St. Anne's Church of England VA Primary School

DATA PROTECTION POLICY

This policy should be taken and used as part of St Anne's Church of England School overall strategy and implemented within the context of our vision, instrument of governance, aims and values as a Church of England School. It is the intention of the Governors that St Anne's CofE VA Primary School will provide education within a Christian ethos to the local community; however this school welcomes opportunities to work within the local community with groups of other faiths and of no faith.

Why we have it

St Anne's Church of England VA Primary School (St Anne's) collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order 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.

Schools have a duty to be registered, as Data Controllers, with the Information Commissioners Office [ICO] detailing the information held and its use. These details are then available on the ICO's website. Schools also have a duty to issue a Fair Processing Notice (also known as Privacy Notices) 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. We also have a Staff Privacy Notice explaining how we will use their personal information.

Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities we will collect, store and process personal data about our students, staff (which will include permanent, temporary employees and volunteer staff, consultants and contractors), parents/carers and clients, and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 1998 and other related legislation. Schools and their employees should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature. It is the responsibility of all members of the school community to take care when handling, using or transferring personal data and to ensure that it cannot be accessed by anyone who does not:

- have permission to access that data
- need to have access to that data.

Data breaches can have serious effects on individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office - for the school and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination and may require separate handling, for example on the form of encryption.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance (where relevant from the Local Authority).

Data users are obliged to comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary action.

This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

This policy does not form part of any employee's contract of employment and may be amended at any time.

This policy has been approved by the Governing Body. It sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

Definition of data protection terms
Data is information which is stored electronically, on a computer, or in certain paper-based filing systems.

Data subjects include all living individuals about whom we hold personal data.

Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour. The types of personal data that St Anne's CEVA Primary School (We) may be required to handle include information about current, past and prospective staff (as defined above), students, parents/carers and others that we communicate with. The personal data, which may be held on paper or on computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 1998 (the Act) and other regulations.

The **Data Protection Compliance Manager** is responsible for ensuring compliance with the Act and with this policy. That post is held by the Headteacher, Lisa Dadds. Any questions about the operation of this policy or any concerns that the policy has not been

followed should be referred in the first instance to the Data Protection Compliance Manager.

Data controllers are the people who or the organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Act. We are the data controller of all personal data used in our business for our own commercial purposes.

Data users are those of our staff (which means our employees, governors, contractors and consultants) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

Data processors include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions. This includes our payroll service agents, pension providers and legal and professional advisors. Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

Data protection principles

Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

- Processed fairly and lawfully.
- Processed for limited purposes and in an appropriate way.
- Adequate, relevant and not excessive for the purpose.
- Accurate.
- Not kept longer than necessary for the purpose.
- Processed in line with data subjects' rights.
- Secure.
- Not transferred to people or organisations situated in countries without adequate protection.

Fair and lawful processing

The Act is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in the Act. These include, among other things, the data subject's consent to the processing, or that the processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed.

When processing personal data as data controllers in the course of our business, we will ensure that those requirements are met.

Processing for limited purposes
In the course of our business, we will collect and process personal data. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, parents/carers/family members, health professionals, business partners, regulatory authorities (eg. Disclosure & Barring Service, Police, social services, local authority), previous employers, credit reference agencies and others).

We will only process personal/sensitive personal data for purposes specifically permitted by the Act, including but not limited to:

- The provision of education
- Employment – effective human resource management – recruitment (vetting and verifying applications), equal opportunities monitoring, the management of grievance and disciplinary matters, employment reference provision, performance management
- Statutory obligations – reporting and monitoring obligations, recruitment (e.g. Keeping Children Safe in Education 2015), performance management (teachers - Education (School Teachers' Appraisal) (England) Regulations 2012)
- Health management – sickness absence monitoring, occupational health referrals, early/ill health retirement applications, special educational needs management
- Financial – payroll, pensions, insurances, funding applications.

Adequate, relevant and non-excessive processing
We will only collect personal data to the extent that it is required for the specific purpose.

Accurate data we will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

Timely processing we will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

Processing in line with data subject's rights We will process all personal data in line with data subjects' rights, in particular their right to:

- Request access to any data held about them by a data controller.
- Prevent the processing of their data for direct-marketing purposes.
- Ask to have inaccurate data amended (see also clause 8).
- Prevent processing that is likely to cause damage or distress to themselves or anyone else.

