Start children off on the way they should go, and even when they are old they will not turn from it."

Proverbs 22:6

DATA PROTECTION & GDPR POLICY

Adopted	Autumn Term 2025
Committee	Resources
Review Date	Autumn Term 2026

We are a Christian school where quality and opportunities make a difference. We value all children as unique 'Children of God' and nurture each other to show LOVE in our relationships and a RESPECT for all. We foster HOPE within our community and encourage children to find PEACE by creating times and places for stillness and reflection. We strive for excellence, inspiring dreams both now and in the future. We promote POSITIVITY, celebrate COURAGE, demonstrate RESPONSIBILITY and share JOY through…

'Learning, loving, laughing in the light of Jesus'.

Data protection is about regulating the way that organisations who use and store personal identifiable information about people (personal data), and it provides individuals with various rights regarding the use of their data.

This policy is in place to ensure all staff (including volunteers) and Governing Board members are aware of their responsibilities and outlines how we comply with the principles and requirements of the UK GDPR and DPA 2018.

Legal framework

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

- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA)
- School Standards and Framework Act 1998
- Freedom of Information Act 2000
- The Electronic Commerce (EC Directive) Regulations 2002
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2018)
- Protection of Freedoms Act 2012
- DfE (2024) 'Keeping children safe in education 2024'

This policy also has regard to the following guidance:

- ICO (2022) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- DfE (2023) 'Data protection in schools'
- DfE (2025) 'Generative artificial intelligence (AI) in education'

1. RESPONSIBILITIES

All users of personal data at Forsbrook CE Primary School have a responsibility to ensure that personal data is always held securely and not disclosed to any unauthorised third party either accidentally, negligently or intentionally. Everyone is responsible for protecting personal data.

For most of the personal data that is collected, stored and used, Forsbrook CE Primary School is the data controller. This means that we are responsible under the Data Protection Act 2018 for protecting data in every situation where our organisation decides:

- Whose information to collect
- What types of data is required to permit our organisation to function in accordance with our official duties as a public sector organisation

- The reasons that this data is needed
- Whether the information can be shared with a third party or third parties
- When and where data subjects' rights apply
- How long to keep the data for

In certain circumstances, the role of the data controller may also be extended to third parties, for example, when the organisation is required to supply a copy of some personal data to the Department for Education (DfE), DfE also becomes an independent data controller of the copy it receives.

All employees, volunteers and others accessing and processing personal data of Forsbrook CE Primary School must adhere to data protection policies and code of conduct, keep all personal data secure throughout its lifespan and participate in relevant data protection inductions and training.

Forsbrook CE Primary School will:

- ✓ Monitor their data protection performance
- ✓ Support the DPO and senior leaders
- ✓ Have good network security infrastructure to keep personal data protected
- ✓ Have a business continuity plan in place, and a cyber response plan held separately to the business continuity plan, which are reviewed at least annually ensuring that all personal data is kept securely and security management measures are sufficient
- ✓ Maintain records relating to data protection, including all actions and decisions relating to data protection matters, subject access requests, information asset registers, potential breaches, requests made in relation to personal data, records of processing activities
- ✓ Ensure that queries regarding data protection, including subject access requests and complaints, are promptly directed to the Headteacher as necessary
- ✓ Ensure that any data protection breaches are swiftly brought to the attention of the DPO in adherence with the Personal Data Breach Management Plan and that they support the Headteacher when investigating breaches
- ✓ Where there is uncertainty around a data protection matter, advice is sought from the DPO
- ✓ Providing the required training and inductions for staff or arranging this with the DPO, and ensuring that refresher training is undertaken annually

The 'responsible person' for data protection, or 'Data Protection Lead', and the Headteacher, will be responsible for ensuring and monitoring compliance with data protection policies, and reporting as required to the DPO, including:

- Maintaining records of training
- Communicating with the DPO where a Data Protection Impact Assessment (DPIA) be required
- Supporting data protection audits

- Adhering to data protection risk management requirements

Senior leaders will:

