THE VINE CHRISTIAN SCHOOL

Data Protection Policy

16 June 2025

About This Document

Policy Period	2025 - 2026
Policy Adopted by Governors	January 2019
Last Policy Review	16 June 2025
Next Policy Review	September 2026

History

Version	Date	Name	Description
0.1	Jan 2019	René Esterhuizen, Clerk to Trustees	First release. DRAFT
1.0	Jan 2019	School Governors	Approved and adopted.
1.1	21 May 2021	School Governors	Reviewed and approved.
1.2	22 Sep 2021	School Governors	Reviewed and approved.
1.3	15 Sep 2022	School Governors	Reviewed and approved.
1.4	19 Aug 2023	School Governors	Reviewed and approved.
1.5	16 May 2024	School Governors	Reviewed and approved.
1.6	9 Sep 2024	School Governors	Reviewed and approved.
1.7	16 Jun 2025	René Esterhuizen	Reviewed, no changes.

Contents

1. Purpose

1.1. This policy incorporates the following procedures and guidance:

i. School Data Breach Procedure

ii. Data Protection Act 2018

1.2. This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018, and other legislation. It will apply to information regardless of the way it is collected, used, recorded, stored, and destroyed, and irrespective of whether it is held in paper files or electronically.

i. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection- regulation-UK GDPR/principles/

1.3. The Vine Christian School collects and uses personal information about staff, pupils, parents, governors, trustees, and other individuals who come into contact with the school. This information is gathered to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

1.4. This policy statement applies to all School Governors, Trustees, employees, volunteers, other staff, and individuals about whom the school processes personal information, as well as other partners and companies with which the school undertakes its business. All staff involved with collecting, processing, and disclosing personal data will be aware of their duties and responsibilities by adhering to these guidelines.

2. Data Controllers

2.1. Schools are 'Data Controllers' under the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 and must 'Notify' (register with), the Information Commissioner's Office on the following website, unless exempt:

i. https://ico.org.uk/for-organisations/register/

2.2. Review frequency: At least every two years (Registration is annual).

2.3. Approval: The Governing body is free to determine how to implement. Further information is on the Information Commissioner's Office website:

i. https://ico.org.uk/

2.4. The Registration/Self-Assessment (to find out if we are exempt can be found at:

i. https://ico.org.uk/for-organisation/data-protection-fee/self-assessment/

2.5. Legislation: The Data Protection Act 2018 (with consideration to the six data protection principles appearing in Chapter 2):

i. https://www.legislation.gov.uk/ukpga/2018/12/part/4/chapter/2/enacted

2.6. We at The Vine Christian School are the Data Controller for the purpose of the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018.

2.7. The Vine Christian School is required under Data Protection legislation to comply with essential good practice in respect to the information collected here and to manage it securely. All records will be kept confidential. We will only pass on information to third parties if we have received permission to do so. The individuals who are the subject of the information or who have parental/guardian responsibility are generally entitled to see the information and are encouraged to help keep the information up to date. This information will be used for educational, planning, or managerial purposes and to keep parents and staff informed of school events and dates.

2.8. Schools also have a duty to issue a Fair Processing Notice to all pupils/parents; this summarises the information held on pupils, why it is held and the other parties to whom it may be passed on.

2.9. Under Article 6 of the UK GDPR, the lawful basis for processing school workforce, parents and governors' information is to fulfil legal, contractual obligations and other legitimate interests. For data collection purposes (Departmental Censuses) provisions of the Education Act 1996 will be followed. Consent will be requested for specific activities (at the time of activity) where activities require processing of data if deemed suitable.

3. Data Protection Officer/Lead

3.1. The Data Protection Officer/Lead in The Vine Christian School is Mr. James Neale.

4. Personal Information

4.1. Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held. The UK GDPR applies to automated personal data and manual filing systems where personal data is accessible according to specific criteria.

4.2. We need to collect and use certain types of personal information about people with whom we deal to operate. These include current, past, and prospective employees, pupils, suppliers, clients, and others we communicate with. In addition, it may be required by law to collect and use certain types of information to comply with the requirements of government departments.

