Data Protection Policy

Approved by:	Full Governing Body	**Date:** May 2021
Last reviewed on:	December 2024	
Next review due by:	December 2025	

POLICY

1. AIMS

Radford Semele C of E Primary School aims to ensure that all personal data collected about staff, pupils, parents/carers, governors, visitors, volunteers and any other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act 2018 (DPA 2018).

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:

- UK General Data Protection Regulation (UKGDPR) – the EU GDPR was incorporated into UK legislation, with some amendments by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020.
- Data Protection Act 2018 (DPA 2018).

This policy is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR.

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.
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. APPLICATION

This Policy applies to all members of the school community, including, but not limited to, staff, pupils, parents/carers, governors, volunteers and any other individuals about whom the school collects data.

4. DEFINITIONS

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

TERM	DEFINITION
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Criminal convictions data	Personal data relating to criminal convictions and offences, including personal data relating to criminal allegations and proceedings.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
Privacy notice	A separate notice setting out information that may be provided to data subjects when the organization collects information about them.
Data privacy impact assessment (DPIA)	Tools and assessments used to identify and reduce risks of a data processing activity. A DPIA can be carried out as part of 'privacy by design' and will be conducted for all major system or change programmes involving the processing of personal data.

5. DATA CONTROLLER

Radford Semele C of E Primary School processes personal data relating to parents, pupils, staff, governors, visitors, volunteers and others, and therefore is a data controller.

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

6. ROLES & RESPONSIBILITIES

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

6.1. GOVERNING BODY ROLE & RESPONSIBILITIES

The Governing Body has overall responsibility for ensuring that the school complies with all relevant data protection obligations.

6.2. DATA PROTECTION OFFICER'S ROLE & RESPONSIBILITIES

The data protection officer (DPO) is responsible for providing advice and guidance to Radford Semele C of E Primary School in order to assist the school in the implementation of this policy, monitoring compliance with data protection law, and developing related policies and guidelines where applicable.

The DPO will carry out an annual audit of the School's data processing activities and report to the Governing Body 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.

The DPO is the School DPO Service and is contactable via schooldpo@warwickshire.gov.uk or alternatively;

School Data Protection Officer
Warwickshire Legal Services
Warwickshire County Council
Shire Hall
Market Square
Warwick
CV34 4RL

6.3. HEADTEACHER'S ROLE & RESPONSIBILITIES

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

6.4 DATA PROTECTION LEAD

The School has nominated the following individual as designated persons to be contacted internally in relation to all matters relating to data protection issues, and to make referrals, where necessary, to the Data Protection Officer:

Julie Jennings (Data Protection Lead) who is contactable via Jennings.j3@welearn365.com or 01926 426940

6.5. ROLE & RESPONSIBILITIES OF 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 Data Protection Officer 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

7. DATA PROTECTION PRINCIPLES

The GDPR is based on data protection principles that the school must comply with. Radford Semele C of E Primary School has adopted the principles to underpin its Data Protection Policy.

The principles require that all personal data shall be:

- Processed lawfully, fairly and in a transparent manner ("lawfulness, fairness and transparency")
- Used for specified, explicit and legitimate purposes ("purpose limitation")
- Used in a way that is adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed ("data minimisation")
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate are erased or rectified without delay ("accuracy")
- Kept for no longer than is necessary for the purposes for which it is processed ("storage limitation")
- Processed in a manner that ensures it is safe and secure, ensuring that measures against unauthorised or unlawful processing and against accidental loss, destruction or damage are in place ("integrity and confidentiality")

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

8. COLLECTING PERSONAL DATA

8.1. LAWFULNESS, FAIRNESS & TRANSPARENCY

Radford Semele C of E Primary School shall only process personal data where it has 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 or another person, for example, 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 (where the processing is not for any tasks the school performs as a public authority) 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, the school will also meet one of the special category conditions for processing which are set out in the UK GDPR and Data Protection Act 2018:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise of defence of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **pubic health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, the school will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

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

The school will always consider the fairness of any data processing. The school will ensure it does not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

8.2. LIMITATION, MINIMISATION & ACCURACY

The school will only collect personal data for specified, explicit and legitimate reasons. The school will explain these reasons to the individuals when the data is first collected.