- ✓ Decide how the school uses technology and maintains its security
- ✓ Decide what data is shared and how, in conjunction with the Data Sharing Policy
- ✓ Set procedures for the use of data and technology
- ✓ Understand what UK GDPR and the Data Protection Act covers and obtain advice from the DPO, as appropriate
- ✓ Assure the Governing body that their setting has the right policies and procedures in place / is following policies and procedures
- ✓ Ensure that staff receive annual training on data protection
- ✓ Ensure no personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party
- ✓ Ensure any queries regarding data protection, including subject access requests and complaints, are promptly directed to the responsible person at Forsbrook CE Primary School
- ✓ Ensure any data protection breaches are swiftly brought to the attention of the responsible person and the DPO and that they support the Headteacher in resolving breaches
- ✓ Ensure training and inductions are attended, including annual refresher training
- ✓ Communicate with the responsible person where new processing activities are due to take place so that a DPIA can be considered and arranged
- ✓ Supporting data protection audits
- ✓ Adhering to data protection risk management requirements

All staff have responsibilities to ensure:

All staff, including but not limited to teaching staff, catering staff, welfare supervisors, library staff, cleaning staff, first aiders, Governors, volunteers should be aware of what:

- Personal data is
- 'Processing' means
- Their duties are in handling personal information
- The processes are for using personal information
- Is permitted usage of that data
- The risks are if data gets into the wrong hands
- Their responsibilities are when recognising and responding to a personal data breach
- The process is for recognising and escalating information rights requests

There are extra requirements for any staff in school who create and store data, enter data into applications or software, decide if and when they'll process certain data and handle paper documents containing personal data. These staff members are responsible for:

- Making sure they have a legitimate need to process the data

- Checking that any data they store is needed to carry out necessary tasks
- Identifying any risks
- Understanding the governance arrangements that oversee the management of risks

Contractors, Short-Term and Voluntary Staff are responsible for ensuring:

- Any personal data collected or processed in the course of work undertaken for Forsbrook CE Primary School is kept securely and confidentially at all times
- All personal data is returned to Forsbrook CE Primary School on completion of the work, including any copies that may have been made. Alternatively, that the data is securely destroyed and the school provide approval in this regard from the contractor or short term / voluntary member of staff. Evidence of destruction must be provided
- Forsbrook CE Primary School receive prior notification of any disclosure of personal data to any other organisation or any person, and approve this disclosure
- Any personal data made available by Forsbrook CE Primary School, or collected in the course of the work, is neither stored nor processed outside the EEA unless written consent to do so has been given by the school
- All practical and reasonable steps are taken to ensure that contractors, short term or voluntary staff do not have access to any personal data beyond what is essential for the work to be carried out properly, that there is a lawful basis for providing them with that information, and that consent to process personal data is obtained where necessary.

2. PERSONAL DATA

Personal data refers to information that relates to a living individual, who could directly or indirectly be identified through the processing of their personal data. This includes information such as an online identifier, for example an IP address.

The UK GDPR applies to electronic and automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data (where pseudonymisation enhances the privacy of data by replacing identifying fields within a data record by one or more artificial identifiers), e.g. key-coded.

Examples of personal data are:

• Identity details; name, title, role

• Contact details; address, phone number

• A pupil report

• Pupil behaviour and attendance records

• Assessment and exam results

• A contract of employment, staff recruitment information

• Staff development reviews

• Pupils'/students' exercise books, coursework and mark books

• Health records

• Email correspondence relating to an individual
• Governance recruitment records
• Payroll data
• Risk assessments

Sensitive personal data is referred to in the UK GDPR as 'special categories of personal data' (SCD). SCD is considered to be more sensitive and is given more protection in data protection law.

Special category data includes:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data (e.g. fingerprints)
- Data concerning health (mental and physical health) and medical records
- Data concerning a natural person's sex life or sexual orientation

Criminal office data is personal data that is treated in a similarly sensitive way to SCD; it records criminal convictions and offences or related security measures. Criminal offence data includes the alleged committing of an offence and the legal proceedings for an offence that was committed or alleged to have been committed, including sentencing.