4.3. This personal information must be dealt with appropriately; however, it is collected, recorded, and used – whether on paper, in a computer, or recorded on other material – and there are safeguards to ensure this in the Data Protection Act 2018. We regard the lawful and correct treatment of personal information by the school as very important to secure the successful carrying out of operations and the delivery of our services, and to maintaining confidence with those whom we deal. The school wishes to ensure that it treats personal information lawfully, correctly and in compliance with the 2018 Act.

4.4. To this end we fully endorse the obligations of the Act and adhere to the Principles of Data Protection, as enumerated in the 2018 Act.

4.5. We collect information from parents/carers and may receive information about students from their previous school. We hold this personal data and use it to:

i. Support teaching and learning.

ii. Monitor and report on progress.

iii. Provide appropriate pastoral care.

iv. Assess how well the school is doing.

4.6. This information includes contact details, attendance information, characteristics such as ethnic group, special educational needs, and any relevant medical information.

4.7. We will not give information to anyone outside the school without consent unless the law and our rules permit it.

4.8. We are required by law to pass some information to the Local Authority (LA), and the Department for Education (DfE).

4.9. If anyone would like to see a copy of the information we hold and share about them personally, then please contact the Data Protection Officer/Lead Mr. James Neale.

5. Data Protection Principles

5.1. Specifically, the Principles require that personal information shall:

i. be processed fairly and lawfully and shall not be processed unless specific conditions as set out in the 2018 Act are met.

ii. be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.

iii. be adequate, relevant, and not excessive concerning the purpose or purposes for which they are processed.

iv. be accurate and, where necessary, kept up to date.

v. not be kept for longer than is necessary for that purpose or those purposes.

vi. be processed in accordance with the rights of the data subject under the 2018 Act.

vii. be kept secure i.e., protected by an appropriate degree of security; and that:

viii. be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction, or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

6. Our Commitment

6.1. The school will, through appropriate management and application of criteria and controls:

i. Observe fully conditions regarding the fair collection and use of information.

ii. Meet its legal obligations to specify the purposes for which information is used.

iii. Collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs, or to comply with any legal requirements.

iv. Ensure the quality of information used, including its accuracy and relevancy for the purpose(s) specified.

v. Apply strict checks to determine the length of time information is held.

vi. Ensure that the rights of people about whom information is held can be fully exercised under the 2018 Act.

6.2. These include:

i. Taking appropriate technical and organisational security measures to safeguard personal information.

ii. Ensuring that personal information is transferred abroad with suitable safeguards.

7. Compliance

7.1. In addition, the school will take steps to ensure that:

i. There is an understanding that everyone is personally responsible for Data Protection within the school.

ii. Everyone managing and handling personal information understands that they are responsible for following good data protection practice.

iii. Everyone managing and handling personal information is appropriately supervised.

iv. Anybody wanting to make enquiries about handling personal information knows what to do.

v. Queries about handling personal information are promptly and courteously dealt with.

vi. Methods of handling personal information are regularly assessed and evaluated.

vii. It disseminates to employees, information on good practice in regarding handling, using, and storing personal information.

8. Procedures/Methods

8.1. All staff (employed and voluntary) must take appropriate technical and organisational security measures to safeguard personal information.

8.2. Personal information must be protected from unauthorised or accidental disclosure.

8.3. Staff are responsible for ensuring that the personal information which they use during their role is appropriately secured and any concerns regarding its security are brought to the attention of the Data Protection Officer/Lead. This includes ensuring that personal information is removed from desks out of hours and sensitive personal information is locked in filing cabinets or desks when not in use.

8.4. The Data Protection Officer/Lead is responsible for ensuring that personal information when in use is only accessible by those with a need and right to access it to perform their function or role.

8.5. Staff must respect the privacy of the subject of the personal information they are handling by treating personal information about others with the utmost care and attention.