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

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

The school will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

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 guidance set out in the school's record retention schedule.

9. SHARING PERSONAL DATA

The school will not normally share personal data with anyone else without consent, but there are certain circumstances where it may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a pupil or parent/carer that puts the safety of school staff at risk
- There is a need to liaise with other agencies – the school will seek consent as necessary before sharing personal data
- Third party suppliers or contractors need data to enable us to provide services to school staff and pupils, for example, IT companies. When doing this, the school 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 shared
    - 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

The school will also share personal data with law enforcement and government bodies where it is 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 safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymized or consent has been provided

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

If the school transfers personal data internationally, it will do so in accordance with data protection law.

10. SUBJECT ACCESS REQUESTS & OTHER RIGHTS OF INDIVIDUALS

10.1. 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
- The safeguards provided if the data is being transferred internally

Subject access requests may be submitted in any form, but the school may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual
- Name of School
- Correspondence address
- Contact number and email address
- Details of the information requested

The DPO will send the subject access request to the Data Protection Lead. If staff receive a subject access request they must immediately forward it to the Data Protection Lead, who will ensure that the DPO is informed.

If staff receive a subject access request in any form they must immediately forward it to the designated Data Protection Lead, who will ensure that the DPO is informed.

10.2. CHILDREN & 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 person should have parental responsibility for the child, and 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 13 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 those with parental responsibility for pupils at the 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, the school:

- 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 (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual the request will be complied with within 3 months, where a request is complex or numerous. The individual will be informed of this within 1 month, with an explanation of why the extension is necessary

The school 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 being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that can't reasonably be anonymised, and the school doesn't have the other person's consent and it would be unreasonable to proceed without it

- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, the school may refuse to act on it, or charge a reasonable fee to cover 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. The school will take into account whether the request is repetitive in nature when making this decision.

Where the school refuses a request, the individuals will be told why the request has been refused and they will also be informed of their right to complain to the ICO or that they can seek to enforce their subject access right through the courts.

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 the school collects their data about how it is used and processed (see section 8), individuals also have the right to:

- Withdraw their consent to processing at any time, where processing is based on the consent of the pupil or parent
- 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
- Object to processing which has been justified on the basis of public task, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- 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 Data Protection Lead who will send it to the DPO for information purposes.

11. 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.

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it.

This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

12. PHOTOGRAPHS & VIDEOS

As part of school activities, photographs and recorded images may be taken of individuals within the school.

The school will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. The school will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Parents/carers are not usually permitted to take photos/videos at school events, however, should the taking of photos/videos be permitted on occasion, any photographs and videos taken by parents/carers must be for their own personal use and are not covered by data protection legislation. However, photos or videos with other pupils must not be shared publicly on social media for safeguarding reasons, uncles all the relevant parents/carers have agreed to this.

Where the school takes photographs and videos, uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on the school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, the photograph or video will be deleted and not distributed further.

When using photographs and videos in this way, unless the school has consent, it will not accompany them with any personal information, other than first name, about the child, to ensure they cannot be identified.

See the child protection and safeguarding policy for more information about the use of photographs and videos.

13. DATA PROTECTION BY DESIGN & DEFAULT

The school will put measures in place to show that it has integrated data protection into all 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 7)
- Considering whether a data protection impact assessment needs to be undertaken. The school will consider this if any of the following kinds of processing are to be undertaken:
    - Use of systematic and extensive automated processing
    - Large scale processing of data, particularly where it involves special category or criminal offence data
    - Systematic monitoring of publicly accessible areas and any other form of surveillance
    - Processing of biometric or genetic data
    - Transfer of data outside of the European Economic Area (EEA)
    - Profiling, evaluation or scoring
    - Automated decision making with legal or significant effects
    - Matching or combining datasets
    - Processing of data concerning vulnerable data subjects
    - Implementation of new technology or solutions
    - If processing would prevent a data subject from exercising a right or using a service or contract

On reviewing these criteria, if the school finds that the processing of personal data presents a high risk to the rights and freedoms of individuals, it will undertake a data protection impact assessment.

- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Training members of staff on data protection law, this policy, any related policies and any other data protection matters; the school will also keep a record of attendance at training
- Regularly conducting reviews and audits to test privacy measures and make sure the school is compliant
- Appropriate safeguards being put in place if any personal data is transferred outside of the European Economic Area (EEA), where different data protection laws will apply
- Maintaining records of the schools processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of the school and DPO and all information the school is required to share about how data is used and processed (via the schools privacy notices)
    - For all personal data that is held, an internal record of the type of data, data subject, how and why the data is used, any third party recipients, how and why the data is being stored, retention periods and how the data is being kept secure, will be maintained

13. DATA SECURITY & STORAGE OF RECORDS

The school 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 stored securely when not in use
- Papers containing confidential personal data will not be left on office or classroom desks, on staffroom tables, pinned to notice boards/displays or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff will sign it in and out from the school office
- Staff must ensure that passwords are hard for anyone else to guess by incorporating numbers and mixed cases into them. Staff and pupils are reminded that they must not reuse passwords from other sites
- 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
- Where the school needs to share personal data with a third party, it will carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

14. DATA SECURITY & STORAGE 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 the school cannot or does not need to rectify or update it.

For example, paper based records will be shredded or incinerated, and electronic files will be deleted or over-written. The school may also use a third party to safely dispose of records on the school's behalf.

Where a third party is used, they will be required to provide sufficient guarantees that they comply with data protection law.

15. 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 it cannot or does not need to be rectified or updated.

For example, the school will shred or incinerate or otherwise confidentially dispose of paper-based records, and overwrite or delete electronic files. The school may also use a third party to safely dispose of records on it's behalf. If the school uses a third party, they will be required to provide sufficient guarantees that they comply with all current data protection legislation.

16. PERSONAL DATA BREACHES

The school will take all reasonable steps to ensure that there are no personal data breaches.

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

When appropriate, the school will report the data breach to the ICO within 72 hours of becoming aware of the breach.

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

17. 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.

18. LEGISLATION AND GUIDANCE

This policy meets the requirements of the GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) and on the GDPR.

19. LINKS TO OTHER DOCUMENTS

This document should be read in conjunction with the following:
- Child Protection & Safeguarding Policy
- Freedom of Information Policy & Publication Scheme
- Information Security Policy
- Records Retention Policy
- On-line Safety Policy
- IT Acceptable Use Policy & Agreement
- Security Incidents and Breach Reporting Policy

20. REVIEW OF POLICY

The Governing Body will review the data protection policy annually. The policy will also be revised as required to introduce any changes in regulation and statutory guidance to ensure that it is always up to date.

APPENDIX 1: PERSONAL DATA BREACH PROCEDURE

If staff become aware that information has not been handled according to procedures and there is a data breach or potential security incident, they must report it in accordance with this procedure.

When appropriate, the school will report the data breach to the ICO within 72 hours in accordance with the requirements of the GDPR.

1. Data protection breaches occur where personal data is lost, damaged, destroyed, stolen, misused and/or accessed unlawfully.

2. Examples of how a breach may occur include:

    a. Theft of data or equipment on which data is stored;
    b. Loss of data or equipment on which data is stored;
    c. Inappropriate access controls allowing unauthorised use;
    d. Accidental Loss;
    e. Destruction of personal data;
    f. Damage to personal data;
    g. Equipment failure;
    h. Unlawful disclosure of personal data to a third party;
    i. Human error;
    j. Unforeseen circumstances such as fire or flood;
    k. Hacking attack; or
    l. 'Blagging' offences where information is obtained by deceiving the organisation which holds it.

3. If any member of staff or governor of the school discovers that data has been lost, or believes that there has been a breach of the data protection principles in the way that data is handled, they must immediately or no later than within 24 hours of it first coming to notice, inform the school's Data Protection Lead, Julie Jennings jennings.j3@welearn365.com.

