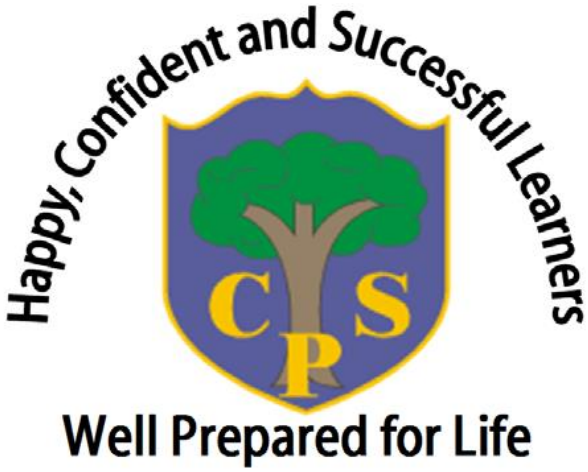


The Coppice Primary School GDPR Data Policy

Written by	Claire Emery
Approved by Governors	July 2021
Date for Review	July 2022

Data Protection Statement
The procedures and practice created by this Policy have been reviewed in the light of our GDPR Data Protection Policy.

All data will be handled in accordance with the School's GDPR Data Protection Policy.

Name of Policy	Content	Reason for Policy	Who does it relate to?	Where is it stored?
Data Protection Policy (inc GDPR and Freedom of Information)	Guidelines for staff in relation to data protection	To ensure staff follow the guidelines	All staff	Network drive

As such, our assessment is that this Policy:

Has Few / No Data Compliance Requirements	Has A Moderate Level of Data Compliance Requirements	Has a High Level Of Data Compliance Requirements
		✓

Purpose

This Policy sets out the basis on which the School will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources. It does not form part of any employee's contract of employment and may be amended at any time.

The Policy meets the requirements and expectations of the General Data Protection Regulation introduced in law as of the 25th May 2018 and the Freedom of Information Act 2000.

Those who are involved in the processing of personal data are obliged to comply with this Policy when doing so. Any breach of this Policy may result in disciplinary action.

General Statement of Duties

The School is required to process relevant personal data regarding individuals as part of its operation and shall take all reasonable steps to do so in accordance with this Policy. Processing may include obtaining, recording, holding, disclosing, destroying or otherwise using data.

Data Protection Officer

The School has appointed Claire Emery as Data Protection Officer (DPO), who will endeavour to ensure that all personal data is processed in compliance with this Policy and the principles of the Act. Any questions about the operation of this Policy or any concerns that the Policy has not been followed should be referred in the first instance to the DPO. Overall responsibility for data protection lies with the Headteacher.

The Data Protection Principles

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

- Fairly and lawfully processed
- Processed for a lawful purpose
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Not kept for longer than necessary
- Processed in accordance with the data subject's rights
- Secure
- Not transferred to other countries without adequate protection

Types of Personal Data processed by the School for pupils, parents and carers

Personal data covers both facts and opinions about an individual. The School may process a wide range of personal data about individuals including current, past and prospective pupils and their parents as part of its operation, including, by way of example:

- Personal information (such as name, date of birth, copy of birth certificate, unique pupil number, parental responsibility and address)
- Educational History (previous schools or nurseries)
- Characteristics (such as gender, racial or ethnic origin, language, nationality, country of birth and free school meal eligibility)
- Religious or other beliefs of a similar nature
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information (such as internal tests, student progress information and examination results)

- Medical information (such as allergies, healthcare plans, medication, specific medical needs, medical incidents that have occurred inside or outside of school that may affect learning, dietary needs, outside agency referrals and Doctor's contact details)
- Health & Safety information (such as records of minor injuries and information that is required to comply with the Health & Safety Executive (HSE) RIDDOR requirements.
- Special Educational Needs and Disabilities information (such as specific learning difficulties, EHCPs, outside agency referrals and previous learning, physical or mental health needs)
- Safeguarding information (detail of disclosures, outcomes of meetings, various plans and sensitive information regarding court proceedings, child protection plans and correspondence with outside agencies.)
- 'Looked After Child' status
- Contact information (such as telephone numbers of contacts that the school would contact in an emergency)
- Behavioural information (such as rewards, achievements, incident slips and exclusions)
- Static and moving images (such as photographs of pupils and video recordings)
- Financial information (such as parent's bank details for donations)