Forsbrook CE Primary School processes criminal offence data in storing the outcome of a Disclosure and Barring Service (DBS) check on their employees, non-employed staff and volunteers. As this data relates to criminal convictions, collecting and retaining it means that we are processing criminal offence data. This applies even if a check has not revealed any conviction.

We are able to process data about criminal allegations, proceedings or convictions where data is:

- Under the control of official authority; or
- Authorised by domestic law.

The processing must be necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller of the data subject in connection with employment, social security, social protection, health or social care purposes, public health, and research.

Forsbrook CE Primary School collects, stores and uses personal data about individuals, who are known as data subjects under data protection laws. Data subjects include but are not limited to:

- Pupils and former pupils
- Parents and carers
- Employees and non-employed staff
- Governors

- Volunteers, visitors and job applicants
- Students on work placement
- Contractors

Forsbrook CE Primary School holds personal data in several forms. These are known as data assets and data items and include:

- Data item groups – data items about the same process
- Data sets – collections of related data that can be manipulated as a unit by a computer
- Systems – administrative software
- System groups – the larger systems housing administrative software

3. PRINCIPLES

The UK GDPR provides 7 principles of data protection. The principles of data protection lie at the heart of data protection laws and designate that personal data must be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals (Lawfulness, Fairness and Transparency Principle).
- Collected and processed 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 (Purpose Limitation Principle).
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (Data Minimisation Principle).
- Accurate and, where necessary, kept up-to-date; every reasonable step must 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 (Accuracy Principle).
- Kept in a form which permits identification of data subject 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 UK GDPR in order to safeguard the rights and freedoms of individuals (Storage Limitation Principle). This will be managed in accordance with the Data Retention Policy.
- 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 (Integrity and Confidentiality Principle).

The UK GDPR requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles". Processing activities shall be documented effectively. (Accountability Principle).

"Processing" covers virtually every aspect of a setting's use of personal information from the point of collection and throughout its lifespan. Processing includes using, disclosing, copying, sharing, entering data into electronic and filing systems, storing and disposing of personal data.

Individuals must be told what data is collected about them, what it is used for, and who it might be shared with. They must also be given other information, such as, what rights they have in relation to their personal information, how long it is kept for and about their right to complain to the Information Commissioner's Office (ICO), as the UK's regulator for data protection and is the independent body that upholds the UK's information rights. This information is provided in the schools privacy notices and can be obtained from the school website.

4. ACCOUNTABILITY

Forsbrook CE Primary School will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the UK GDPR.

This includes:

- The use of privacy notices; comprehensive, clear and transparent template privacy notices will be provided and shared with data subjects. Privacy notices will be reviewed on a regular basis.

Internal records of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and their personal data
- Retention schedules
- Categories of recipients of personal data
- Details of third parties using the data
- Description of technical and organisational security measures
- Information requests and details of how and when the request was responded to
- Personal data breaches, how and when the breach was managed
- The sharing of privacy notices and information
- Consent obtained for the processing of personal data (this includes consent from parents / carers, secondary students and staff)
- The compliant disposal of personal data at the end of its retention period, or legal reasons for keeping data beyond its retention period
- Data protection impact assessments undertaken for processing personal data

Forsbrook CE Primary School will maintain appropriate records in relation to their processing activities relating to personal data. It will maintain appropriate policies and procedures in relation to the processing of personal data, which shall be reviewed on a regular basis.

Individuals processing personal data during the course of their work for the school shall be appropriately trained in data protection and cyber security, according to the nature of their role and type of data that they are processing. Inductions relating to data protection will also be provided. All staff must learn about UK GDPR and data protection as part of their induction and annual CPD in the same way they learn about safeguarding.

5. Data Protection Officer (DPO)

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

The Headteacher 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 Headteacher 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 the Information Governance Unit at Staffordshire County Council and is contactable via email.

6. LAWFUL PROCESSING

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 UK GDPR at Article 9.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

Under UK GDPR, there are 10 additional conditions for processing Special Category Data (SCD). At least one lawful basis and one condition must apply.

