CHELLINGTON CHURCH OF ENGLAND FEDERATION

PRIVACY NOTICE

Happiness Through Wisdom

"Gold there is, and rubies in abundance, but lips that speak knowledge are a rare jewel."

Proverbs 20:15

St. Lawrence VA Primary School /

Christopher Reeves VA Primary School

March 2026

Review Date

Spring Term 2028

Privacy Notice

How we use personal information relating to our pupils Data Controller
Chellington Church of England Federation

Christopher Reeves V.A. Primary School
Diocese of St Albans
Hinwick Road
Podington
Nr. Wellingborough
Northants
NN29 7HU

St Lawrence C of E VA Primary School
Diocese of St Albans
Manor Lane
Wymington
Nr Wellingborough
Northants
NN10 9LL

This Privacy Notice is to let you know how we as educational settings look after personal information about the pupils. This includes the information you provide us as well as information we hold about the pupils relating to their education. This notice explains the reasons why we hold personal information, how we use this information, who we share it with and how we keep it secure. This notice meets with the requirements of the General Data Protection Regulations (GDPR).

A copy of this Privacy Notice is available on the websites www.christopher-reeves-school.co.uk and https://www.st-lawrenceschool.co.uk

Please refer to the website copy of the Privacy Notice for the latest version as it will be updated from time to time to reflect any changes in our circumstances.

If you have any questions or queries or would like to discuss anything in this Privacy Notice, please contact: Executive Headteacher Mrs Sarah Bush (Chellington Church of England Federation) through either school office.

How we collect pupil information

Pupil information is obtained at the start of each academic year through our 'new pupil' registration forms. We also collect any changes to pupil information through update forms during the academic year as part of our data administration process to keep the information we hold as up-to-date as possible. We also collect information through secure file transfers which contain relevant information (e.g. name, date of birth, attendance details) about our new pupils from their previous schools.

We collect and hold pupil information that includes:

- Personal information about the pupils that come to our school such as name, unique pupil number and address, date of birth
- Characteristics such as home language, meal arrangements and eligibility, special educational needs
- Information that is categorised as sensitive data such as gender, ethnicity, religion and medical information

- Contact information such as parental and other contact names and telephone numbers for use in cases of emergency
- Safeguarding information such as court orders, professional involvement and contact with non-resident parents
- Medical information such as GP surgery details, allergies, medication and dietary requirements
- Sibling information
- History of previous schools or nurseries attended
- Information about your child's date of birth and nationality

In addition to the information we collect from parents/carers, we also record and hold the following information:

- Attendance information such as sessions attended, number of absences and absence reasons
- Assessment information recorded at various assessment capture points during the academic year as well as end of year attainment information such as Phonics outcomes and Key Stage 1 and 2 results
- Behaviour information and where relevant, lunch time, fixed and permanent exclusions and any relevant alternative provision
- Information about your child's proficiency in speaking the English language

Why we collect and use this information

We use the pupil data to:

- support pupil learning
- safeguard pupils in our care
- record attendance
- monitor and report on pupil attainment and progress
- keep children safe whilst in our care
- provide appropriate pastoral care
- assess the quality of our services
- comply with the law regarding data returns and sharing
- provide any additional support
- identify support needed to help children develop English speaking skills

We use parent/carer contact information to:

- email parent/carers for purpose of notification of school events, share pupil school work and various reports relating to the pupil's life at the school
- telephone parents/carers in cases of emergency or other matters relating to the safety of the child

The lawful basis on which we hold and use this information

We collect and use pupil information under the legal basis of public interest as an educational setting/school with the delegated task of educating and safeguarding the children in our care and under a legal obligation which necessitates our school making statutory data returns to the Department for Education (DfE) and the our Local Authority [as described in Article 6, GDPR).

The schools are obliged to make statutory pupil census returns and hold attendance information under the following legislation:

Education Act 1996 – Section 434 (1),(3), (4) & (6) and Section 458 (4) & (5) Education (Pupil Registration) (England) (Amendment) Regulations 2013 Department of Education Advice on Attendance (September 2022)

The special categories of data have been collected through explicit consent from the data subject in support of the specific purposes for which the data is being used in the education and safeguarding of pupils in our care [Article 9, GDPR].