8.6. Careful consideration must be given to the transmission of Personal Data. Personal data must not normally be transmitted externally via email. Although it is acceptable to transmit personal data internally, you should consider choosing another method if possible.

8.7. Personal information must be disposed of safely and securely.

8.8. Documents and any storage media containing input to and output from systems (paper or electronic) detailing personal information must be held, transported, and disposed of with due regard to its sensitivity.

8.9. Where information is particularly sensitive it may be appropriate to ensure that the information is shredded on site.

8.10. Publishing personal information on the internet would make it available internationally therefore personal information must not be published on the internet, other that the names and work contact details of some employees and members if appropriate to their role.

9. Privacy Policies

9.1. We provide child-friendly privacy information using engaging formats like diagrams, comic strips, and videos to make it easier for children to understand their rights.

9.2. We introduce the idea of data privacy within wider online safety lessons, using age-appropriate language to ensure understanding and encourage questions.

9.3. We use simple language in our privacy notices, with shorter versions available for quick reading and links to more detailed information, if needed.

9.4. Children have the right to know how their data is used and shared. We provide this information in clear, simple language so it is easy to understand.

10. Use of Images

10.1. An ‘image’ is personal data if the subject can be identified and therefore the Data Protection Act 2018 principles apply. Photographs, videos, and webcams of clearly identifiable people must not be processed for any other purpose than that which it was originally collected for.

10.2. The school will get the permission for all use of photographic images and video footage by ensuring parents sign a consent form when a child is admitted to the school.

10.3. Images taken (including video) at an event attended by others, such as a sports event or assemblies are only to be used for personal viewing (or if taken by the school the purpose for which it is being collected) and the person in charge should address everyone to alert them to this and give them the opportunity to move away.

10.4. In the case of children, the purpose for which the images are to be used should be covered by a school consent form, but if not a separate, signed parental consent form for each child will be obtained for that specific project.

10.5. Photographic/video images used on a website will not include the child's first name in the accompanying text or photo caption. If a child is named in the text, a photograph will not be included unless specific parental consent has been given.

10.6. Photographs may be taken for security reasons to enable access to buildings for example and this is a legitimate business purpose for processing personal data.

11. Inappropriate and Unacceptable Use

11.1. Unacceptable use includes:

i. unauthorised access of personal information

ii. unauthorised disclosure of personal information

iii. unauthorised use of personal information (e.g., not for reason given to access personal information)

iv. non-adherence to the school's information-sharing protocol

v. unauthorised deletion

11.2. Employee or customer personal information must not be used for:

i. any illegal purpose.

ii. any purpose which is inappropriate in the workplace by virtue of the fact that it may cause embarrassment or distress to another person or may bring the school into disrepute.

iii. any purpose which is not in accordance with the staff member's role or job description.

11.3. This is not an exhaustive list. Cases where staff do not comply with this Policy or legislation will be dealt with under the Disciplinary Procedure and, depending on the circumstances; non-compliance may be deemed an act of gross misconduct.

11.4. Staff are required to notify an appropriate person, if they become aware, or suspect that personal information is being misused or handled inappropriately.

12. Subject Access

12.1. Staff have a right to access their own personal information. Requests by individuals for copies of their own information must be made in writing and supported by original proof of identity – copies are not acceptable (passport, driving licence, birth, or marriage certificate). Parents may request their child's information by giving proof of their own identity, and proof of parental responsibility e.g., birth certificate naming them as the parent. The decision on whether to release information, in the event of a request will be that of the Data Protection Officer/Lead. Subject Access requests will be supplied within 15 school days for students and 30 days for staff. Where an investigation of a member of staff has commenced and Subject Access has been requested by them, the processing should be done as quickly as possible.

13. Complaints

13.1. If a complaint is received regarding Subject Access, complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator)

14. Training

14.1. All staff will be trained on Data Protection on induction to the school by using this policy and online training. The Data Protection Officer/Lead will ensure staff are kept up to date with any changes in legislation.

