Believe Grow Achieve

Copmanthorpe Primary School

Data Protection Policy

Approved by:	FGB	**Date:**	September 2026
Last reviewed:	September 2025		
Next review due by:	September 2027		

Contents

1. INTRODUCTION AND SCOPE 3
2. STATUTORY FRAMEWORK 4
3. ROLES AND RESPONSIBILITIES 4
3.1 Governing Body 4
3.2 Data Protection Officer (DPO) 4
3.3 Senior Information Risk Owner (SIRO) 4
3.4 Single Point of Contact (SPOC) 4
3.5 Information Asset Owners (IAOs) 5
3.6 All staff and other authorised users 5
4. DATA PROTECTION PRINCIPLES 5
5. LAWFUL BASES AND SPECIAL CATEGORY DATA 5
6. CONSENT 5
7. PRIVACY INFORMATION AND CHILDREN'S DATA 6
8. DATA SUBJECT RIGHTS 6
9. RECORDS OF PROCESSING, RETENTION AND DISPOSAL 6
10. DATA PROTECTION BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENTS 7
11. INFORMATION SHARING 7
12. CONTRACTS, PROCESSORS AND EDTECH 7
13. INTERNATIONAL TRANSFERS 8
14. ARTIFICIAL INTELLIGENCE AND AUTOMATED DECISION-MAKING 8
15. FILTERING AND MONITORING 8
16. PHOTOGRAPHS, VIDEO AND OTHER IMAGES 8
17. INFORMATION SECURITY AND PERSONAL DATA BREACHES 9
18. TRAINING AND AWARENESS 9
19. DATA PROTECTION COMPLAINTS 9
20. MONITORING AND REVIEW 9
APPENDIX 1 – APPROPRIATE POLICY DOCUMENT 11
1. Purpose 11
2. Special category and criminal offence data 11
3. Conditions for processing 11
4. Compliance with the data protection principles 11
5. Retention and erasure 11
6. Review 12
APPENDIX 2 – SUBJECT ACCESS REQUEST (SAR) PROCEDURE 13
1. Recognising a request 13
2. Logging and clarification 13
3. Identity and authority 13
4. Timescale 13
5. Searching for information 13
6. Reviewing and redacting information 13
7. Providing the response 13
8. Fees, refusal and excessive requests 13
9. Education records 14
10. Complaints 14
APPENDIX 3 – FREEDOM OF INFORMATION (FOI) AND ENVIRONMENTAL INFORMATION REGULATION (EIR) REQUESTS 15
1. Freedom of Information 15
2. Environmental Information Regulations 15
3. Handling requests 15
4. Timescales 15
5. Fees 15
6. Internal review and ICO 15

7. Copyright and re-use.....15
KEY EXTERNAL GUIDANCE 15

1. Introduction and scope

Copmanthorpe Primary School processes personal information about pupils, parents and carers, staff, governors, volunteers and other individuals with whom the school interacts. We are committed to protecting this information and handling it lawfully, fairly, transparently and securely.

This policy sets out the framework through which the school meets its data protection and information governance responsibilities. It applies to all personal

data processed by or on behalf of the school, whether held electronically, on paper, in photographs, video, audio or other formats.
The policy applies to employees, governors, contractors, agency and temporary staff, volunteers and others who process personal information on behalf of the school. Everyone who handles personal information has a responsibility to do so appropriately. Deliberate or reckless breaches of this policy may result in disciplinary or other appropriate action.
This policy should be read alongside the school's Information Security, Online Safety, Records Management, Safeguarding and acceptable use arrangements.

2. Statutory framework

The school will comply with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and the amendments made by the Data (Use and Access) Act 2025. The school will also comply with other relevant information rights legislation, including the Freedom of Information Act 2000 and the Environmental Information Regulations 2004.
The Data (Use and Access) Act 2025 does not replace the UK GDPR or Data Protection Act 2018. It amends and builds on the existing framework. The school will have regard to current guidance issued by the Information Commissioner's Office (ICO), the Department for Education (DfE) and its Data Protection Officer (DPO).

3. Roles and responsibilities

3.1 Governing Body

The Governing Body has overall responsibility for ensuring that the school complies with its statutory data protection obligations. Governors will receive appropriate assurance about the school's arrangements and will support and challenge leaders in maintaining effective information governance.

