school is registered as a data controller with the Information Commissioner's Office and renews this registration annually.

5. Data protection principles

The Data Protection Act 2018 is based on the following data protection principles, or rules for good data handling, and our school ensures the integrity of data based on these:

• Data shall be processed fairly and lawfully;
• Personal data shall be obtained only for one or more specified and lawful purposes;
• Personal data shall be relevant and not excessive in relation to the purpose(s) for which it is processed;
• Personal data shall be accurate and, where necessary, kept up to date;
• Personal data shall not be kept for longer than is necessary for the purpose(s) for which it is processed;
• Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 2018 and the General Data Protection Regulations;
• Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of, or damage to, personal data;
• Personal data shall not be transferred to a country or territory outside the European Economic Area unless the country or territory ensures an adequate level of protection for the rights and freedoms of data in relation to the processing of personal data.

6. Roles and responsibilities

The governing board has overall responsibility for ensuring that Consett Junior School complies with its obligations under the Data Protection Act 2018.

Day-to-day responsibilities rest with the Headteacher or the Deputy Headteacher in the headteacher's absence. The headteacher will ensure that all staff are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data.

Staff are responsible for ensuring that they collect and store any personal data in accordance with this policy, the Privacy notice for Staff, Staff IT Acceptable Usage Policy and the Data Retention Policy.

Staff must also inform the school of any changes to their personal data, such as a change of address.

7. Privacy/fair processing notice

We, Consett Junior School, hold personal data about pupils to support teaching and learning, to provide pastoral care, and to assess how the school is performing. We may also receive data about pupils from other organisations, or ask third parties to process data on our behalf (data processors). We process data relating to those we employ to work at, or otherwise engage to work at, our school including of governing body. The purpose of processing this data is to assist in the running of the school.

For full information about the data we collect, use, store, and share please see our Privacy Notice for Pupils and Parents, Privacy Notice for Staff and Privacy Notice for Governors.

8. Subject access requests

Under the Data Protection Act 2018, individuals have a right to request access to information the school holds about them. This is known as a subject access request. Personal data about a child belongs to that child, and not the child's parents. This is the case even where a child is too young to understand the implications of subject access rights. For a parent to make a subject access request, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Subject access requests must be submitted in writing, either by letter or email. Requests should include:
- The data subjects name
- A correspondence address
- A contact number and email address
- Details about the information requested

The school will not reveal the following information in response to subject access requests:

- Information that might cause serious harm to the physical or mental health of the pupil or another individual
- Information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests
- Information contained in adoption and parental order records
- Certain information given to a court in proceedings concerning the child

Subject access requests for all or part of the pupil's educational record will be provided within 30 days free of charge.

The school will maintain a documented record of all requests for personal information with details of who dealt with the request, what information was provided and when, and any outcomes. The record will be used if there is a subsequent complaint in relation to the request.

9. Parental requests to see the educational record

Parents have the right of access to their child's educational record, free of charge, within 15 school days of a request.

Personal data about a child belongs to that child, and not the child's parents. This is the case even where a child is too young to understand the implications of subject access rights.

For a parent to make a subject access request, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

The Information Commissioner's Office, the organisation that upholds information rights, generally, regards children aged 12 and above as mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents of pupils at our school may be granted without the express permission of the pupil.

If parents ask for copies of information, they will be required to pay the cost of making the copies.

10. Information Security

Objective
The information security objective is to ensure that the school's information base is protected against identified risks so that it may continue to deliver its services and obligations to the community. It also seeks to ensure that any security incidents have a minimal effect on its business and academic operations.

Responsibilities
The Headteacher of the school has direct responsibility for maintaining the Information Security policy and for ensuring that the staff of the school adheres to it.

General Security
It is important that unauthorised people are not permitted access to school information and that we protect against theft of both equipment and information. This means that we must pay attention to protecting our buildings against unauthorised access. Staff must:

• Not reveal pin numbers or building entry codes to people that you do not know or who cannot prove themselves to be employees;
• Beware of people tailgating you into the building or through a security door;
• If you don't know who someone is and they are not wearing some form of identification, ask them why they are in the building;
• Not position computer screens on desks where members of the public could see them;
• Lock secure areas when they are unattended;
• Not let anyone remove equipment or records unless you are certain who they are;
• Visitors and contractors in school buildings should always sign in at the main reception.

