

# DATA PROTECTION POLICY



**St. Vincent's Catholic Primary School**

*Together through Christ we grow and learn*

**Approved by:** Marina Coleman

**Date:** 24.05.2018

**Last reviewed on:** 01.10.2018

**Next review due by:** 01.09.2020

## 1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the [General Data Protection Regulation \(GDPR\)](#) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the [Data Protection Bill](#).

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

## 2. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the [GDPR](#) and the ICO's [code of practice for subject access requests](#).

It also reflects the ICO's [code of practice](#) for the use of surveillance cameras and personal information.

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

## 3. Definitions

Term	Definition
<b>Personal data</b>	<p>Any information relating to an identified, or identifiable, individual.</p> <p>This may include the individual's:</p> <ul style="list-style-type: none"><li>Name (including initials)</li><li>Identification number</li><li>Location data</li><li>Online identifier, such as a username</li></ul> <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.</p>
<b>Special categories of personal data</b>	<p>Personal data which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none"><li>Racial or ethnic origin</li><li>Political opinions</li><li>Religious or philosophical beliefs</li><li>Trade union membership</li><li>Genetics</li><li>Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes</li><li>Health – physical or mental</li><li>Sex life or sexual orientation</li></ul>
<b>Processing</b>	<p>Anything done to personal data, such as collecting, recording, organising, structuring,</p>

	storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
<b>Data subject</b>	The identified or identifiable individual whose personal data is held or processed.
<b>Data controller</b>	A person or organisation that determines the purposes and the means of processing of personal data.
<b>Data processor</b>	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
<b>Personal data breach</b>	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

#### 4. The data controller

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

#### 5. Roles and responsibilities

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

##### 5.1 Governing board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

##### 5.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is John Pearson Hicks and is contactable via [john.pearson-hicks@london.anglican.org](mailto:john.pearson-hicks@london.anglican.org)

##### 5.3 Headteacher

The Headteacher, Marina Coleman, acts as the representative of the data controller on a day-to-day basis.

## 5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
- With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
- If they have any concerns that this policy is not being followed
- If they are unsure whether or not they have a lawful basis to use personal data in a particular way
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

## 6. Data protection principles

The GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles.

## 7. Collecting personal data

### 7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest**, and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

### 7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's [Information and Records Management Society's toolkit for schools](#).

## **8. Sharing personal data**

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this

Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

## **9. Subject access requests and other rights of individuals**

### **9.1 Subject access requests**

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter, email or fax to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address

- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO.

## 9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

## 9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

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

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

## 9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

## 10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

## 11. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's [code of practice](#) for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to Mr Normunds Cukermanis, Premises Manager.

## 12. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school. We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- Within school on notice boards, newsletters and in school magazines (such as the SVPA Auction Catalogue) etc.
- Online on our school website [www.stvincentsprimary.org.uk](http://www.stvincentsprimary.org.uk) and Vimeo (password protected)
- Outside of school by external agencies such as the school photographer, newspapers, campaigns. However specific, separate permission will be obtained for this.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

Unless instructed otherwise, a child's photo will remain on the school website for two years after the child has left St. Vincent's Year 6 (i.e. the end of August Year 8). This includes pupils who may leave the school at different point during their primary education.

See our [Parents Acceptable Use Policy](#) for more information on our use of photographs and videos (Appendix 5).

## 14. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices

- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
- For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
- For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

## **15. Data security and storage of records**

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access (please note that essential medical/ allergy information is an exception to this as names/ photographs and a summary of needs are displayed around the school to ensure the pupils are safe and treated efficiently and effectively in an emergency)
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices

Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (Refer to our Acceptable Use Policy, which all staff and governors sign annually)

Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

## **16. Disposal of records**

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

## **17. Personal data breaches**

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium

Safeguarding information being made available to an unauthorised person



The theft of a school laptop containing non-encrypted personal data about pupils

## **18. Training**

All staff and governors are provided with data protection training as part of their induction process.

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

## **19. Monitoring arrangements**

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed every 2 years and shared with the full governing board.