3.2 Data Protection Officer (DPO)

The school has appointed Veritau as its Data Protection Officer. The DPO provides independent advice and support, monitors compliance, advises on Data Protection Impact Assessments (DPIAs) and liaises with the ICO where appropriate.
Schools Data Protection Officer
Veritau
West Offices
Station Rise
York
YO1 6GA
schoolsDPO@veritau.co.uk | 01904 554025

3.3 Senior Information Risk Owner (SIRO)

The Headteacher is the school's Senior Information Risk Owner and has overall operational responsibility for information risk and for ensuring that appropriate policies, procedures and controls are in place.

3.4 Single Point of Contact (SPOC)

The School Business Manager acts as the school's operational point of contact for data protection. The SBM coordinates day-to-day data protection matters, including liaison with the DPO and the management of information rights requests.

3.5 Information Asset Owners (IAOs)

Where appropriate, the school will identify staff responsible for significant information assets or systems. IAOs are responsible for understanding how information within their area is collected, used, stored, shared and protected. Relevant responsibilities will be recorded within the school's Information Asset Register (IAR).

3.6 All staff and other authorised users

Everyone who processes personal information on behalf of the school must:

- handle personal information securely and only for legitimate school purposes
- access only the information needed to carry out their role
- follow the school's data protection, information security and acceptable use requirements
- complete required training
- report suspected data breaches, loss of information or other data protection concerns promptly
- seek advice where they are unsure whether information can lawfully be accessed, used or shared

4. Data protection principles

The school will comply with the principles in Article 5 of the UK GDPR. Personal data will be:

- processed lawfully, fairly and transparently
- collected for specified, explicit and legitimate purposes and not used incompatibly with those purposes
- adequate, relevant and limited to what is necessary
- accurate and, where necessary, kept up to date
- kept in identifiable form for no longer than necessary
- processed securely using appropriate technical and organisational measures.

The school is also responsible for demonstrating compliance with these principles (accountability).

5. Lawful bases and special category data

The school will identify and document an appropriate lawful basis for each processing activity. As a maintained school carrying out public functions, the bases most commonly relied upon are legal obligation and public task. Other bases may apply where appropriate, including contract, vital interests, consent and legitimate interests.

The Data (Use and Access) Act 2025 introduced the concept of recognised legitimate interests. The school will only rely on this or any other legitimate interests basis where it is appropriate to the particular processing and will document the basis relied upon. Where a legitimate interests assessment is required, it will be completed before the processing begins.

Where special category data or criminal offence data is processed, the school will identify the additional condition required by law and will comply with its Appropriate Policy Document where applicable. The school's Appropriate Policy Document is at Appendix 1.

6. Consent

The school will only rely on consent where it is the appropriate lawful basis and where individuals have a genuine choice. Consent will be specific, informed, freely given and demonstrated by a clear affirmative action. It can be withdrawn at any time.

Where consent is used, the school will keep an appropriate record and will review the consent where the purpose, relationship or processing changes. For children, the school will consider age, understanding and the nature of the processing when deciding whose consent is appropriate.
Consent is not required for processing that the school must carry out because of a legal obligation or its public functions.

7. Privacy information and children's data

The school will provide clear privacy information explaining how and why personal data is used, the lawful basis relied upon, who it may be shared with, how long it is kept and the rights available to individuals.
Privacy notices will be accessible and reviewed when processing changes.
Information intended for pupils will be written and presented in a way that is appropriate to their age and understanding.
Children have data protection rights in their own right. When processing children's personal data, the school will take particular account of their interests, rights, development and reasonable expectations. Where EdTech or online services are used, the school will consider whether suppliers are subject to the ICO's Children's Code and will seek appropriate assurances.

8. Data subject rights

Individuals have rights under data protection law, subject to the circumstances and lawful basis of the processing. These include:

- the right to be informed
- the right of access
- the right to rectification
- the right to erasure in appropriate circumstances
- the right to restrict processing in appropriate circumstances
- the right to object in appropriate circumstances
- the right to data portability where applicable
- rights relating to automated decision-making and profiling.

Requests may be made to any member of staff and do not normally have to use a particular form. Staff must forward any request to the School Business Manager promptly. The school will seek advice from the DPO where necessary and will keep an appropriate record of requests and decisions.
Subject access requests are dealt with in accordance with Appendix 2.