4. Upon being notified, the school's Data Protection Lead will assess whether a breach of personal information has occurred, and the level of severity. If a breach has occurred but the risk of harm to any individual is low (for example, because no personal information has left the control of the school), then the school's Data Protection Lead will undertake an internal investigation to consider whether the Information Security Policy was followed, and whether any alterations need to be made to internal procedures as a result.

5. In all other cases, the incident must be notified to the Data Protection Officer immediately, who must follow the Information Commissioner's Office guidelines on notification and recording of the breach. The Data Protection Officer will provide advice and support on managing and responding to the data breach and advise whether they consider the incident to be reportable to the ICO. The priority must then be to close or contain the breach to mitigate/minimise the risks to those individuals affected by it.

All staff and governors at Radford Semele C of E Primary School are expected to work in partnership with the Data Protection Lead and the Data Protection Officer in relation to the following matters:

Notification of Breaches

Any member of staff or governor who becomes aware of a personal information breach should provide full details to the Data Protection Lead for the school within 24 hours of being made aware of the breach. The Data Protection Lead will then complete the Data Breach Record Form and Incident Log. When completing the form details must be provided of the reporter's name, the date/time of the breach, the date/time of detecting the breach, and basic information about the type of breach and information about personal data concerned. Details of what has already been done to respond to the risks posed by the breach should also be included.

Containment and Recovery

The initial response is to investigate and contain the situation and a recovery plan including, damage limitation. The school may need input from specialists such as IT, HR and legal and in some cases contact with external third parties.

- Seek assistance in the containment exercise. This could be isolating or closing a compromised section of the network, recovery of released documents, finding a lost piece of equipment or simply changing any related access codes
- Establish whether there is anything that can be done to recover any losses and limit the damage the breach can cause.
- As well as the physical recovery of equipment, this could involve the use of backup records to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts.
- Consider whether any individual affected by the data breach should be notified

Assessing the Risks

Levels of risk can be very different and vary on an individual breach of data security depending what is lost/damaged/stolen. For example, if a case file is lost then risks are different depending on type of data and its sensitivity with potential adverse consequences for individuals. The Data Protection Lead should consider the following points:

- What type of data is involved?
- How sensitive is the data?
- If data has been lost or stolen, are there any protections in place such as encryption?
- What has happened to the data?
- If data has been stolen, could it be used for purposes which are harmful to the individuals to whom the data relate? If it has been damaged, this poses a different type and level of risk.
- Regardless of what has happened to the data, what could the data tell a third party about the individual? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people
- How many individuals' personal data has been affected by the breach?
- Who are the individuals whose data has been breached?
- What harm can come to those individuals?
- Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
- Are there wider consequences to consider such as a risk to life?
- Loss of public confidence in the school?

All staff and governors should establish whether there is anything they can do to recover any losses and limit the damage the breach can cause.

APPENDIX 2: APPROPRIATE POLICY DOCUMENT

1. ABOUT THIS POLICY

The Data Protection Act 2018 sets out the requirement to have an appropriate policy document when processing special category data and criminal offence data.

To fulfil the duties and function as a school, there is a requirement to process personal information that is listed within Schedule 1 of the Data Protection Act 2018. Most of the processing within Schedule 1 of the Data Protection Act 2018 is required to have an appropriate policy document in place.

This is the appropriate policy document for Radford Semele Church of England Primary School, setting out how special categories of personal data and criminal convictions data will be protected.

2. WHY THE SCHOOL PROCESSES SPECIAL CATEGORIES OF PERSONAL DAAT AND CRIMINAL CONVICTIONS DATA

The school processes special categories of Personal Data and Criminal Convictions Data for the following purposes:

- Assessing an employee's fitness to work
- Complying with health and safety obligations
- Complying with the Equality Act 2010
- Checking applicants and employees' right to work in the UK
- Verifying that candidates are suitable for employment or continued employment
- To safeguard pupils, staff and the community
- To support pupils, staff and visitors who have medical conditions or a disability
- To support pupils with Special Educational Needs (SEN)
- To meet the legal and ethical duties for the provision of education

Where the school processes special categories of personal data and criminal convictions data, it will identify the lawful basis under both Article 6 and Article 9 of the UK GDPR and, where appropriate, identify the condition within Schedule 1 that allows for the processing.