## **20. Links with other policies**

This data protection policy is linked to our:

- Freedom of information publication scheme
- Safeguarding and Child Protection Policy
- Online Safety Policy
- Staff Handbook
- Acceptable Use Policies for Staff, Pupils and Parents

## Appendix 1: Personal data breach procedure



### St. Vincent's Catholic Primary School

### Personal Data Breach Procedure

This procedure is based on [guidance on personal data breaches](#) produced by the ICO.

On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO

The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people

The DPO will alert the headteacher and the chair of governors

The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)

The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen

The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

- Loss of control over their data
- Discrimination
- Identify theft or fraud
- Financial loss
- Unauthorised reversal of pseudonymisation (for example, key-coding)
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school SMT Network.

Where the ICO must be notified, the DPO will do this via the ['report a breach' page of the ICO website](#) within 72 hours. As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible:
- The categories and approximate number of individuals concerned
- The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts and cause
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- Records of all breaches will be stored on the school SMT Network.

The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

## **Actions to minimise the impact of data breaches**

We will take appropriate actions to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

For example:

### **Sensitive information being disclosed via email (including safeguarding records)**

If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error

Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error

If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it

In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way

The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request

The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

## Appendix 2: Privacy Notice for Pupils and Parents



### St. Vincent's Catholic Primary School

### Privacy Notice (How we use pupil information)

Under General Data Protection Regulations (GDPR) we are obliged to inform you of the information we hold on and your child(ren), what we use it for, who we share it with, and for how long we keep it. This privacy notice (also known as a fair processing notice) aims to provide you with this information. If if, or any information linked to is unclear, please contact the school office, or the school's Data Protection Officer. Contact details for both are available at the end of this privacy notice.

We, St. Vincent's Catholic Primary School at St.Vincent Street, W1U 4DF are the Data Controller for the purposes of data protection law. As a public body as we have appointed a Data Protection Officer (DPO), John Pearson-Hicks and he is contactable via [john.pearson-hicks@london.anglican.org](mailto:john.pearson-hicks@london.anglican.org) .

#### **The categories of pupil information that we collect, hold and share include:**

- Personal information (such as name, unique pupil number and address)
- Contact details and preference (contact telephone numbers, email addresses, addresses)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information (such as data scores, tracking, and internal and external testing, targets, end of year reports)
- Medical information (any allergies, inhalers health checks, physical and mental health care)
- Behaviour information ( incident / people involved / reflection sheet and consequences including exclusions)
- Special Educational Needs information (such as EHCP's, statements, applications for support, care or support plans)
- Photographs (for internal safeguarding & security purposes, school newsletters, website)
- CCTV images (for security)

We may also hold data about pupils that we have received from other organisations, including other schools, local authorities and the Department for Education.

#### **Why we collect and use this information**

We use the pupil data:

- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral and medical care
- to assess the quality of our services
- to comply with the law regarding data sharing
- for safeguarding and pupil welfare purposes
- to administer admissions waiting lists
- to inform you about events and significant school events

#### **The lawful basis on which we use this information**

We collect and use pupil information under Article 6, and the following sub-paragraphs in the GDPR apply:

- Data subject gives consent for one or more specific purposes.
- Processing is necessary to comply with the legal obligations of the controller.
- Processing is necessary to protect the vital interests of the data subject.

- Processing is necessary for tasks in the public interest or exercise of authority vested in the controller
- (the provision of education).

Our lawful basis for collecting and processing pupil information is also further defined under Article 9, in that some of the information we process is deemed to be sensitive, or special, information and the following subparagraphs in the GDPR apply:

- The data subject has given explicit consent.
- It is necessary to fulfill the obligations of controller or of data subject.
- It is necessary to protect the vital interests of the data subject.
- Processing is carried out by a foundation or not-for-profit organisation (includes religious, political or philosophical organisations and trade unions)
- Reasons of public interest in the area of public health
- It is in the public interest

A full breakdown of the information we collect on pupils can be found on our Data Map and data Audit Log.