9. Records of processing, retention and disposal

The school will maintain an Information Asset Register or equivalent record of processing activities. This will document, as appropriate, the information held, purposes, categories of individuals and data, lawful bases, access and sharing arrangements, retention periods, locations, international transfers and security measures.
The school will review its information assets regularly and at least annually.
Personal data will not be retained for longer than necessary. Retention periods will be set out in the school's retention schedule, informed by legal requirements and relevant sector guidance.
Information that is no longer required will be securely deleted, destroyed or anonymised. The school will maintain appropriate records of significant destruction activity.

10. Data protection by design and Data Protection Impact Assessments

Data protection will be considered from the outset when introducing or significantly changing systems, services, projects or ways of working. The school will apply data minimisation, appropriate access controls, secure defaults and other proportionate safeguards.

A Data Protection Impact Assessment (DPIA) will be completed where processing is likely to result in a high risk to individuals' rights and freedoms. This may include, for example, large-scale or particularly sensitive processing, systematic monitoring, biometric processing, profiling or certain uses of artificial intelligence.

DPIAs will be started early enough to influence decisions, reviewed when processing changes and referred to the DPO for advice. High residual risks will be escalated in accordance with legal requirements.

11. Information sharing

The school may share personal information where this is necessary and lawful to carry out its educational, safeguarding, employment and other statutory functions. Routine sharing arrangements will be reflected in privacy information and the Information Asset Register.

Before sharing personal data, staff should consider what information is necessary, who needs it, the lawful basis, how it will be shared securely and whether the sharing should be recorded.

Safeguarding information will be shared where necessary to protect a child or another person. Data protection law does not prevent appropriate safeguarding information sharing. Staff should follow the school's safeguarding procedures and seek advice where needed.

Regular or higher-risk sharing arrangements may require a data sharing agreement or other documented arrangement.

12. Contracts, processors and EdTech

Where another organisation processes personal data on the school's behalf, the school will carry out proportionate due diligence and ensure that an appropriate written contract or data processing agreement is in place. Contracts will include the requirements of data protection law and address security, confidentiality, sub-processors, data subject rights, breach notification, return or deletion of data and audit or assurance where appropriate.

When procuring or adopting educational technology, digital platforms or applications, the school will consider data protection from the outset. This includes:

- what personal data is required and whether collection is proportionate
- the lawful basis and any special category conditions
- the roles of the school, supplier and any sub-processors
- where data is stored and whether international transfers occur
- security, authentication, access controls and audit logging
- retention, deletion and exit arrangements
- support for information rights requests
- whether AI, profiling or automated decision-making is used
- whether a DPIA is required and whether privacy notices need updating.

The DPO and, where relevant, the school's IT lead and Designated Safeguarding Lead will be consulted before introducing higher-risk technology. Suppliers and processing arrangements will be reviewed where significant changes occur.

13. International transfers

Where personal data is transferred or made accessible outside the UK, the school will ensure that the transfer complies with UK data protection law. This may include relying on UK adequacy regulations or putting in place an appropriate transfer mechanism and any additional safeguards required.
The school will identify international transfers through its procurement, contract and information asset processes and will seek advice from the DPO before entering into arrangements where the position is unclear or higher risk.

14. Artificial intelligence and automated decision-making

The school recognises that artificial intelligence (AI), including generative AI, can create additional data protection risks. AI tools used for school purposes must be approved and used in accordance with the school's Online Safety, Information Security and acceptable use arrangements.
Staff should avoid entering personal data, special category data, safeguarding information or other confidential information into generative AI tools. Where there is a proposed need to use personal data within an AI system, this must be considered in advance with the DPO or appropriate school lead so that the lawful basis, transparency, security, supplier terms and any DPIA requirements can be addressed.
The school will understand whether information entered into an AI tool is retained, used to train models, shared with third parties or transferred internationally. Privacy information will be updated where necessary.
Where automated decision-making or profiling is used, the school will ensure that the processing is lawful, fair and transparent and that any safeguards required by law are in place. Decisions with significant effects on individuals will not be left to automated systems without appropriate consideration of the legal requirements and human oversight.

15. Filtering and monitoring

The school uses filtering and monitoring arrangements to support safeguarding, online safety and the security of its systems. Personal data generated through these systems will be handled lawfully, proportionately and transparently.
Access to monitoring data and alerts will be restricted to authorised personnel with appropriate training. The school will establish appropriate retention and safeguarding arrangements and ensure relevant privacy information explains what is monitored, why it is monitored, who may access the information and how long it is retained.
A DPIA will be completed before introducing a new filtering or monitoring system or making a significant change to an existing system. Third-party providers will be subject to appropriate due diligence and contractual controls.