Processing subject to Schedule 1 of the Data Protection Act 2018:

PROCESSING CONDITION FOR SPECIAL CATEGORIES OF PERSONAL DATA	DESCRIPTION OF PROCESSING
Schedule 1, Part 1 – Conditions relating to employment, social security and social protection	Processing data concerning health where there is a duty outlined under employment law. Processing data concerning criminal convictions under Article 10 of the UK GDPR where we have a duty under employment law for recruitment, discipline, and dismissal. To comply with statutory guidance for safer recruitment. Processing information relating to Trade Union Membership to facilitate the right and preference to participate as a member of any trade union, and where there is industrial action that may impact the function of the school.
Schedule 1, Part 2 – Substantial public interest conditions	**Statutory etc. and government purposes:** • Compliance with legal obligations and support the provision of education, such as completing the school census, providing a common transfer file, to support pupils with medical conditions, to support pupils with special educational needs • Compliance with legal obligations in connection with legal proceedings • The school may also process criminal offence data under this condition
	Equality of opportunity and treatment • To provide equal access to education • Compliance with legislation, including the Equality Act 2010 • To ensure equality of treatment
	Preventing and detecting unlawful acts • To comply with the duty to safeguard pupils and the community • To reduce risks to pupils, staff and visitors • Sharing information with relevant and authorised agencies to support the prevention or investigations of unlawful acts.
	Protecting the public against dishonesty • Assisting other agencies in connection with regulatory requirements • Protect and safeguard pupils and the community

PROCESSING CONDITION FOR SPECIAL CATEGORIES OF PERSONAL DATA	DESCRIPTION OF PROCESSING
	Support for individuals with a disability or medical condition • To ensure all pupils and staff are safe at all times • To ensure all pupils can access education and other services in school • To ensure all school employees are properly supported and able to do their job
	Counselling • To allow for individuals to access confidential counselling services as arranged through occupational health or other support services
	Safeguarding of children and individuals at risk • To protect and safeguard pupils from physical and emotional harm, neglect or abuse • To support the wellbeing of pupils at the school
	Insurance To process data that is required for insurance purposes
	Occupational pensions To meet the school's legal obligations to provide a pension scheme for the workforce
Schedule 1, Part 3 – Additional conditions relating to criminal convictions, etc….	Criminal offence data is processed for the purposes of recruitment and employment vetting, The school may also process criminal offence data to protect and safeguard pupils, staff and the wider school community

3. PERSONAL DATA PROTECTION PRINCIPLES

3.1. The UL GDPR requires personal data to be processed in accordance with the six principles set out in Article 5(1). Article 5(2) requires controllers to be able to demonstrate compliance with Article 5(1).

3.2. The school complies with the principles relating to the processing of personal data set out in the UK GDPR which requires personal data to be:

3.2.1. Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency
3.2.2. Collected only for specified, explicit and legitimate purposes (Purpose Limitation)
3.2.3. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (Data Minimisation)
3.2.4. Accurate and, where necessary, kept up to date (Accuracy)
3.2.5. Not kept in a form which permits identification of the data subjects for longer than is necessary for the purposes for which the data is processed (Storage Limitation)

3.2.6. Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality)

3.3. The school is responsible for and must be able to demonstrate compliance with the data protection principles outlined above (Accountability).

4. COMPLIANCE WITH DATA PROTECTION PRINCIPLES

4.1. Lawfulness, fairness and transparency

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

The school will only process personal data fairly and lawfully and for specified purposes. The UK GDPR restricts the actions the school can take regarding personal data to specified lawful purposes. The school can process special categories of personal data and criminal convictions data only if there is a legal ground for the processing and one of the specific processing conditions relating to special categories of personal data applies. The school will identify and document the legal ground and specific processing condition relied on for each processing activity.