Data security

We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

- Confidentiality means that only people who are authorised to use the data can access it.
- Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.
- Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on the School's central computer system instead of individual PCs.

Security procedures include:

- Entry controls. Any stranger seen in entry-controlled areas should be reported.
- Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
- Methods of disposal. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.
- Passwords. All staff will have individual, confidential passwords for access to their IT and communication equipment, memory sticks, software, cloud based storage and electronic files containing personal data.
- Encryption. All staff will be encouraged to: - encrypt files containing personal data before transmitting them electronically outside of the School network including cloud storage; - encrypt and password protect the contents of any memory stick containing personal data.

- Equipment. Data users must ensure that individual monitors do not show confidential information to passers-by and that they lock/log off from their PC when it is left unattended.
- Security. All staff will be discouraged from leaving their laptop computers, school files/work unattended in their vehicles or on public transport, where there is an increased risk of theft.
- Cloud service providers. We conduct a privacy impact assessment to include ensuring that we obtain a contract and/or data processing agreement which confirms the cloud service provider complies with the requirements of the DPA.
- Confidentiality agreements. We will require all staff, consultants, contractors and volunteers who have access to personal data held by the School to enter into contractual agreements with the School to protect and preserve confidentiality and to comply with the terms of this Data Protection Policy.

Transferring personal data to a country outside the EEA

We may transfer any personal data we hold to a country outside the European Economic Area ("EEA"), provided that one of the following conditions applies:

- The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms.
- The data subject has given his consent.
- The transfer is necessary for one of the reasons set out in the Act, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.
- The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.
- The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

Subject to the requirements in Data Security, personal data we hold may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. That staff maybe engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

Disclosure and sharing of personal information

We may share personal data for the purposes of staff secondment and their provision of health and safety services to the School.

We may also disclose personal data we hold to third parties:

- such as another school, college or university which requires information about the data subject’s education, achievements or needs;
- in the event that we acquire any business or assets, in which case we may disclose personal data we hold to the owner of such business or assets;

- if we or substantially all of our assets are acquired by a third party, in which case personal data we hold will be one of the transferred assets;
- such as the provider of hosted/online educational software or business services where the provision of personal data supports login/access arrangements (for example, Google, Microsoft) (Appendix A);
- for the purposes of obtaining professional advice (for example, legal, educational, health and welfare advice) for ourselves and/or the data subject;
- if we are under a duty to disclose or share a data subject's personal data in order to comply with any legal or regulatory obligation; for example, to:
    - OfSTED
    - Police, Disclosure & Barring Service, National College for Teaching & Leadership
    - Local Authority
    - Children's and Social Services
    - HMRC, Department of Work & Pensions, Avon Pension Fund/Local Government Pension Scheme.
    - Occupational health service providers, employee assistance programme providers • Education Funding Agency;
    - Health Authority;
- in order to enforce or apply any contract with the data subject; and
- to protect our rights, property, or safety of our employees, students, parents/carers or others.

We will, wherever possible, prior to disclosing any personal data, obtain written confirmation from the third party that it will:

- not itself share such personal data with any third party;
- keep the personal data confidential;
- comply with the requirements of this policy and any additional relevant provisions of the Data Protection Act.

Dealing with subject access requests

Data subjects must make a formal request for information we hold about them. This must be made in writing and submitted to the School's Main Office, marked for the attention of the Data Protection Compliance Officer.

Provided that there is sufficient information to process the request, an entry will be made in the Subject Access log book, showing the date of receipt, the data subject's name, the name and address of the requester (if different), the type of data required (e.g. Student Record, Personnel Record), and the planned date of supplying the information (normally not more than 40 days from the request date).

Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will be the date on which sufficient information has been provided.

The identity of the requestor must be established before the disclosure of any information, and checks should be carried out regarding proof of relationship to the student. Evidence of identity can be established by requesting production of (this list is not exhaustive): passport, driving licence, utility bills with current address, Birth / Marriage Certificate, P45/P60, Credit Card or Mortgage statement.