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

Whilst the majority of pupil information you provide to us is mandatory (for reasons described above), there may be some information which we ask you for which is not mandatory but provided on a voluntary basis.

In some cases, we will ask you for information on the legal basis of legitimate interest where the information is required to support an educational or safeguarding function (e.g. a parent/carer email address or mobile contact number so that we can contact the parent/carer in an emergency or reasons involving the safety of the child)

The data we collect relating to medical health information is necessary to protect the vital interests of a child so that we can ensure a child's medical needs are properly addressed and catered for. As a Parent/carer, you cannot decline a data collection but you have right to decline providing information for self-declared data items by selecting the 'Refused' option e.g. ethnicity.

There are certain personal data items (e.g. photographs) which we collect on the legal basis of legitimate interest. We will ask you for your explicit consent about how these data items can be used if the purpose extends beyond holding the data within our main management information system (e.g. photograph on our school's website). As a parent/carer you can change your decision to grant or withdraw consent at any time.

If at any point in the future, we seek to use any previously collected information for another purpose or use the information in new software, we will ask for your explicit consent to do so.

Who we share pupil information with

We routinely share pupil information with:

- the school that a pupil attends after leaving us
- our local authority
- the Department for Education (DfE)

We also provide certain pupil data with other parties that provide a service for our school:

- School Nurse
- Peripatetic music teacher
- Cool Milk At School
- School Meal provider
- Residential Trip providers (eg Frontier Centre)
- SEND provision

The majority of our pupil information is processed in our main Management Information System (MIS). However, our school also purchases third party software to help us provide additional functions and services. Certain data held on our main management information system is also shared with third party software providers for the following reasons:

- Assessment software which uses the main pupil information such as name, class, date of birth and some contextual information to help us record attainment and track progress
- Text messaging software which uses the contact names and telephone numbers used to notify parents/carers of certain events and important notices
- Online payments system which uses our pupil names and classes to link to parent users for the purpose of enabling payments for meals etc.

We actively ensure that all of the third party software organisations we share data with, comply with the General Data Protection Regulations through their Privacy Notices and Data Sharing Agreements that they share with us.

Why we share pupil information with external parties

We do not share information about our pupils with anyone without consent unless the legal basis for holding and sharing the data allows us to do so.

We share pupil data with the Department for Education (DfE) and the Local Authority on a statutory basis through data collections such as the school census under the following statutes:

- Section 573A of the Education Act 1996
- Education Act 1996 s29(3) Education (School Performance Information)(England) Regulations 2007
- Regulations 5 & 8 School Information (England) Regulations 2008
- Education (Pupil Registration) (England) (Amendment) Regulations 2013

Further information about the data collection requirements placed on our school by the DfE through the school census can be found at https://www.gov.uk/education/data-collection-and-censuses-for-schools

The data shared with the DfE and the local Authority is for the purpose of:

- determining school funding which is calculated based upon the numbers of children and their characteristics in our school
- informing the monitoring of 'short term' education policy such as Pupil Progress measures
- supporting the 'longer term' research and monitoring of educational policy

Most of the pupil data we share with the DfE is held within their National Pupil Database (NPD). Please refer to the last page of this Privacy Notice for more information about the NPD and their basis for sharing data with third parties.

Our Local Authority's Privacy Notice relating to **early years pupil information** can be found at: https://www.bedford.gov.uk/schools-education-and-childcare/working-with-children/provider-portal/

How we keep personal data secure

We fully adhere to our Data Protection policies which outline our procedures and processes for accessing, handling and storing data safely in accordance with all the GDPR principles. These policies are regularly reviewed and ratified by our governors. The following processes ensure that we comply with data protection legislation in how we manage the protection of personal data:

- Our networks, file systems and server operating systems are secured through firewalls and spyware/ virus detection programs on our servers to prevent unauthorised access to our data
- Data held in a physical location within the school is held securely and only accessible by staff with appropriate authorisation
- Access to data on systems is through individual passwords which are carefully managed and monitored
- Any data that is removed from the school is minimised and encrypted
- Older data is safely removed from computers and other devices
- Data shared with the DfE and the Local Authority is shared through secure file transfer systems. Any data shared with other legitimate third parties where there is a legal basis for sharing will only be shared through secure methods.
- Data shared with third party software suppliers is controlled by the school. We will only deal with suppliers who can demonstrate that they comply with the requirements of data protection legislation and not use personal data for any other purpose than the purpose for fulfilling the functions we have contracted with them (e.g. assessment).
- We ensure all staff receive regular training on data protection