The conditions are:

- ✓ Explicit consent – the accessing or processing of this personal data has the written consent of the individual concerned
- ✓ Employment, social security or social protection – it's necessary for one of these 3 stated purposes and authorised by law or a collective agreement
- ✓ Vital interests – it is necessary to protect an individual's life, and the data subject is physically or legally incapable of giving consent
- ✓ Not-for-profit body – it's necessary for the legitimate internal-only purposes of a membership body with a political, philosophical, religious or trade-union aim
- ✓ Manifestly made public – it relates to personal data the individual has themselves deliberately made public
- ✓ Legal claims or judicial acts – it's necessary for a legal case, in the exercise or defect of legal claims, or as required by a court of law
- ✓ Substantial public interest – there's a relevant basis in UK law and one of the 23 specific public interest conditions has been met, and contains appropriate safeguards
- ✓ Health or social care – it's necessary for the provision of healthcare or treatment, or of social care, and there's a basis in law, preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services with a basis in law
- ✓ Public health – it's necessary for reasons of public interest, and there's a basis in law, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
- ✓ Archiving, research and statistics – it's necessary for reasons of public interest, and there's a basis in law

Criminal offence data is treated in a similar way to special category data.

The Data Protection Act 2018 (DPA), Schedule 1, Parts 1 and 2 has more information about the conditions that are authorised or have a basis in law. For conditions (b), (h), (i) or (j), the associated condition in UK law, set out in Part 1 of Schedule 1 of the DPA 2018 also need to be met. For substantial public interest condition in Article 9(2)(g), one of 23 specific substantial public interest conditions set out in Part 2 of Schedule 1 of the DPA 2018 also need to be met. The ICO's lawful basis interactive guidance tool can help organisations to decide whether they have the legal right to process particular personal data items and on what grounds.

There may be circumstances where it is considered necessary to process personal data or special category personal data in order to protect the vital interests of a data subject. This may include medical emergencies where it is not possible for the data subject to give consent to the processing. In such circumstances, the DPO will be consulted and a decision made only after seeking further clarification.

7. CONSENT

Consent must be a positive indication expressly confirmed in words. It cannot be inferred from silence, inactivity or pre-ticked boxes. The UK GDPR defines consent as 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'. For consent to be considered 'freely given', an individual must suffer no detriment if they refuse to give it.

Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes. Where consent is given, a record will be kept documenting how and when consent was given. Copies of written consent will be maintained and securely stored.

Consent mechanisms are required to meet the standards of the UK GDPR. Consent cannot be utilised as a lawful basis for processing where the data must be processed in order to fulfil their functions as a public body, where there is a legal or contractual obligation to process the data, or where processing falls under vital or legitimate interests. In short, consent will not be appropriate where it is necessary to process the data, and the individual cannot be given a real choice.

Consent can be withdrawn by the individual at any time and following the withdrawal of consent, the processing will cease. Where consent is withdrawn, all relevant parties who process the fields of personal data for which the consent is withdrawn shall be informed by the designated employee / Data Lead.

If consent is required, it must be obtained in writing at the point of data collection. Individuals will be informed how to withdraw their consent at the point of collection and via Privacy Notices.

Individuals should give written consent wherever possible. Consent should be requested after the individual has been fully informed about how the personal data will be used.

Queries regarding consent should be raised with the schools DPL.

Forsbrook CE Primary School cannot continue to process personal data indefinitely. This should be processed in accordance with the retention policy and storage limitation principle of the UK GDPR and not retained for longer than is required to fulfil the original purpose for using the data.

Consent should be refreshed at regular intervals, and individuals reminded of the procedure for withdrawing their consent.

8. PRIVACY NOTICES

Under UK GDPR and the Data Protection Act 2018, Forsbrook CE Primary School has to make its privacy notices freely available to those whose personal data it handles.

A privacy notice explains:

- Why we need to collect personal data
- Who the Data Controller is
- What data is being processed
- What the setting plans to do with the data and how long the setting will keep the data
- Whether the setting will be sharing the data with any other organisation and why

- What the lawful basis for processing is
- How individuals can exercise their rights over their personal data
- Who to contact if an individual has any concerns

Privacy notices are required to be clear and accessible. Privacy notices are updated based on DfE model privacy notices and shall be reviewed regularly and updated where there are any changes to processes surrounding the use of personal data.