Where a request for subject access is received from a student, the School's policy is that:

- The requested information will be given directly to the student, unless it is clear that the student does not understand the nature of the request;
- Requests from students who do not appear to understand the nature of the request will be referred to their parents or carers; and
- Requests made from parents or carers in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting parent or carer.
- In the case of any written request from a parent/carer regarding their own child's record, access to the record will be provided within 15 school days in accordance with the current Education (Pupil Information) Regulations 2005.

When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

- We will check the caller's identity to make sure that information is only given to a person who is entitled to it.
- We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

Our employees will refer a request to the Data Protection Compliance Manager for assistance in difficult situations. Employees should not be bullied into disclosing personal information.

Photographs/video images

The School uses photographs and video images of students (which may or may not be accompanied by their forename) for the purposes of:

- education, teaching and learning;
- communication and information sharing;
- student recognition and reward;
- marketing and publicity (including but not limited to, news and press reporting, school prospectuses, webcasts/podcasts and annual reports, banner displays and hoardings)
- security and staff and student safety.

When families join our school parents/carers are asked whether they object to the School (and thereby its authorised staff) taking and using photographs and video

images of their child for school related purposes. The School assumes that consent is granted in the absence of an objection.

The Office retains a list of those parents/carers who have objected to or who have placed any restrictions or limitations on the use of images of their child.

Staff should familiarise themselves with the names of the students on that list. It is a disciplinary offence to use, post or publish a photograph or video image of a student contrary to the instructions of their parent/carer.

Changes to this policy
We reserve the right to change this policy at any time. Where appropriate, we will notify data subjects of those changes by mail or email.

General Statement
The school will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for. Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay. All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing". (see Privacy Notice section below).

The school's Senior Information Risk Officer (SIRO) is Lisa Dadds. This person will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's information risk policy and risk assessment
- appoint the Information Asset Owners (IAOs)

The school's Information Asset Owners (IAOs) are Lisa Dadds and Helen Burge. They are responsible for the various types of data being held (eg pupil / student information / staff information / assessment data etc). The IAOs will manage and address risks to the information and will understand:

- what information is held, for how long and for what purpose
- how information has been amended or added to over time
- who has access to protected data and why.
- how and when that data will be securely destroyed

Everyone in the school has the responsibility for handling protected or sensitive data in a safe and secure manner. Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

Privacy Notice for Parents/Carers (Fair Processing Notice)
In order to comply with the fair processing requirements of the DPA, the school will inform parents/carers of all pupils/students of the data they collect, process and hold on

the pupils / students, the purposes for which the data is held and the third parties (e.g. LA, DfE, etc) to whom it may be passed including if this is outside of the European Economic Area (EEA). This privacy notice will be passed to parents/carers via the website. Parents/carers of young people who are new to the school will be signposted via the website or can ask for a printed copy and this will be advertised in our newsletter.

Training and Support

All staff will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through:

- induction training for new staff
- staff meetings / briefings
- day to day support and guidance from our Information Asset Owners - Lisa Dadds and Helen Burge.

Risk Assessment

Information risk assessments will be carried out by Information Asset Owners to establish the security measures already in place and whether they are the most appropriate. The risk assessment will involve:

- recognizing the risks that are present;
- judging the level of the risks (both the likelihood and consequences);
- prioritising the risks;
- mitigating those risks.

Impact levels and protective marking

Most student / pupil or staff personal data that is used within educational institutions will come under the OFFICIAL-SENSITIVE classification. However some, e.g. the home address of a child (or vulnerable adult) at risk will me be more SENSITIVE.

Combining more and more individual data elements together in a report or database increases the risks associated with a breach.

Archived material will be labeled with a 'shred by' date for confidential shredding. E.g. Pupil data, governors minutes, finance information etc.

CCTV

We have Closed Circuit Television (CCTV) at our West Wick campus for the purposes of security and safety and, to monitor that student and staff behaviour and conduct complies with our policies and procedures.

The School has a CCTV Usage Policy, a copy of which is available from the School website. Images recorded by the CCTV system are stored, processed and destroyed in accordance with the "ICO Code of Practice 2015 for surveillance cameras and personal information".

Secure storage of and access to data
The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user and through named staff members. Members of staff will not, as a matter of course, be granted access to the whole management information system.

All users will use strong passwords which must be changed regularly. User passwords must never be shared. See Password Policy.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock at five minutes.