We also adhere to our Data Breach Procedures, Appendix 2 of our Data Protection Policy, in the event of a data breach. These procedures explain how our schools respond to occurrences of known or reported data breaches. A copy of this policy is available on the school websites www.christopher-reeves-school.co.uk / www.stlawrenceprimaryschool.co.uk

Requesting access to your personal data

Under data protection regulations, you as the parent/carer and pupils (from age 13) have the following rights:

- Right to be informed
- Right to access to your child's or your personal information
- Right to have inaccurate personal data rectified, blocked, erased or destroyed in certain circumstances
- Right to object to processing of personal data that is likely to cause, or is causing, damage or distress
- Right to restrict processing for the purpose of direct marketing
- Right to data portability
- Right to object to decisions being taken by automated means
- Right to claim compensation for damages caused by a breach of the Data Protection regulations

It should be noted that some of these rights will not apply in circumstances where allowing them would significantly reduce or prevent our ability to perform our duties as a school and safeguard the children in our care.

You do have the right to request access to personal information about you and/or your child that we hold. To request access to your personal information or to your child's educational record, you can make a **Subject Access Request (SAR**).

The schools will follow the procedures as outlined in our Subject Access Request (SAR) Policy and Procedure document available on our websites www.christopher-reeves-school.co.uk / www.stlawrenceprimaryschool.co.uk this follows the guidelines promoted by the data protection regulations.

Please note that whilst we aim to respond to requests within the required time period of one month, we may not be able to honour this time period if we receive requests just before or during school holidays. If the nature of the request is complex and/or the request falls within a holiday period, we will aim to reach a mutually agreed alternative time period.

How long we keep personal information

We hold pupil data for the period determined appropriate for the different types of data we hold. We will keep information for the minimum period necessary in accordance with DfE's data retention recommendations which take into account legal and safeguarding considerations linked to the types of data held. Our Data Retention Schedule, Appendix 3 of our Data Protection Policy, can be found on our websites at www.christopher-reeves-school.co.uk / www.stlawrenceprimaryschool.co.uk

All information is held securely and will be destroyed as appropriate under secure and confidential conditions.

Let us know of any changes to personal information and emergency contact information

As a matter of course, we will contact you at least once a year to ensure that all the personal information and emergency contact details we have for your child is accurate and up-to-date. We would encourage you very strongly to ensure that any changes to phone numbers in particular are notified to our school office as soon as possible.

The use of CCTV

The Chellington Federation take their responsibility towards the safety of staff, visitors and pupils very seriously. To that end, at St Lawrence, we use surveillance cameras to provide information relating to incidents which may require further investigation, vandalism, trespass or other criminal behaviour directed towards the schools site or members of the school community.

The purpose of this section is to manage and regulate the use of the surveillance and CCTV systems at the school and ensure that:

- We comply with data protection legislation, including the Data Protection Act 2018 (DPA 2018)
- The images that are captured are useable for the purposes we require them for
- We reassure those persons whose images are being captured, that the images are being handled in accordance with data protection legislation.

This policy covers the use of surveillance and CCTV systems which capture moving and still images of people who could be identified, as well as information relating to individuals for any of the following purposes:

- Observing what an individual is doing

- Taking action to prevent a crime
- Using images of individuals that could affect their privacy.

Legal framework

This policy has due regard to legislation and statutory guidance, including, but not limited to the following:

- The Regulation of Investigatory Powers Act 2000
- The Protection of Freedoms Act 2012
- Data Protection Act 2018 (DPA 2018)
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998
- The Children Act 1989
- The Children Act 2004
- The Equality Act 2010

This notice has been created with regard to the following statutory and non-statutory guidance:

- Home Office (2013) 'The Surveillance Camera Code of Practice'
- Information Commissioner's Office (ICO) (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- ICO (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'
- ICO (2017) 'In the picture: A data protection code of practice for surveillance cameras and personal information'.