Security of Paper Records

• Paper documents should always be filed with care in the correct files and placed in the correct place in the storage facility.
• Records that contain personal data, particularly if the information is sensitive should be locked away when not in use and should not be left open or on desks overnight or when you are not in the office;
• Always keep track of files and who has them;
• Do not leave files out where others may find them;
• Where a file contains confidential or sensitive information, do not give it to someone else
to look after.
• Adhere to school's clear desk policy

Security of Electronic Data

Most of our data and information is collected, processed, stored, analysed and reported electronically. It is essential that our systems, hardware, software and data files are kept secure from damage and unauthorised access. School staff must:
• Prevent access to unauthorised people and to those who don't know how to use an item of software properly. It could result in loss of information;
• When we buy a license for software, it usually only covers a limited quantity of machines and/or users. Make sure that you do not exceed this number, as you will be breaking the terms of the contract.
• Passwords are a critical element of electronic information security. All staff must manage their passwords in a responsible fashion:

- Don't write it down;
- Don't give anyone your password;
- Your password should be at least 8 characters;
- The essential rules your password is something that you can remember but not anything obvious (such as password) or anything that people could guess easily such as your name

- You can be held responsible for any malicious acts by anyone to whom you have given your password;

• Include numbers and symbols as well as uppercase letters in the password;
• Take care that no-one can see you type in your password;
• Change your password when prompted. Also change it if you think that someone may know what it is.
• Many database systems, particularly those containing personal data such as our Management Information System should only allow a level of access appropriate to each staff member. The level may change over time.

Use of E-Mail and Internet

The use of the school's e-mail system and wider Internet use is for the professional work of the school. Reasonable personal use of the system in a member of staff's own time is permitted but professional standards of conduct and compliance with the school's wider policies are a requirement whenever the e-mail or Internet system is being used.

The school uses a filtered and monitored broadband service to protect our pupils and staff. Deliberate attempts to access web sites that contain unlawful, pornographic, offensive or gambling content are strictly prohibited. Staff discovering such sites on the system must report this to the IT Network Manager immediately.

• To avoid a computer virus, malware or ransomware arriving over the Internet, do not open any attachments which you either not expecting or from an unknown sender
• Do not send highly confidential or sensitive personal information via e-mail;
• Save important e-mails straight away;
• Unimportant e-mails should be deleted straight away;
• Do not write anything in an e-mail which could be considered inaccurate or offensive, and cannot be substantiated.

Electronic Hardware

• All hardware held within school should be included on the asset register;
• When an item is replaced, the register should be updated with the new equipment removed or replaced;
• Do not let anyone remove equipment unless you are sure that they are authorised to do so; Electronic Hardware
• All hardware held within school should be included on the asset register;
• When an item is replaced, the register should be updated with the new equipment removed or replaced;
• Do not let anyone remove equipment unless you are sure that they are authorised to do so.

Homeworking Guidance

If staff must work outside of the school or at home, all of the 'Information Security' policy principles still apply. However, working outside of the school presents increased risks for securing information.

The following additional requirements apply:

• Do not access confidential information when you are in a public place, such as a train and may be overlooked;
• Do not have conversations about personal or confidential information on your mobile when in a public place. Ensure that, if urgent, you have your conversation in a separate room or away from other people;
• School SharePoint and/or OneDrive should be used so confidential documents do not have to be taken off side whenever possible so data is still being held securely on the school tenancy.

If you use a laptop, tablet or smart phone:

• Ensure that it is locked and password protected to prevent unauthorised access;
• Make sure that you don't leave your device anywhere it could be stolen. Keep it with you at all times and secure it when you are in the School;
• Portable devices or memory sticks that contain personal data must be encrypted. Taking personal data off-site on a device or media that is not encrypted is a disciplinary matter;
• Ensure personal data is not stored on the hard drive of a personal device;
• When working on confidential documents at home do not leave them lying around where others may see them; dispose of documents using a shredder;
• If you are using your own computer, ensure that you access and work on your school computer using the SharePoint and/or OneDrive. Do not transfer documents and data to your own machine. It is strictly forbidden to use a computer owned by you to hold personal data about pupils or staff at the school.