Information rights requests relating to personal data can be made verbally or in writing, including via social media. Unless there's a valid reason, an information rights request must be responded to within one calendar month. If the case is deemed complex after consultation with the DPO, the response deadline can be extended by an extra two calendar months.

Information rights requests only apply to the personal data Forsbrook CE Primary School holds when they receive the request.

All staff must be trained to recognise different kinds of information rights request and know how to escalate a request if they receive one.

9. THE RIGHT TO BE INFORMED

Individuals have the right to be informed regarding how their data is used. Forsbrook CE Primary School will use Privacy Notices to inform individuals about the use of their data.

Privacy notices will be written in clear, plain language, which is concise, transparent, easily accessible, free of charge and can be easily understood by the relevant party; this includes privacy notices provided for pupils and students.

Data should be obtained directly from the data subject wherever possible but in some circumstances, data may need to be requested from third parties, for example, references from previous employers, Occupational Health reports, information which has been transferred from previous schools, and health care plans.

Privacy notices should inform individuals where their data will be sought from third parties, who the third parties are and the legal basis for obtaining information in this format.

Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement and the details of the categories of personal data, as well as any possible consequences of failing to provide the personal data, will be provided.

Where data is not obtained directly from the data subject, information regarding the source the personal data originates from and whether it came from publicly accessible sources, will be provided.

In relation to data that is not obtained directly from the data subject, this information will be supplied, where relevant to do so:

- Without undue delay, following receipt of the data.
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- If the data are used to communicate with the individual, at the latest, when the first communication takes place.

10. RIGHTS OF ACCESS

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 can be submitted in any way and should in 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 Data Protection Lead in school.

All requests will be acknowledged as soon as possible. Subject access requests will be responded to without undue delay but within one calendar month, unless an extension is required. Extensions may be applied where a request is considered to be complex. Where an extension is required, this will be assessed and agreed by the DPO in conjunction with the ICO's criteria for extending response times, and the decision will be recorded in writing. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one calendar month of the setting receiving the request.

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 (30 calendar days), 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.

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
- 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 schools Data Protection Lead. If staff receive such a request, they must immediately forward it to them.

11. THE RIGHT TO ERASURE

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

Forsbrook CE Primary School has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

12. THE RIGHT TO RESTRICT PROCESSING

Individuals have the right to restrict the processing of personal data in certain circumstances. In the event that processing is restricted, Forsbrook CE Primary School will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

Forsbrook CE Primary School will restrict the processing of personal data in the following circumstances:

- Where the basis for processing the data is consent;
- Where an individual contests the accuracy of the personal data, processing will be restricted until we have verified the accuracy of the data;
- Where an individual has objected to the processing and the school is considering whether their legitimate grounds override those of the individual;
- Where processing is potentially unlawful and the individual opposes erasure and requests restriction instead;
- Where we no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

If the personal data in question has been disclosed to third parties, we will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

Forsbrook CE Primary School will inform staff members involved in processing the data, where a request to restrict processing is approved. Where a restriction on processing is subsequently lifted, staff and other third parties who process the data will be informed.

Where we are restricting the processing of personal data in response to a request, we will make that data inaccessible to others, where possible, e.g. by temporarily moving the data to another processing system or unpublishing published data from a website.

We reserve the right to refuse requests for restricting processing if they are manifestly unfounded or excessive or if exemptions apply. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

13. THE RIGHT TO DATA PORTABILITY

Individuals have the right to obtain and reuse their personal data for their own purposes and across different services.

Personal data must be moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

The right to data portability applies:

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

Personal data will be provided in a structured, commonly used and machine-readable form.

Where feasible, data will be transmitted directly to another organisation at the request of the individual. Prior to transferring the requested data, the individual must provide confirmation of their identification to the school.