This policy operates in conjunction with the following school policies:

- Data Protection Policy

Definitions

For the purpose of this notice a set of definitions will be outlined, in accordance with the surveillance code of conduct:

- Surveillance – monitoring the movements and behaviour of individuals; this can include video, audio or live footage. For the purpose of this notice only video footage will be applicable
- Overt surveillance – any use of surveillance for which authority does not fall under the Regulation of Investigatory Powers Act 2000
- Covert surveillance – any use of surveillance which is intentionally not shared with the subjects it is recording. Subjects will not be informed of such surveillance.

The Chellington Federation does not engage in covert surveillance when monitoring the school's staff, pupils and/or volunteers. Covert surveillance will only be operable in extreme circumstances; copies of the Home Office's authorisation forms will be completed and retained.

Any overt surveillance footage will be clearly signposted around the school.

Roles and responsibilities

The Chellington Federation, as the corporate body, is the data controller. The governing board of the Chellington Federation therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations. Our GDPR Lead deals with the day-to-day matters relating to data protection and thus, for the benefit of this policy will act as the data controller.

The role of the data controller includes:

- Processing surveillance and CCTV footage legally and fairly
- Collecting surveillance and CCTV footage for legitimate reasons and ensuring that it is used accordingly
- Collecting surveillance and CCTV footage that is relevant, adequate and not excessive in relation to the reason for its collection
- Ensuring that any surveillance and CCTV footage identifying an individual is not kept for longer than is necessary
- Protecting footage containing personal data against accidental, unlawful destruction, alteration and disclosure – especially when processing over networks
- Monitoring legislation to ensure the school is using surveillance fairly and lawfully
- Communicating any changes to legislation with all members of staff.
- Informing data subjects of how their data captured in surveillance and CCTV footage will be used by the school, their rights for the data to be destroyed and the measures implemented by the school to protect individuals' personal information
- Preparing reports and management information on the school's level of risk related to
- Reporting to the highest management level of the school, e.g. the SLT and governors
- Presenting reports regarding data processing at the school to senior leaders and governors.

Purpose and justification

- The school will only use surveillance cameras for the safety and security of the school and its staff, pupils and visitors
- Surveillance will be used as a deterrent for violent behaviour and damage to the school
- The school will only conduct surveillance as a deterrent. Surveillance and CCTV cameras are on the outside of the school building, and under no circumstances will the surveillance and the CCTV cameras be present in school classrooms or any changing facility
- If the surveillance and CCTV systems fulfil their purpose and are no longer required the school will deactivate them
- Cameras on the front gate are not part of the CCTV system, and images or video are not recorded.

The data protection principles Data collected from surveillance and CCTV will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and, where necessary, kept up-to-date; every reasonable step will be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Objectives The surveillance system will be used to:

- Monitor the safety of the environment
- Monitor the welfare of pupils, staff and visitors
- Deter criminal acts against persons and property
- Assist the police in identifying persons who have committed an offence.

Protocols

- The surveillance system will be registered with the ICO in line with data protection legislation. The surveillance system is a closed digital system which does not record audio
- Warning signs have been placed throughout the premises where the surveillance system is active, as mandated by the ICO’s Code of Practice
- The surveillance system has been designed for maximum effectiveness and efficiency; however, the school cannot guarantee that every incident will be detected or covered and ‘blind spots’ may exist
- The surveillance system will not be trained on individuals unless an immediate response to an incident is required
- The surveillance system will not be trained on private vehicles or property outside the perimeter of the school.

Security

- Access to the surveillance system, software and data will be strictly limited to authorised operators. The school's authorised CCTV system operators is Mr Garry Pittam - Site Manager
- The main control facility is kept in a secure location. It is monitored during the day, and is locked away after school hours
- If, in exceptional circumstances, covert surveillance is planned, or has taken place, copies of the Home Office's authorisation forms will be completed and retained
- Surveillance and CCTV systems will be tested for security flaws regularly to ensure that they are being properly maintained at all times
- Surveillance and CCTV systems will not be intrusive
- The data controller and site manager will decide when to record footage, e.g. a continuous loop outside the school grounds to deter intruders
- Any unnecessary footage captured will recorded over by subsequent footage every 30 days
- Any cameras that present faults will be repaired immediately as to avoid any risk of a data breach
- All visual display monitors are located in the Coms room

