



## **DATA PROTECTION POLICY**

### **INCLUDING SCHOOL PRIVACY NOTICE**

Data Protection Act 1998

Schools are 'Data Controllers' under the Data Protection Act 1998 and must 'Notify' (register with), the Information Commissioner's Office on the following website:

<https://ico.org.uk/for-organisations/register/>

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

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

<https://ico.org.uk/>

Legislation: The Data Protection Act 1998 (with consideration to the eight data protection principles appearing in Schedule 1):

<http://www.legislation.gov.uk/uk/a/1998/29/contents>

This policy statement applies to all School Governors, Trustees, employees, staff and volunteers, and individuals about whom the School processes personal information, as well as other partners and companies with which the School undertakes its business.

We at The Vine Christian School are the Data Controller for the purposes of the Data Protection Act.

The Vine Christian School is required under Data Protection legislation to comply with essential good practice in respect of the information collected here and to manage it securely. All records will be kept confidential. We will not pass on information to any third parties unless 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.

## **SCOPE:**

- 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, students, suppliers, clients, and others with whom we communicate. In addition, it may be required by law to collect and use certain types of information to comply with the requirements of government departments.
- This personal information must be dealt with properly 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 1998. 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 1998 Act.

To this end we fully endorse the obligations of the Act and adhere to the Principles of data protection, as enumerated in the 1998 Act.

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:

- Support teaching and learning,
- Monitor and report on progress,
- Provide appropriate pastoral care,
- Assess how well the school is doing,

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

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

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

If anyone would like to see a copy of the information we hold and share about them personally, then please contact the Senior Administrator.

## **DATA PROTECTION PRINCIPLES:**

- Specifically, the Principles that require personal information:
- shall be processed fairly and lawfully and shall not be processed unless specific conditions as set out in the 1998 Act are met;
- shall 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;
- shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed, be accurate and, where necessary, kept up to date and not be kept for longer than is necessary for that purpose or those purposes, be processed in accordance with the rights of the data subject under the 1998 Act, and that,
- 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.
- information shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

## **OUR COMMITMENT:**

The School will, through appropriate management and application of criteria and controls:

- ensure the fair collection and use of information, meet its legal obligations to specify the purposes for which information is used.
- 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.
- ensure the quality of information used, including its accuracy and relevancy for the purpose(s) specified, apply strict checks to determine the length of time information is held.
- ensure that the rights of people about whom information is held can be fully exercised under the 1998 Act. These include:
- the right to be informed that processing is being undertaken, the right of access to one's personal information, the right to prevent processing in certain circumstances, the right to correct, block or erase information which is regarded as erroneous.
- take appropriate technical and organisational security measures to safeguard personal information and ensure that personal information is not transferred abroad without suitable safeguards.

## **COMPLIANCE:**

In addition, the School will take steps to ensure that:

- there is an understanding that everyone is personally responsible for Data Protection within the school.
- everyone managing and handling personal information understands that they are responsible for following good data protection practice, that everyone managing and handling personal information is appropriately supervised, and anybody wanting to make enquiries about handling personal information knows what to do.
- Queries about handling personal information are promptly and courteously dealt with, and methods of handling personal information are clearly described.
- methods of handling personal information are regularly assessed and evaluated, and it disseminates to employees, information on good practice in respect of handling, using, and storing personal information.

## **PROCEDURES:**

- All staff (employed and voluntary) must take appropriate technical and organisational security measures to safeguard personal information.
- Personal information must be protected from unauthorised or accidental disclosure. 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 Headteacher. 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.
- The Headteacher 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.
- Staff must respect the privacy of the subject of the personal information they are handling by treating personal information about others as we would expect information about ourselves to be treated.
- Careful consideration must be given to the transmitting 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.
- Personal information must be disposed of safely and securely.
- 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.
- Where information is particularly sensitive it may be appropriate to ensure that the information is shredded on site.

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

### **USE OF IMAGES:**

- An 'image' is personal data if the subject can be identified and therefore the Data Protection Act 1998 principles apply. Photographs, videos and webcams of clearly identifiable people must not be processed for any other purpose other than that what it was originally collected for. 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.
- 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.
- 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 project.
- 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.
- 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.

### **INAPPROPRIATE AND UNACCEPTABLE USE:**

Unacceptable use includes:

- unauthorised access of personal information, unauthorised disclosure of personal information, unauthorised use of personal information (e.g. not for reason given to access personal information) non- adherence to the school's information-sharing protocol, unauthorised deletion.
- Employee or customer personal information must not be used for:
- any illegal purpose, any purpose which is inappropriate in the workplace where it may cause embarrassment or distress to another person or may bring the school into disrepute, any purpose which is not in accordance with the staff member's role or job description.

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.

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

### **SUBJECT ACCESS:**

Staff have a right to access their own personal information. Requests by individuals for copies of their own information must be made in writing 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 Headteacher. Subject Access requests will be supplied within 15 school days for students and 40 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. If a complaint is received regarding Subject Access, the Complaints Procedure will be followed.

### **TRAINING:**

All staff will be trained on Data Protection on induction to the school by using this policy, and the Headteacher will ensure staff are kept up to date with any changes in legislation.

### **REVIEW:**

This policy will be updated as necessary (at least once every two years) to reflect best practice in data management, security, and control to ensure compliance with any changes or amendments made to the Data Protection Act 1998.

Policy Adopted by Governors/Trustees on: 7 September 2018

Policy Due for Review: September 2019