Where we have obtained consent to use pupils' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

Some of the reasons listed above for collecting and using pupils' personal data overlap, and there may be several grounds which justify our use of this data.

An example of how we use the information you provide is:

*The submission of the school census returns, including a set of named pupil records, is a statutory requirement on schools under Section 537A of the Education Act 1996.*

*Putting the school census on a statutory basis:*

- *means that schools do not need to obtain parental or pupil consent to the provision of information*
- *ensures schools are protected from any legal challenge that they are breaching a duty of confidence to pupils*
- *helps to ensure that returns are completed by schools*

## Collecting pupil information

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

## Storing pupil data

We hold pupil data for whilst the child remains at St. Vincent's Catholic Primary School. The file will follow the pupil when he / she leaves. However where there is a legal obligation to retain the information beyond that period, this will be done in accordance with the school's [Information and Records Management Society's toolkit for schools](#).

We have data protection policies and procedures in place, including strong organisational and technical measures, which are regularly reviewed. Further information can be found on our website.

## Who we share pupil information with

We routinely share pupil information with appropriate third parties, including:

- schools that the pupil's attend after leaving us
- our local authority
- the Department for Education (DfE)
- the Diocese of Westminster
- The pupil's family and representatives
- Educators and examining bodies
- Ofsted

- Suppliers and service providers – to enable them to provide the service we have contracted them for
- Financial organisations
- Our auditors
- Health authorities
- Security organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals
- Professional bodies
- Schools that the pupil's transfer to

## Why we share pupil information

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.

We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our pupils with our local authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

## Data collection requirements:

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.

### The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the NPD, go to <https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information>.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: <https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website: <https://www.gov.uk/government/publications/national-pupil-database-requests-received>

To contact DfE: <https://www.gov.uk/contact-dfe>

## Requesting access to your personal data

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold, through a Subject Access Request. Parents/carers can make a request with respect to their child's data where the child is not considered mature enough to understand their rights over their own data (usually under the age of 12), or where the child has provided consent. Parents also have the right to make a subject access request with respect to any personal data the school holds about them.

To make a request for your personal information, or be given access to your child's educational record, contact Mrs Elaine Cooper, Senior Administrator [admin@stvincentsprimary.org.uk](mailto:admin@stvincentsprimary.org.uk)

If you make a subject access request, and we do hold information about you or your child, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you or your child
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

Individuals also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances. You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at <https://ico.org.uk/concerns/>

## Contact

If you would like to discuss anything in this privacy notice, please contact:

Mrs Elaine Cooper, Senior Administrator [admin@stvincentsprimary.org.uk](mailto:admin@stvincentsprimary.org.uk)

Mr John Pearson Hicks, Data Protection Officer (DPO), [john.pearson-hicks@london.anglican.org](mailto:john.pearson-hicks@london.anglican.org)

## Appendix 3: Privacy Notice for Staff



# St. Vincent's Catholic Primary School

## Privacy Notice (How we use staff information)

Under General Data Protection Regulations (GDPR) we are obliged to inform you of the information we hold on you as our employees, including what we use it for, who we share it with, and for how long we keep it. This privacy notice (also known as a fair processing notice) aims to provide you with this information. If, or any information linked to is unclear, please contact the school office, or the school's Data Protection Officer. Contact details for both are available at the end of this privacy notice.

We, St. Vincent's Catholic Primary School at St. Vincent Street, W1U 4DF are the Data Controller for the purposes of data protection law.

As a public body as we have appointed a Data Protection Officer (DPO), John Pearson-Hicks and he is contactable via [john.pearson-hicks@london.anglican.org](mailto:john.pearson-hicks@london.anglican.org).