Code of practice

- The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles
- The school notifies all pupils, staff and visitors of the purpose for collecting surveillance data through public signage and privacy notices
- CCTV cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose
- All surveillance footage will be kept for one month for security purposes; the site manager is responsible for keeping the records secure and allowing access
- The school has a surveillance system for the purpose of the prevention and detection of crime and the promotion of the health, safety and welfare of staff, pupils and visitors
- The surveillance and CCTV system is owned by the school and images from the system are strictly controlled and monitored by authorised personnel only.
- The school will ensure that the surveillance and CCTV system is used to create a safer environment for staff, pupils and visitors to the school, and to ensure that its operation is consistent with the obligations outlined in data protection legislation.

The surveillance and CCTV system will:

- Be designed to take into account its effect on individuals and their privacy and personal data
- Have clear responsibility and accountability procedures for images and information collected, held and used
- Only keep images and information for as long as required. Any incident footage kept beyond 30 days will be kept on a secure server by the DPO and reviewed annually
- Restrict access to retained images and information with clear rules on who can gain access

- Consider all operational, technical and competency standards, relevant to the surveillance and CCTV system and its purpose, and work to meet and maintain those standards in accordance with the law
- Be subject to stringent security measures to safeguard against unauthorised access
- Be regularly reviewed and audited to ensure that policies and standards are maintained
- Only be used for the purposes for which it is intended, including supporting public safety, the protection of pupils, staff and volunteers, and law enforcement
- Be accurate and well maintained to ensure information is up-to-date.

Access

- Under the DPA (2018), individuals have the right to obtain confirmation that their personal information is being processed
- All disks containing images belong to, and remain the property of, the school
- Individuals have the right to submit an SAR to gain access to their personal data in order to verify the lawfulness of the processing
- The school will verify the identity of the person making the request before any information is supplied
- A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to comply with requests for further copies of the same information
- Where an SAR has been made electronically, the information will be provided in a commonly used electronic format
- Requests by persons outside the school for viewing or copying disks, or obtaining digital recordings, will be assessed by the data controller, who will consult the DPO, on a case-by-case basis with close regard to data protection and freedom of information legislation
- Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged
- All fees will be based on the administrative cost of providing the information
- All requests will be responded to without delay and at the latest, within one month of receipt
- In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request
- Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the ICO and to a judicial remedy, within one month of the refusal
- In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to
- It is important that access to, and disclosure of, the images recorded by surveillance and CCTV footage is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact, should the images be required for evidential purposes.

Releasing the recorded images to third parties will be permitted only in the following limited and prescribed circumstances, and to the extent required or permitted by law:

- The police – where the images recorded would assist in a specific criminal inquiry
- Prosecution agencies – such as the Crown Prosecution Service (CPS)
- Relevant legal representatives – such as lawyers and barristers
- Persons who have been recorded and whose images have been retained where disclosure is required by virtue of data protection legislation and the Freedom of Information Act 2000
- Requests for access or disclosure will be recorded and the Executive Headteacher will make the final decision as to whether recorded images may be released to persons other than the police.

Reporting concerns about our data protection processes

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 by contacting Executive Headteacher Mrs Bush or Mrs Ashby, Chair of Governors. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Keeping you informed through this Privacy Notice

We aim to keep you informed of any changes to our data collections and data protection obligations through this Privacy Notice – the latest copy will be available on our websites at www.christopher-reeves-school.co.uk / www.stlawrenceprimaryschool.co.uk

We incorporate information about the pupil data we hold and how we adhere to the GDPR principles for protecting this data in our e-Safety and ICT lessons so that our children are aware of what we do.

This Notice agreed by Full Governing Board on 19th March 2026

Review due in Spring Term 2028

Department for Education (DfE)

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.

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

Sharing data by the DfE

The DfE can legally share information about our pupils from the NPD with third parties who are:

- organisations involved with promoting the education or well-being of children in England :
- researchers or analysts
- schools

- local authorities
- other government departments and agencies
- organisations fighting or identifying crime

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

How the DfE keeps data secure

All data is transferred securely and held by DfE under a combination of software and hardware controls, which meet **ISO27001** standards and the **government security policy framework.**

The Department has robust processes in place to ensure the confidentiality of our pupils' 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 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