Audit of Data Access

• Where possible our software specifications will include the function to audit access to confidential data and attribute access, including breaches of security, to specific users.

Data Backup

• The school will arrange that all critical and personal data is backed up to physical storage on a daily basis.
• All backups taken are checked for integrity on a weekly basis.
• All backups are encrypted wherever possible.
• If the school is physically damaged critical data backups in a remote location will allow the school to continue its business at another location with secure data.
• Data backup should routinely be managed on a rolling daily process to secure off-site areas.

11. Information Sharing

• The school only shares personal information with other organisations where there is a legal requirement to do so or the organisation has been contracted by the School to carry out a function of the school.
• The school is required, for example, to share information with the Department for Education and the Education Funding Agency. Under certain circumstances, such as child protection, we may also be required to share information with Children's Social Services or the police.
• Because our pupils are of primary school age, their own right to access their own personal information held by the school will be exercised through their parents or guardians.
• The Headteacher will be ultimately responsible for authorising the sharing of data with another organisation. The principle, in authorising the sharing of data will take account of:

- Whether it is lawful to share it;
- Whether there is adequate security in place to protect the information while it is being transferred and then held by the other organisation;

• Include in the Privacy Notice a simple explanation of who the information is being shared with and why.

Considerations regarding the method of transferring data should include:

• If personal data is sent by e-mail then security will be threatened. You may need to check that the recipient's arrangements are secure enough before sending the message. The data may also need to be password protected and the password sent separately. You should also check that it is going to the correct e-mail address.
• Circular e-mails sent to parents should be sent bcc (blind carbon copy) so that the e-mail addresses are not disclosed to everyone.
• Similar considerations apply to the use of fax machines. Ensure that the recipient will be present to collect a fax when it is sent and that it will not be left unattended on their equipment.
• If confidential personal data is provided by paper copy it is equally important to ensure that it reaches the intended recipient.

12. Websites

The school website will be used to provide important information for parents and pupils including our Privacy Notice and our Freedom of Information publication scheme.
Where personal information, including images, are placed on the web site the following principles will apply:

• We will not disclose personal information (including photos) on a web site without the consent of the pupil, parent, member of staff or Governor as appropriate;
• Comply with regulations regarding cookies and consent for their use;
• Our website design specifications will take account of the principles of data protection.

13. Digital Images

The school may use photographs of pupils or staff taken for inclusion in the printed prospectus or other school publications without further specific consent being sought.

All other uses by the school of photographic images are subject to data protection.

Full guidance on the use, storage and retention of digital images can be found in the schools Digital Images Policy.

14. Disposal of information

Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely.
• Paper records should be disposed of with care. If papers contain confidential or sensitive information they must be shredded before disposing of them. Particular care must be taken when selecting papers to be placed in a recycling bin.
• Computers and hardware to be disposed of must be completely 'wiped' before disposal. It is not enough just to delete all the files.
• It cannot be assumed that simply deleting a file will prevent it being recovered from electronic media. Electronic memory containing personal information or sensitive personal information must be electronically scrubbed or physically destroyed.
• Where a third party contractor holds personal information on behalf of the school, for example a software provider, the school will seek reassurance from the contractor regarding their data protection policies and procedures.
• Records will be held in accordance with the schools record retention policy.

15. Training

Our staff and governors are provided with data protection training as part of their induction process and at least on an annual basis.

Data protection will also form part of continuing professional development, where changes to legislation or the school's processes make it necessary.

The Headteacher will ensure that all staff are adequately trained to understand their responsibilities in relation to this policy and procedures.

16. Monitoring arrangements

The Headteacher is responsible for monitoring and reviewing this policy.

The Headteacher and chair of governors checks that the school complies with this policy by, among other things, reviewing school records on a termly basis or sooner if required.

At every review, the policy will be shared with the governing board.

17. Links with other policies

This data protection policy and privacy notice is linked to the freedom of information publication scheme.

Other policies which may be relevant to this policy include, but not limited to;
• Staff Privacy Notice
• Pupil/parent Privacy Notice
• Governor Privacy Notice
• Digital Images Policy
• Data Retention Policy