In the event that the personal data concerns more than one individual, Forsbrook CE Primary School will consider whether providing the information would prejudice the rights of any other individual and how the data of other individuals will be adequately protected.

Where no action is being taken in response to a request, Forsbrook CE Primary School will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority.

14. THE RIGHT TO OBJECT

Forsbrook CE Primary School will inform individuals of their right to object to their data being collected via a privacy notice, upon the point of data collection. This information will be provided clearly and explicitly.

Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest;
- Direct marketing;
- Processing for purposes of scientific or historical research and statistics.

Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation. An individual cannot exercise their right to object if they have given consent for the processing of their personal data, they must instead withdraw their consent.
- Forsbrook CE Primary School will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

Where personal data is processed for direct marketing purposes:

- Forsbrook CE Primary School will stop processing personal data for direct marketing purposes as soon as an objection is received.
- Forsbrook CE Primary School cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes. The setting will retain only enough information about the individual to ensure that the individual's preference not to receive direct marketing is respected in future.

Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, Forsbrook CE Primary School is not required to comply with an objection to the processing of the data.

15. RIGHTS IN RELATION TO AUTOMATED DECISION MAKING

Article 22(1) of the UK GDPR limits the circumstances in which you can make solely automated decisions, including those based on profiling, that have a legal or similarly significant effect on individuals.

Solely means a decision-making process that is totally automated and excludes any human influence on the outcome. A process might still be considered solely automated if a human inputs the data to be processed, and then the decision-making is carried out by an automated system.

Any processing of this nature must be consulted with the DPO, prior to this being undertaken. A DPIA must also be undertaken.

Forsbrook CE Primary School will ensure that individuals concerned are given specific information about the processing and an opportunity to challenge or request a review of the decision.

Individuals have the right not to be subject to a decision when both of the following conditions are met:

- It is based on automated processing, e.g. profiling
- It produces a legal effect or a similarly significant effect on the individual

Forsbrook CE Primary School will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

When automatically processing personal data for profiling purposes, Forsbrook CE Primary School will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.
- Using appropriate mathematical or statistical procedures.
- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

Generative AI systems will not be used to make solely automated decisions with significant effects on individuals, such as decisions regarding academic grading, behaviour sanctions, admissions, or staff appraisals, unless a suitably qualified person reviews and authorises the decision-making outcome.

Individuals have the right not to be subject to a decision when both of the following conditions are met:

- It is based on automated processing, e.g. profiling
- It produces a legal effect or a similarly significant effect on the individual

Forsbrook CE Primary School will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

When automatically processing personal data for profiling purposes, we will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.
- Using appropriate mathematical or statistical procedures.

- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

16. PRIVACY & DATA BREACHES

Forsbrook CE Primary School will act in accordance with the UK GDPR by adopting a privacy by design approach, and implementing technical and organisational measures which demonstrate how we have considered and integrated data protection into processing activities.

Data Breaches - The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. A data breach is a security incident that has resulted in personal data being:

- Lost or stolen
- Destroyed without consent
- Changed without consent
- Accessed by someone without permission

All members of staff must be trained to:

- Recognise when a personal data breach has taken place
- Know how to report it formally in accordance with the personal data breach management plan

Where we hold concerns about an issue relating to data privacy, this must be reported to the DPO immediately, for support, advice and investigation.

Once an individual becomes aware of a suspected data breach, a check must be made to establish whether the breach involves personal information. If personal data is involved, it must be established as to what types of personal data are involved and who the data subjects are. The investigation must identify how many people are affected by the breach to help determine the level of risk involved. This is the risk to the people who are affected; how seriously people might be harmed and the probability of this happening. This will consider all the information currently available, for example:

- Who's affected
- How many people are affected
- The ways it might affect them, such as:
    - Safeguarding issues
    - Identity theft
    - Significant distress

The priority is to establish what has happened to the personal data; where the personal data that has been accessed, lost or stolen now is, and who might have it. If the data can be recovered, this must be done immediately and protect those who'll be most impacted.