15. General Statement

15.1. The school is committed to maintaining the above principles always. Therefore, the school will:

i. Inform individuals why the information is being collected when it is collected.

ii. Inform individuals when their information is shared, and why and with whom it was shared.

iii. Check the quality and the accuracy of the information it holds.

iv. Ensure that information is not retained for longer than is necessary.

v. Ensure that when obsolete information is destroyed that it is done so appropriately and securely.

vi. Ensure that clear and robust safeguards are in place to protect personal information from loss, theft, and unauthorised disclosure, irrespective of the format in which it is recorded.

vii. Share information with others only when it is legally appropriate to do so.

viii. Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests.

ix. Ensure our staff are aware of and understand our policies and procedures.

16. School Data Breach Procedure

16.1. Important Note

i. This procedure has been produced based on current UK General Data Protection Regulations (UK GDPR) information. As further updates are released this procedure may be updated to reflect the changes.

17. Policy Statement

17.1. The Vine Christian School holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as

soon as possible. This procedure applies to all personal and sensitive data held by The Vine Christian School and all school staff, Governors and Trustees, volunteers, and contractors, referred to herein after as 'staff'.

18. Purpose

18.1. This breach procedure sets out the course of action to be followed by all staff at The Vine Christian School if a data protection breach takes place.

19. Legal Context

19.1. Article 33 of the General Data Protection Regulations

19.2. Notification of a personal data breach to the Commissioner

i. In the case of a personal data breach, the Data Controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Commissioner, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification under this paragraph is not made within 72 hours, it shall be accompanied by reasons for the delay.

ii. The processor shall notify the Data Controller without undue delay after becoming aware of a personal data breach.

iii. The notification referred to in paragraph 1 shall at least:

a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned.

b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained.

c) describe the likely consequences of the personal data breach.

d) describe the measures taken or proposed to be taken by the Data Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

e) Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

f) The Data Controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the Commissioner to verify compliance with this Article.

20. Types of Breach

20.1. Data protection breaches could be caused by several factors. Several examples are shown below:

i. Loss or theft of pupil, staff, or governing body data and/ or equipment on which data is stored.

ii. Inappropriate access controls allowing unauthorised use.

iii. Equipment Failure.

iv. Poor data destruction procedures.

v. Human Error.

vi. Cyber-attack.

vii. Hacking.

21. Managing a Data Breach

21.1. In the event that the school identifies or is notified of a personal data breach, the following steps should be followed:

i. The person who discovers/receives a report of a breach must inform The Data Protection Officer / Lead or, in their absence, the Head Teacher. If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.

ii. The Data Protection Officer / Lead or nominated person must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as the IT technician.

iii. The Data Protection Officer / Lead or nominated person must inform the Chair of Governors and Trustees as soon as possible. As a registered Data Controller, it is the school's responsibility to take the appropriate action and conduct any investigation.

iv. The Data Protection Officer / Lead or nominated person must also consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future. In such instances, advice from the school's legal support should be obtained.

21.2. The Data Protection Officer / Lead or nominated person must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

i. Attempting to recover lost equipment.

ii. Contacting the relevant County Council Departments, so that they are prepared for any potentially inappropriate enquiries ('phishing') for further information on the individual or individuals concerned. Consideration should be given to a global email to all school staff. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer's name and contact details if possible and confirm that they will ring the individual, making the enquiry, back. Whatever the outcome of the call, it should be reported immediately by the Data Protection Officer / Lead.

iii. The use of back-ups to restore lost/damaged/stolen data.

iv. If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.

v. If the data breach includes any entry codes or IT system passwords, then these must be changed immediately, and the relevant agencies and members of staff informed.

22. Investigation

22.1. In most cases, the next stage would be for the Data Protection Officer / Lead to fully investigate the breach. The Data Protection Officer / Lead should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation should consider:

i. The type of data.

ii. Its sensitivity.

iii. What protections were in place (e.g., encryption).

iv. What has happened to the data?

v. Whether the data could be put to any illegal or inappropriate use.

vi. How many people are affected?

vii. What type of people have been affected (pupils, staff members, suppliers etc) and whether there are wider consequences to the breach.