### **The categories of school workforce information that we collect, process, hold and share include:**

- Personal information (such as name, address, national insurance number).
- Contact details and preference (contact telephone numbers, email addresses, addresses)
- Characteristics (such as ethnicity, religion, language, nationality, country of birth)
- the terms and conditions of your employment;
- details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the organisation;
- information about your remuneration, including entitlement to benefits such as pensions or insurance cover;
- details of your bank account and national insurance number;
- information about your marital status, next of kin, dependants and emergency contacts;
- information about your entitlement to work in the UK;
- information about your criminal record;
- details of your schedule (days of work and working hours) and attendance at work;
- details of periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave;
- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence;
- assessments of your performance, including appraisals, performance reviews and ratings, training you have participated in, performance improvement plans and related correspondence;
- information about medical or health conditions, including whether or not you have a disability for which the organisation needs to make reasonable adjustments and fulfil its duty of care (including the use of Occupational Health Services);
- details of trade union membership where provided by yourself or your trade union;
- equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief. where this has been provided.
- Photographs (for internal safeguarding & security purposes, school newsletters, media and promotional purposes).
- CCTV images

We may also hold personal data about you from third parties, such as references supplied by former employers, information provided during the completion of our pre-employment checks, and from the Disclosure & Barring Service, in order to comply with our legal obligations and statutory guidance.

### **Why we collect and use this information**

The purpose of collecting and processing this data is to help us recruit staff and run the school efficiently, including to:

- Enable you to be paid and other benefits be provided
- Facilitate our safer recruitment of staff, as part of our safeguarding obligations towards pupils
- Fulfil our legal obligations in recruiting staff



- Support effective performance management and appraisal
- Support effective management of the school workforce, along with the implementation of its policies and procedures
- Inform our recruitment and retention policies
- Allow better financial modelling, administration and planning
- Provide references where requested
- Equalities monitoring and reporting
- Respond to any staffing issues
- Improve the management of workforce data across the sector
- Support the work of the School Teachers' Review Body
- To assess the quality of our services
- To comply with the law regarding data sharing

## The lawful basis on which we use this information

Our lawful basis for collecting and processing staff information is defined under Article 6, and the following sub-paragraphs in the GDPR apply:

- Data subject gives consent for one or more specific purposes.
- Processing is necessary to comply with the legal obligations of the controller.
- Processing is necessary to protect the vital interests of the data subject.
- Processing is necessary for tasks in the public interest or exercise of authority vested in the controller (the provision of education).

Our lawful basis for collecting and processing your information is also further defined under Article 9, in that some of the information we process is deemed to be sensitive, or special, information and the following sub-paragraphs in the GDPR apply:

- The data subject has given explicit consent.
- It is necessary to fulfill the obligations of controller or of data subject.
- It is necessary to protect the vital interests of the data subject.
- Processing is carried out by a foundation or not-for-profit organisation (includes religious, political or philosophical organisations and trade unions)
- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment
- It is in the public interest.

Where we have obtained consent to use staff members personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn. Some of the reasons listed above for collecting and using your personal data overlap, and there may be several grounds which justify our use of this data.

## Collecting this information

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain your information to us or if you have a choice in this. Where we have obtained consent to use your personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

## Storing this information

We create and maintain an employment file for each staff member. The information contained in this file is kept secure and is only used for purposes directly relevant to your employment.

Once your employment with us has ended, we will retain this file and delete the information in it in accordance with the school's [Information and Records Management Society's toolkit for schools](#).

We have data protection policies and procedures in place, including strong organisational and technical measures, which are regularly reviewed. Further information can be found on our website.

## Who we share information this with

We routinely share staff information with appropriate third parties, including:

- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and information relating to certain staffing matters
- The Department for Education - to meet our legal obligations to share certain information with it,
- Your family and representatives – such as in the event of an emergency
- Educators and examining bodies – such as ensuring we adhere to examining regulations to guarantee the validity of examinations
- Ofsted – such as during the course of a school inspection
- Suppliers and service providers – to enable them to provide the service we have contracted them for eg, HR, payroll, employee benefit schemes
- Financial organisations eg Pension Scheme
- Central and local government – such as workforce analysis
- Our auditors, to ensure our compliance with our legal obligations
- Trade Unions and Professional Associations - to enable them to provide the service their members require
- Health authorities and Occupational Health and employee support schemes – to ensure the wellbeing of our staff body in accordance with our responsibilities as employer
- Security organisations – to create a secure workplace for staff
- Health and social welfare organisations – to ensure the wellbeing of our staff body in accordance with our responsibilities as employer
- Professional advisers and consultants – for us to develop our service to best provide our public service
- Charities and voluntary organisations -
- Police forces, courts, tribunals
- Employment and recruitment agencies
- Future employers

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

## Why we share your information

We do not share information about you with anyone without consent unless the law and our policies allow us to do so.