The person reporting the breach must make notes about the breach and provide sufficient information to allow an investigation to start and send this via email to the Headteacher They will ask for further information as necessary. This must be reported once the individual becomes aware of the breach to allow as much time as possible to investigate.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed within 72 hours, following an initial assessment by the DPO. The DPO will assist in making the report.

The breach will be investigated to record findings and outcomes. Any actions taken in relation to managing and mitigating the breach will also be recorded.

In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the school will notify those concerned directly, without undue delay.

In the event that a breach is sufficiently serious, the public will be notified without undue delay, in consultation with the ICO and insurance providers.

If the breach involves a cyber incident, the Cyber Incident Response Plan will be followed. The breach will be reported to the relevant authorities which may include Action Fraud, the Police, the NCSC.

Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

Failure to report a breach when required to do so can result in a fine, as well as a fine for the breach itself. Fines will be operated on a two-tier system by the ICO. The fine is dependent on factors such as the measures that were undertaken to mitigate the risk of the breach occurring, and the nature of the breach.

After every personal data breach or near miss, the following should be reviewed:

- What happened
- How it happened
- Why it happened
- What actions can be taken to prevent it happening again

In accordance with DfE guidance, every personal data breach shall be recorded and investigated, and trend analysis should be undertaken, if necessary.

It is important to take steps to reduce the possibility of personal data breaches occurring.

Prevention can include:

- Mandatory data protection training undertaken annually for all staff, that includes how to recognise and report a personal data breach
- Ensuring that staff have an awareness of common data breaches and how they can be avoided, such as by checking recipients and attachments are correct before sending emails
- Having appropriate controls in place to protect personal data

17. DATA RETENTION

Data will not be kept for longer than is necessary.

Data that reaches its retention period will be deleted / destroyed as soon as practicable. The Data Protection Act 2018 and UK GDP Rays data should only be kept for as long as it is needed unless there is a legal reason to continue processing the data. All personal data must be disposed of securely.

Some educational records relating to former pupils or employees of Forsbrook CE Primary School may be kept for an extended period for legal reasons, but also to enable the provision of references, academic transcripts, historical or archiving purposes. Data which is retained must be anonymised wherever possible, without losing its meaning.

Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained. Electronic memories are inclusive of those relating to leased devices such as photocopiers and printers.

Forsbrook CE Primary School will ensure that any copies of personal data are not retained beyond specified retention periods, inclusive of those which are held with third parties.

As data becomes older, there are steps that can be taken to keep data about pupils for analytical purposes. Before deleting the data completely, remove names and personal identifiers. Another option is to replace the personal information with non-personal identifiers. For example, replace the:

- Name with a random ID
- Date of birth with year of birth
- Postcode with locality or town name

When records have reached the end of their retention period, data must be disposed of securely and confidentially. All records containing personal information or sensitive policy information must be made either unreadable or so they cannot be reconstructed. Do not dispose of records with the regular waste or in a skip. Data can be disposed of by:

- Shredding paper records using a cross-cutting shredder, or get a compliant external company to shred them
- Destroy storage media and hard disks to particles no larger than 6mm
- Dismantle and shred audio and video tapes

External companies should:

- Shred all records on-site in the presence of an employee

- Be able to prove that the records have been destroyed and provide a certificate of destruction
- Have trained its staff in the handling of confidential documents

School has procedures for record retention and disposal:

- A senior leader has approved the record to be destroyed.
- Document the destruction. Record a brief description of the data, the number of files and who authorised the destruction.
- Shred the records as soon as they have been documented as having been destroyed.

18. Disclosure and Barring Service (DBS) Data

All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication. Data provided by the DBS will never be duplicated.

DBS data will be collected in line with the Safer Recruitment Policy, KCSiE and the Retention and Records Management Policy. Copies of DBS certificates will not be taken.

DBS data will remain strictly confidential and be kept secure at all times, and only be accessed by those who need the data to perform their role.

19. SAFEGUARDING

The UK GDPR does not prevent or limit the sharing of information for the purposes of keeping children safe. Forsbrook CE Primary School will ensure that staff have due regard to their ability to share personal information for safeguarding purposes, and that fears about sharing information must not be allowed to obstruct the need to safeguard and protect pupils.