16. Photographs, video and other images

The school may take and use photographs or video for educational, assessment, celebration, communication and publicity purposes where there is an appropriate lawful basis.

Where consent is the appropriate basis, including for particular external publication or publicity uses, the school will operate a clear permissions process and will respect changes to those preferences.
Before publishing or externally sharing identifiable images, staff will check relevant permissions and consider any safeguarding, privacy or welfare concerns. Personal information will not normally be published alongside an identifiable image unless there is a clear reason and appropriate authority to do so.
Staff will use school-authorised devices, accounts and systems for pupil images unless an alternative arrangement has been specifically authorised. Individual safeguarding arrangements may override general permissions.

17. Information security and personal data breaches

The school will use appropriate technical and organisational measures to protect personal data against unauthorised or unlawful processing and against accidental loss, destruction, alteration or disclosure.
All staff must report suspected or actual personal data breaches promptly in accordance with the school's Information Security procedures. This includes lost or misdirected information, inappropriate access, accidental disclosure, compromised accounts and cyber incidents involving personal data.
Breaches will be recorded, investigated and assessed. The DPO will be consulted where appropriate. Where the legal threshold is met, the school will notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of the breach. Individuals will also be informed where required by law.

18. Training and awareness

The school will provide appropriate data protection and information security training to staff and other authorised users. Training will form part of induction and will be refreshed at appropriate intervals.
Staff with additional responsibilities, including the SIRO, SPOC and Information Asset Owners, will receive role-appropriate support. The school will maintain records of training and reinforce key expectations through briefings and other communications.

19. Data protection complaints

The school will provide a clear and accessible way for individuals to raise concerns or complaints about the way their personal data has been handled. Complaints should normally be directed to the School Business Manager, who will liaise with the DPO where appropriate.
In accordance with current data protection law, the school will acknowledge a data protection complaint within 30 days, investigate it appropriately and communicate the outcome without undue delay. The school will keep an appropriate record of the complaint and the action taken.
If an individual remains dissatisfied, they may complain to the Information Commissioner's Office (ICO). The school will provide current ICO contact information or direct individuals to the ICO's official website.

20. Monitoring and review

The school will review this policy at least annually and sooner where there are significant changes to legislation, statutory guidance, school systems or

processing activities. The Governing Body will receive appropriate assurance about data protection compliance.
Operational documents, including privacy notices, the Information Asset Register, retention schedule, DPIAs, contracts and data sharing arrangements, will be reviewed and updated as necessary.

Appendix 1 – Appropriate Policy Document

1. Purpose

Copmanthorpe Primary School processes special category data and criminal offence data in the course of carrying out its functions. The Data Protection Act 2018 requires an Appropriate Policy Document (APD) where certain Schedule 1 conditions are relied upon. This appendix records the school's approach and should be read alongside the main policy, Information Asset Register, retention schedule and information security arrangements.

2. Special category and criminal offence data

Special category data may include information about:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic or biometric data used for identification
- health
- sex life or sexual orientation

The school may also process criminal offence data, including information relevant to safer recruitment, DBS checks and safeguarding or employment matters.

3. Conditions for processing

The school will identify an Article 6 lawful basis and, where required, an Article 9 condition and a condition under Schedule 1 of the Data Protection Act 2018. Conditions commonly relevant to the school include:

- employment, social security and social protection
- substantial public interest, including statutory and government purposes
- preventing or detecting unlawful acts
- safeguarding children and individuals at risk
- health or social care purposes where applicable
- explicit consent where this is genuinely appropriate.

The exact condition relied upon will depend on the processing activity and will be recorded in the school's information governance documentation.

4. Compliance with the data protection principles

The school will process special category and criminal offence data in accordance with the data protection principles. In particular, it will:

- provide appropriate privacy information
- collect only information that is necessary and proportionate
- take reasonable steps to keep information accurate
- apply retention periods and securely dispose of information when no longer required
- restrict access to those who need it
- use appropriate technical and organisational security measures
- maintain records sufficient to demonstrate accountability.

5. Retention and erasure

Retention periods are set out in the school's retention schedule and Information Asset Register. Information will be securely erased, destroyed or anonymised when it is no longer required, unless there is a lawful reason to retain it.

6. Review

This APD will be retained and reviewed in accordance with the requirements of the Data Protection Act 2018 and whenever the school materially changes the relevant processing.