### Local authority

We are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments

### Department for Education (DfE)

We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment educational attainment. We are required to share information about our school employees with our local authority (LA) and the Department for Education (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

### Data collection requirements:

The DfE collects and processes personal data relating to those employed by schools and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.

The department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit:

<https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

To contact the department: <https://www.gov.uk/contact-dfe>

## **Requesting access to your personal data and your Data Protection Rights**

Under data protection legislation, staff members have the right to request access to information about them that we hold, through a Subject Access Request.

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you or your child
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

Individuals also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request please contact our data protection officer, John Pearson-Hicks and he is contactable via [john.pearson-hicks@london.anglican.org](mailto:john.pearson-hicks@london.anglican.org) .

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations
- If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at <https://ico.org.uk/concerns/>

Further information

If you would like to discuss anything in this privacy notice, please contact:

Mrs Elaine Cooper, Senior Administrator [admin@stvincentsprimary.org.uk](mailto:admin@stvincentsprimary.org.uk)

Mr John Pearson Hicks, Data Protection Officer (DPO), [john.pearson-hicks@london.anglican.org](mailto:john.pearson-hicks@london.anglican.org)



## **Appendix 4 Privacy Notice for Governors**

### **St. Vincent's Catholic Primary School**

### **Privacy Notice (How we use governor information)**

Under General Data Protection Regulations (GDPR) we are obliged to inform you of the information we hold on you as our employees, including what we use it for, who we share it with, and for how long we keep it. This privacy notice (also known as a fair processing notice) aims to provide you with this information. If it, or any information linked to it is unclear, please contact the school office, or the school's Data Protection Officer. Contact details for both are available at the end of this privacy notice.

We, St. Vincent's Catholic Primary School at St.Vincent Street, W1U 4DF are the Data Controller for the purposes of data protection law.

As a public body as we have appointed a Data Protection Officer (DPO), John Pearson-Hicks and he is contactable via [john.pearson-hicks@london.anglican.org](mailto:john.pearson-hicks@london.anglican.org)

#### **The categories of governor information that we collect, process, hold and share include:**

- Personal information (such as name, address, national insurance number).
- Contact details and preference (contact telephone numbers, email addresses, addresses)
- details of your qualifications, skills, and experience for skills audit purposes;
- details of your bank account and national insurance number for reimbursement of expenses
- information about your criminal record;
- details of your appointment, including the appointing body, the date of appointment, and term of office.
- Training you have attended in your role as a governor
- Your attendance and visits to the school in your role as a governor
- Any roles or leadership responsibilities you hold within the governing body
- Your business or other charitable interests
- equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief where this has been provided.
- Photographs (for internal safeguarding & security purposes, school newsletters, media and promotional purposes).
- CCTV images

We may also hold personal data about you from third parties, such as references supplied by former employers, information provided during the completion of our pre-employment checks, and from the Disclosure & Barring Service, in order to comply with our legal obligations and statutory guidance.

#### **Why we collect and use this information**

The purpose of collecting and processing this data is to help us recruit staff and run the school efficiently, including to:

- Comply with our statutory safeguarding obligations
- Ensure we comply with our instrument of governance / Articles of Association
- Support effective governor development
- Support effective management of the school
- Statutory reporting the Department for Education
- Equalities monitoring and reporting
- Respond to any staffing issues
- Improve the management of workforce data across the sector
- Support the work of the School Teachers' Review Body
- to assess the quality of our services
- to comply with the law regarding data sharing

#### **The lawful basis on which we use this information**

Our lawful basis for collecting and processing staff information information is defined under Article 6, and the following sub-paragraphs in the GDPR apply:

- Data subject gives consent for one or more specific purposes.
- Processing is necessary for tasks in the public interest or exercise of authority vested in the controller (the provision of education).