Personal data can only be stored on school equipment (this includes computers and portable storage media) Private equipment (i.e. owned by the users) must not be used for the storage of personal data.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected;
- the device must be password protected and encrypted;
- the device must have approved virus and malware checking software;
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

All paper based OFFICIAL-SENSITIVE material must be held in lockable storage.

The school recognises that under Section 7 of the DPA, http://www.legislation.gov.uk/ukpga/1998/29/section/7 data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

Secure transfer of data and access out of school
The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location;
- users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (eg family members) when out of school;
- when restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform;
- if secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location;
- users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software;
- particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event. (NB to carry encrypted material is illegal in some countries).

Destruction of data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance, and other media must be shredded, incinerated or otherwise disintegrated for data.

Audit logging/ Reporting/ Incident Handling

It is good practice, as recommended in the "Data Handling Procedures in Government" document that the activities of data users, in respect of electronically held personal data, will be logged and these logs will be monitored by responsible individuals.

The audit logs will be kept to provide evidence of accidental or deliberate data security breaches – including loss of protected data or breaches of an acceptable use policy, for example.

The school is working towards a policy for reporting, managing and recovering from information risk incidents, which establishes:

- a "responsible person" for each incident;

- a communications plan, including escalation procedures;
- and results in a plan of action for rapid resolution;
- a plan of action of non-recurrence and further awareness raising.

All significant information and security incidents must be reported through the SIRO to the Information Commissioner's Office based upon the local incident handling policy and communication plan.

The Senior Leadership Team and Governors at St Anne's must comply fully with the requirements and principles of the "Data Protection Act of 1998".

Confirmation the Data Protection Policy in respect of St. Anne's Church of England VA Primary School has been discussed by the Governing Body.

Signed by:

Chair of Governors: .....……. Date: .....

Head teacher: ..... …….....Date: ….....

Agreed at the Governing Body Meeting on:

Guidance from SWGFL [South West Grid for Learning] on the use of technologies and protective marking

	The information	The technology	Notes on Protect Markings (Impact Level)
School life & events	School terms, holidays, training days, the curriculum, extra-curricular activities, events, displays of pupils work, lunchtime menus, extended services, parent consultation events	Common practice is to use publically accessible technology such as school websites or portal, emailed newsletters, subscription text services	Most of this information will fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.
Learning & achievement	Individual pupil / student academic, social and behavioural achievements, progress with learning, learning behaviour, how parents can support their child's learning, assessments, attainment, attendance, individual and personalised curriculum and educational needs.	Typically schools will make information available by parents logging on to a system that provides them with appropriately secure access, such as a Learning Platform or portal, or by communication to a personal device or email account belonging to the parent.	Most of this information will fall into the PROTECT (Impact Level 2) category. There may be students/ pupils whose personal data requires a RESTRICTED marking (Impact Level 3) or higher. For example, the home address of a child at risk. In this case, the school may decide not to make this pupil / student record available in this way.

Messages & alerts	Attendance, behavioural, achievement, sickness, school closure, transport arrangements, and other information that it may be important to inform or contact a parent about as soon as possible. This may be particularly important when it is necessary to contact a parent concerning information that may be considered too sensitive to make available using other online means.	Email and text messaging are commonly used by schools to contact and keep parents informed. Where parents are frequently accessing information online then systems e.g. Learning Platforms or portals, might be used to alert parents to issues via "dashboards" of information, or be used to provide further detail and context.	Most of this information will fall into the PROTECT (Impact Level 1) category. However, since it is not practical to encrypt email or text messages to parents, schools should not send detailed personally identifiable information. General, anonymous alerts about schools closures or transport arrangements would fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.

Appendix A: Third parties with whom the School shares data

Organisation	**Reason for sharing Information shared**
Parentpay	To facilitate payments into school for trips, events and other purchases Student name, DOB, Gender, school admission number, Unique Pupil Number, registration group, year group, parent name, address, telephone number, meal arrangements, eligibility for free school meals, ethnicity, religion, dietary needs, meal pattern Payments secured by Payment Card Industry Data Security Standard (PCIDSS)
Secondary Schools	To ensure that Year 6 students have full information available to them during the transition to KS3 education Student name, DOB, gender, address