When collecting special categories of personal data and criminal convictions data from data subjects, either directly from data subjects or indirectly (for example, from a third party or publicly available source), the school will provide data subjects with a privacy notice setting out all the information required by the UK GDPR which is concise, transparent, intelligible, easily accessible and in clear, plain language which can be easily understood.

4.2. Purpose limitation

Personal data must be collected only for specified, explicit and legitimate purposes. The data must not be further processed in any manner incompatible with those purposes.

The school will only collect personal data for specified purposes and will inform data subjects what those purposes are in a published privacy notice. The school will not use personal data for new, different or incompatible purposes from those disclosed when it was first obtained unless the data subject has been informed of the new purposes and they have consented where necessary.

4.3. Data minimisation

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

The school will only collect or disclose the minimum personal data required for the purposes for which the data is collected or disclosed. The school will ensure that it does not collect excessive data and that the personal data collected is adequate and relevant for the intended purposes.

4.4. Accuracy

Personal data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

The school will ensure that the personal data held and used is accurate, complete, kept up to date and relevant to the purpose for which it is collected. The school will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. The school will take all reasonable steps to destroy or amend inaccurate or out-of-date personal data.

4.5. Storage limitation

The school will only keep personal data in an identifiable form for as long as is necessary for the purpose for which it was collected, or where there is a legal obligation for the school to do so. Once the personal data is no longer needed it will be deleted or rendered permanently anonymous.

The school maintains a Data Retention Policy and related procedures to ensure that personal data is deleted after a reasonable period of time has elapsed for the purposes for which it was being held, unless there is a legal requirement to retain the data for longer.

The school will ensure that data subjects are informed of the period for which data is stored and how that period is determined in any applicable privacy notice.

4.6. Security, integrity and confidentiality

Personal data shall be 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.

The school will implement and maintain reasonable and appropriate security measures against unlawful or unauthorised processing of personal data and against the accidental loss of or damage to personal data.

4.7. Accountability principle

The school is responsible for, and able to demonstrate compliance with these principles. The school's DPO is responsible for ensuring that the school is compliant with these principles. Any questions about this policy should be submitted to the DPO>

The school will:

4.7.1. Ensure that records are kept of all personal data processing activities, and that these are provided to the Information Commissioner on request
4.7.2. Carry out a DPIA for any high-risk personal data processing to understand how processing may affect data subjects and consult the Information Commissioner if appropriate
4.7.3. Ensure that a DOP is appointed to provide independent advice and monitoring of personal data handling, and that the DPO has access to report to the highest level of management
4.7.4. Have internal processes to ensure that personal data is only collected, used, or handled in a way that is compliant with data protection law

4.8. Controller's policies on retention and erasure of personal data

The school takes the security of special categories of personal data and criminal convictions data very seriously. The school has administrative, physical and technical safeguards in place to protect personal data against unlawful or unauthorised processing, or accidental loss or damage. The school will ensure that, where special categories of personal data or criminal convictions data is processed, that:

4.8.1. The processing is recorded, and the record sets out, where possible, a suitable time for the safe and permanent erasure of the different categories of data in accordance with our Data Retention Policy and the relevant retention schedules.

4.8.2. Where the school no longer requires special categories of personal data or criminal convictions data for the purposes for which it was collected, the school will delete it or render it permanently anonymous as soon as possible

4.8.3. Where records are destroyed, the school will ensure that they are safely and permanently disposed of

4.8.4. Data subjects receive a privacy notice setting out how their personal data will be handled when first obtained, including information about how retention periods are determined. The privacy notice is also available on the school website.

5. REVIEW

This Appropriate Policy Document will be reviewed annually, alongside the Data Protection Policy (please see review dates detailed on the header page of the Data Protection Policy).

It will be retained where we process special categories of personal data and criminal convictions data and for a period of at least six months after any such processing is ceased.

A copy of this policy document will be provided to the Information Commissioner on request and free of charge.

For further information about our compliance with data protection law, please contact our Data Protection Lead at the details specified in the Data Protection Policy, or our Data Protection Officer at the School DPO Service, Warwickshire Legal Service, Shire Hall, Warwick, or email schooldpo@warwickshire.gov.uk (when contacting the DPO, please state which school your query relates to).