Our lawful basis for collecting and processing your information is also further defined under Article 9, in that some of the information we process is deemed to be sensitive, or special, information and the following subparagraphs in the GDPR apply:

- (a) The data subject has given explicit consent.
  - (b) It is necessary to fulfill the obligations of controller or of data subject.
  - (d) Processing is carried out by a foundation or not-for-profit organisation (includes religious, political or philosophical organisations and trade unions)
  - (i) It is in the public interest.

Where we have obtained consent to use governor members personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn. Some of the reasons listed above for collecting and using your personal data overlap, and there may be several grounds which justify our use of this data.

### Collecting this information

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain your information to us or if you have a choice in this. Where we have obtained consent to use your personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

### Storing this information

We create and maintain a file for each governing body member. The information contained in this file is kept secure and is only used for purposes directly relevant to your term as a governor at the school. Once your term(s) of office with us has ended, we will retain this file and delete the information in it in accordance with our in accordance with the school's [Information and Records Management Society's toolkit for schools](#).

We have data protection policies and procedures in place, including strong organisational and technical measures, which are regularly reviewed. Further information can be found on our website.

### Who we share information this with

We routinely share governor information with appropriate third parties, including:

- Our local authority – to meet our legal obligations to share certain information with it, The Department for Education - to meet our legal obligations to share certain information with it,
- Your family and representatives – such as in the event of an emergency
- Ofsted – such as during the course of a school inspection
- Our auditors, to ensure our compliance with our legal obligations
- Police forces, courts, tribunals

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

### Why we share your information

We do not share information about you with anyone without consent unless the law and our policies allow us to do so.

### Department for Education (DfE)

We share personal data with the Department for Education (DfE) on a statutory basis. Under s.538 of the Education Act 1996, and the Academies Financial Handbook, the Secretary of State requires boards to provide certain details they hold about people involved in governance, as volunteered by individuals, and the information kept up to date.

## Data collection requirements:

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.

For more information about the department's data sharing process, please visit:

<https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

To contact the department: <https://www.gov.uk/contact-dfe>

## Requesting access to your personal data and your Data Protection Rights

Under data protection legislation, staff members have the right to request access to information about them that we hold, through a Subject Access Request.

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you or your child
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

Individuals also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request please contact our data protection officer, John Pearson-Hicks and he is contactable via [john.pearson-hicks@london.anglican.org](mailto:john.pearson-hicks@london.anglican.org) 020 7932 1161.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at <https://ico.org.uk/concerns/>

## Further information

If you would like to discuss anything in this privacy notice, please contact:

Mrs Elaine Cooper, Senior Administrator [admin@stvincentsprimary.org.uk](mailto:admin@stvincentsprimary.org.uk)

Mr John Pearson-Hicks, Data Protection Officer (DPO), [john.pearson-hicks@london.anglican.org](mailto:john.pearson-hicks@london.anglican.org)



# Appendix 5 Subject Access Request Log

## St. Vincent's Catholic Primary School

### Subject Access Record Log

<b>Name of data subject</b>		
<b>Name of person making the request and relationship to data subject if different</b> (e.g. parents / carers making a subject access request on behalf of a child who does not have the capacity to exercise their own rights, trade union representative, solicitor on behalf of a client)		
<b>Contact details of requester</b> (email / telephone etc.)		
<b>Has the DPO been notified?</b>	Y   N	
<b>Date data request received</b>		
<b>Date acknowledgment sent</b>		
<b>Deadline for responding to the request</b>		
<b>Name of person dealing with request</b>		
<b>Do you have sufficient proof / information to be assured of the requester's identity?</b>	Y   N	
<b>If a parent has made request on behalf of their child, have you established whether the child has the capacity to exercise their own rights in relation to their personal data (age 13+)?</b>	Y   N	
<b>Are there any court orders in place which would restrict the parent's ability to access the personal data?</b>	Y   N	
<b>What personal data have they requested?</b>		
<b>Do you need to clarify the request? Should the requester be asked to refine their request?</b>	Y   N	