22.2. A clear record should be made of the nature of the breach and the actions taken to mitigate it. The investigation should be completed as a matter of urgency due to the requirements to report notifiable personal data breaches to the Information Commissioner's Office. A more detailed review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

23. Notification

23.1. Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an initial investigation has taken place. The Data Protection Officer / Lead should, after seeking expert or legal advice, decide whether anyone is notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) must be notified within 72 hours of the breach. Every incident should be considered on a case-by-case basis.

23.2. When notifying individuals, give specific and clear advice on what they can do to protect themselves and what the school is able to do to help them. You should also give them the opportunity to make a formal complaint if they wish (see the School's Complaints Procedure). The notification should include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to mitigate the risks posed by the breach.

24. Review and Evaluation

24.1. Once the initial aftermath of the breach is over, the Data Protection Officer / Lead should fully review both the causes of the breach and the effectiveness of the response to it. It should be reported to the next available Senior Management Team and **full** Governors and Trustees meeting for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put correct these. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

25. Implementation

25.1. The Data Protection Officer / Lead should ensure that staff are aware of the School's Data Protection policy and its requirements including this breach procedure. This should be undertaken as part of induction, supervision, and ongoing training. If staff have any queries in relation to the School's Data Protection policy and associated procedures, they should discuss this with the Data Protection Officer / Lead or the nominated person.

Appendix 1

26. Actioning a Subject Access Request

26.1. Requests for information must be made in writing, which includes email, and be addressed to the Headteacher. If the initial request does not clearly identify the information required, then further enquiries will be made.

26.2. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:

i. Passport

ii. Driving licence

iii. Utility bills with the current address

iv. Birth/marriage certificate

v. P45/P60

vi. Credit card or mortgage statement

This list is not exhaustive.

26.3. Any individual has the right of access to information held about them. However, with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the 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, most subject access requests from parents of students at this school will not be granted without the express permission of the student. Parents at this school do not have automatic right to access their child's educational record. The school will decide on a case-by-case basis whether to grant such requests, bearing in mind guidance issued from time to time from the Information Commissioner's Office.

26.4. The school may make a charge for the provision of information, dependent upon the following:

i. Should the information requested contain the educational record then the amount charged will be dependent upon the number of pages provided.

ii. Should the information requested be personal information that does not include any information contained within educational records, schools can charge up to £10 to provide it.

iii. If the information requested is only the educational record, viewing will be free, but a charge not exceeding the cost of copying the information can be made by the Headteacher.

26.5. The response time for subject access requests for all or part of the student's educational record, once officially received, is 15 school days. If the subject access request does not relate to the educational record, we will respond within 40 days (not working or school days but calendar days, irrespective of school holiday periods). However, the 40 days will not commence until after the receipt of fees or clarification of information sought.

26.6. The Data Protection Act 2018 allows exemptions as to the provision of some information; therefore, all information will be reviewed prior to disclosure.

26.7. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the 40-day statutory timescale.

26.8. Any information which may cause serious harm to the physical or mental health or emotional condition of the student, or another should not be disclosed, nor should information that would reveal the child is at risk of abuse, or information relating to court proceedings.

26.9. If there are concerns over the disclosure of information, then additional advice should be sought.

26.10. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained to establish, if a complaint is made, what was redacted and why.

26.11. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

26.12. Information can be provided at the school with a member of staff on hand to help and explain matters if requested or provided face-to-face handover. The views of the applicant should be considered when considering the method of delivery. If postal systems must be used, then registered/recorded mail must be used.

27. Complaints

27.1. Complaints about the above procedures should be made to the Chair of the Governing Body who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaint procedure.

27.2. Complaints which are not appropriate to be dealt with through the school's complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

28. Contacts

28.1. If you have any queries or concerns regarding these policies/procedures, then please contact the Headteacher.

28.2. Further advice information can be obtained from the Information Commissioner's Office, www.ico.gov.uk or telephone 0303 123 1113.