Staff should be:

- Confident of the processing conditions which allow them to store and share information for safeguarding purposes, including information, which is sensitive and personal, and should be treated as 'special category personal data'.
- Aware that information can be shared without consent where there is good reason to do so, and the sharing of information will enhance the safeguarding of a pupil in a timely manner.

Forsbrook CE Primary School will ensure that formation pertinent to identify, assess and respond to risks or concerns about the safety of a child is shared with the relevant individuals or agencies proactively and as soon as is reasonably possible. Where there is doubt over whether safeguarding information is to be shared, especially with other agencies, the DSL (in conjunction with the Data Protection Lead) will ensure that they record the following information:

- ✓ Whether data was shared
- ✓ What data was shared
- ✓ With whom data was shared
- ✓ For what reason data was shared
- ✓ Where a decision has been made not to seek consent from the data subject or their parent
- ✓ The reason that consent has not been sought, where appropriate

Forsbrook CE Primary School will aim to gain consent to share information where appropriate; however, staff will not endeavour to gain consent if to do so would place a child at risk. The school will manage all instances of data sharing for the purposes of keeping a child safe in line with the Safeguarding Policy.

Pupils' personal data will not be provided where the serious harm test is met. Where there is doubt, legal advice can be sought.

20. CLOUD COMPUTING

For the purposes of this policy, 'cloud computing' refers to storing and accessing data and programs, such as documents, photos or videos, over the internet, rather than on a device's hard drive. Cloud computing involves the setting accessing a shared pool of ICT services remotely via a private network or the internet. All staff will be made aware of data protection requirements and how these are impacted by the storing of data in the cloud, including that cloud usage does not prevent data subjects from exercising their data protection rights.

If the cloud service offers an authentication process, each user will have their own account. When assessing any cloud-based or AI-powered service, the setting will ensure that the provider demonstrates UK GDPR compliance, provides explicit guarantees regarding non-retention of input data, and allows the setting to audit or verify compliance where necessary.

The use of any cloud services which involve AI processing will be subject to a prior risk assessment and will require a DPIA where personal data is involved. A system will be implemented to allow user accounts to be created, updated, suspended and deleted, and for credentials to be reset if they are forgotten, lost or stolen. Access for employees will be removed when they leave the setting.

All files and personal data will be encrypted before they leave a work device and are placed in the cloud, including when the data is 'in transit' between the device and cloud. A robust encryption key management arrangement will be put in place to maintain protection of the encrypted data. The loss of an encryption key will be reported to the IT Support Provider immediately; failure to do so could result in accidental access or destruction of personal data and, therefore, a breach of the relevant data protection legislation.

As with files on work devices, only authorised parties will be able to access files on the cloud. An audit process will be put in place to alert the setting should unauthorised access, deletion or modification occur and ensure ongoing compliance.

Cloud providers must:

- ✓ Ensure that the service provider can delete all copies of personal data within a timescale in line with the Data Protection and Retention Policies.
- ✓ Confirm that they will remove all copies of data, including back-ups, if requested.
- ✓ Implement a plan for returning the data should the setting no longer require services, or transfer to another provider securely.
- ✓ Ensure that the platform is secure and backed up appropriately at all times.
- ✓ Generative AI

Forsbrook CE Primary School recognises that generative AI technologies involve the processing of extensive datasets and may pose increased risks to data privacy and security. Staff and pupils must

not input personal, identifiable, or sensitive data into generative AI platforms unless the system has been formally assessed, and explicit approval has been granted following a full DPIA.

Only AI systems that meet UK GDPR standards and have been assessed for data minimisation, security, transparency, and retention practices will be used in school operations. Use of generative AI tools must comply with the Acceptable Use Policy. Individuals must not rely solely on AI-generated outputs without appropriate human oversight and validation.

Any incidents, breaches, or concerns arising from the use of AI tools must be reported immediately.

21. POLICY REVIEW

This policy is reviewed every year.

The policy will be reviewed by the Governing Body and SLT.

The policy will be shared with all staff.

The policy will be uploaded to the website.