*St. Vincent's Catholic Primary School regularly reviews and updates all Acceptable Use documents to ensure that they are consistent with the school Online Safety and Safeguarding Policies. We attempt to ensure that all students have good access to digital technologies to support their teaching and learning and we expect all our students to agree to be responsible users to help keep everyone safe and to be fair to others.*

## Appendix 6 CONSENT FORM

## Appendix 7 Parents AUP including Photography Policy Parents Acceptable Use Agreement

**Internet and IT:** As the parent or legal guardian of the pupil(s) named below, I grant permission for the school to give my *daughter / son* access to:

the Internet at school

the school's chosen email system

IT facilities and equipment at the school.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.

**Use of digital images, photography and video:** I understand the school has a clear policy on "The use of digital images and video" and I support this.

I understand that the school will necessarily use photographs of my child or including them in video material to support learning activities.

I accept that the school may use photographs / video that includes my child in publicity that reasonably promotes the work of the school, and for no other purpose.

**Social networking and media sites:** I understand that the school has a clear policy on "The use of social networking and media sites" and I support this.

I will not take and then share online, photographs, videos etc., about other children (or staff) at school events, without permission.

I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.

I will support the school by promoting safe and responsible use of the Internet, online services and digital technology at home. I will inform the school if I have any concerns.

**My daughter / son name(s):** \_\_\_\_\_

**Parent / carer signature:** \_\_\_\_\_

**Date:** \_\_\_/\_\_\_/\_\_\_



## The use of digital images and video

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter / son.

St. Vincent's Catholic Primary School 's rules for any external use of digital images are:

**If the pupil is named, we avoid using their photograph.**

**If their photograph is used, we avoid naming the pupil.**

Where showcasing examples of pupils work we only use their first names, rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

Only images of pupils in suitable dress are used.

Staffs are not allowed to take photographs or videos on their personal equipment.

-----  
Examples of how digital photography and video may be used at school include:

Your child being photographed (by the class teacher or teaching assistant) as part of a learning activity; e.g. taking photos or a video of progress made by a nursery child, as part of the learning record, and then sharing with their parent / guardian.

Your child's image being used for presentation purposes around the school;  
e.g. in class or wider school wall displays or PowerPoint© presentations.

Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators;  
e.g. within a CDROM / DVD or a document sharing good practice; in our school prospectus or on our school website [www.stvincentsprimary.org.uk](http://www.stvincentsprimary.org.uk)

In rare events, your child's picture could appear in the media if a newspaper photographer or television film crew attends an event.

Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission e.g. if your child won a national competition and wanted to be named in local or government literature.

Unless instructed otherwise, a child's photo will remain on the school website for two years after the child has left St. Vincent's Year 6(i.e. the end of August Year 8). This includes pupils who may leave the school at different point during their primary education.

## The use of social networking and online media

This school asks its whole community to promote the 3 commons approach to online behaviour:

### **Common courtesy**

### **Common decency**

### **Common sense**

*How do we show common courtesy online?*

We ask someone's permission before uploading photographs, videos or any other information about them online.

We do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.

*How do we show common decency online?*

We do not post comments that can be considered as being **intimidating, racist, sexist, homophobic or defamatory. This is online-bullying** and may be harassment or libel.

When such comments exist online, we do not forward such emails, tweets, videos, etc. By creating or forwarding such materials we are all liable under the law.

*How do we show common sense online?*

We think before we click.

We think before we upload comments, photographs and videos.

We think before we download or forward any materials.

We think carefully about what information we share with others online, and we check where it is saved and check our privacy settings.

We make sure we understand changes in use of any web sites we use.

We block harassing communications and report any abuse.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.

In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site. (All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this.)

In serious cases we will also consider legal options to deal with any such misuse.

The whole school community is reminded of the CEOP process for reporting abuse: [thinkuknow.co.uk/parents/](http://thinkuknow.co.uk/parents/)