Appendix 2 – Subject Access Request (SAR) Procedure

1. Recognising a request

A subject access request is a request by an individual for access to their personal data. A request does not need to mention the UK GDPR, use the words 'subject access request' or be made on a particular form. It may be made verbally or in writing and may be received by any member of staff.

Any member of staff receiving a possible SAR must forward it to the School Business Manager immediately.

2. Logging and clarification

The School Business Manager will log the request and acknowledge it promptly. Where necessary, the school may ask the requester to clarify the information or processing activities to which the request relates. Any clarification sought will be reasonable and proportionate.

3. Identity and authority

The school must be satisfied about the identity of the requester and, where someone is acting on another person's behalf, their authority to do so. Only information reasonably necessary to confirm identity or authority will be requested.

Requests made by parents or carers for a child's personal data will be considered in light of the child's age, understanding, best interests and rights. Parental responsibility does not automatically entitle an adult to all of a child's personal data.

4. Timescale

The school will normally respond without undue delay and within one month of receiving a valid request. Where permitted by law, the period may be extended by up to two further months because of the complexity or number of requests. The requester will be informed within the initial one-month period if an extension is required.

5. Searching for information

The school will carry out reasonable and proportionate searches for personal data falling within the scope of the request. Relevant staff and systems will be identified and search terms, date ranges or other parameters may be used where appropriate.

6. Reviewing and redacting information

Before disclosure, the school will review the information to determine whether it includes personal data relating to other individuals, information subject to an exemption or material that should otherwise be withheld. Advice will be sought from the DPO where necessary.

7. Providing the response

Information will normally be provided electronically where the request was made electronically, unless another reasonable format is requested. The school will provide the information required by law about the processing of the individual's personal data.

8. Fees, refusal and excessive requests

The school will not normally charge a fee. Where the law permits a reasonable fee or permits the school to refuse to act because a request is manifestly unfounded or excessive, the school will seek DPO advice and explain the decision to the requester.

9. Education records

Requests for access to a maintained-school pupil's educational record may also fall under the Education (Pupil Information) (England) Regulations 2005. Where those Regulations apply, the school will follow the applicable statutory procedure and timescale.

10. Complaints

Concerns about the handling of a SAR will be dealt with through the school's data protection complaints process. Individuals may also complain to the ICO.

Appendix 3 – Freedom of Information (FOI) and Environmental Information Regulation (EIR) Requests

1. Freedom of Information

The Freedom of Information Act 2000 gives any person a right to request recorded information held by the school, subject to statutory exemptions. The school also maintains a publication scheme in accordance with ICO requirements.

A valid FOI request must normally be in writing, include the requester's real name and an address for correspondence, and describe the information requested.

2. Environmental Information Regulations

Requests for environmental information are handled under the Environmental Information Regulations 2004. EIR requests may be made verbally or in writing and are subject to a separate regime of exceptions and public interest considerations.

3. Handling requests

Requests that cannot be answered promptly as routine business, or which clearly invoke FOI or EIR rights, should be forwarded to the School Business Manager. The school will log the request, identify whether the information is held, locate relevant records and consider whether any exemption or exception applies.

The Headteacher and, where appropriate, the Chair of Governors will be consulted on significant or sensitive requests, particularly where a public interest test is required. Advice will be sought from the DPO where necessary.

4. Timescales

The school will respond to FOI and EIR requests within the statutory timescales, normally within 20 working days. Where the legislation permits additional time, the requester will be informed.

5. Fees

The school may charge fees only where permitted by the relevant legislation and regulations. Where a charge applies, the requester will be informed before the information is supplied.

6. Internal review and ICO

A requester who is dissatisfied with the handling of an FOI or EIR request may ask for an internal review. The review will be carried out by an appropriate person who was not responsible for the original decision, wherever practicable. If the requester remains dissatisfied, they may complain to the ICO.

7. Copyright and re-use

Disclosure under FOI or EIR does not automatically give permission to re-use information in a way that infringes copyright or other intellectual property rights. Where relevant, the school will draw this to the requester's attention.

Key external guidance

This policy has been reviewed with reference to current Department for Education guidance on data protection in schools, including the Data (Use and Access) Act 2025, filtering and monitoring, generative AI and EdTech procurement, and current Information Commissioner's Office guidance.

Department for Education – Data protection in schools: https://www.gov.uk/guidance/data-protection-in-schools

Information Commissioner's Office: https://ico.org.uk/