Similarly, the School may process a wide range of personal data about employees, volunteers, Trustees and Members, as part of its operation, including, by way of example:

- personal information (such as name, employee or teacher number, national insurance number)
- special categories of data including characteristics information such as gender, age, racial or ethnic group
- contract information (such as start dates, hours worked, post, roles and salary information)
- medical information (such as health declaration and allergies)
- work absence information (such as number of absences and reasons);
- qualifications (and, where relevant, subjects taught)
- contact information (such as telephone numbers of contacts that an employee would want the school to contact in an emergency)
- address information
- payroll information (such as bank account numbers for payment transfers)
- DBS – Disclosure Barring Service
- References and previous employment information
- Where applicable Drivers License details

Sensitive personal data

The School may, from time to time, need to process sensitive personal data regarding individuals. Sensitive personal data includes information about racial or ethnic origin, religion, nationality, country of birth, Armed Forces parent, educational history and medical information. Sensitive personal data is entitled to special protection under the Act, and will only be processed by the School with the explicit consent of the appropriate individual, or as otherwise permitted by the Act. The consent should be informed, which means it needs to identify the relevant data, why it is being processed and to whom it will be disclosed. Parents and staff should contact the DPO for more information on obtaining consent to process sensitive personal data.

Use of personal data by the School

The School will use (and where appropriate share with third parties) personal data about individuals for a number of purposes as part of its operations, including as follows:

We use the pupil information:

- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate care and guidance

- to assess the quality of our services
- to comply with the law regarding data sharing
- to make certain payments to eligible pupils
- to comply with statutory request for data from relevant authorities

We use School workforce data to:

- enable the development of a comprehensive picture of the workforce and how it is deployed
- inform the development of recruitment and retention policies
- enable individuals to be paid
- to contact you directly when you are not on the premises
- to contact others known to you, where you have provided their information, in cases where it would be reasonable for us to contact that individual
- to check for criminal convictions
- for recruitment purposes
- To obtain insurance

Access requests to personal data

Under data protection legislation, parents and staff have the right to request access to information that we hold about them. All requests should be made to the Data Protection Officer (DPO) – Claire Emery at cle38@coppice.worcs.sch.uk

Parents and staff rights

Everyone has rights with regard to the way in which their personal data is handled. It is recognised that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

Parents and staff have the rights to:

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

Exemptions

Certain data is exempted from the provisions of the Act, including the following:

- The prevention or detection of crime
- The assessment of any tax or duty
- Where the processing is necessary to exercise a right or obligation conferred or imposed by law upon the School
- Information which might cause serious harm to the physical or mental health of the pupil or another individual
- Cases where the disclosure would reveal a child is at risk of abuse
- Information contained in adoption and parental order records
- Information given to a court in proceedings under the Magistrates' Courts (Children and Young Persons) Rules 1992
- Copies of examination scripts; and
- Providing examination marks before they are officially announced

Disclosure of information

The School routinely shares student and parent information with:

- Schools and other educational environments that the students attend after leaving us
- Our Local Authority (LA)
- The National Pupil Database (NPD)
- The Department for Education (DfE) – We share students' data with the DfE on a statutory basis under Regulation 5 of The Education (Information About Individual Pupils) (England) Regulation 2013. This data sharing underpins school funding and educational attainment policy and monitoring. We are required, by law, to provide information about our students to the DfE as part of statutory data collections such as the school census. Some of this information is then stored in the NPD.
- The Police and Law Enforcement
- The School Nursing Team
- Standards and Testing Agency and NCA tools (SATS)
- Social Services
- Organisations which provide school milk (such as Cool Milk)
- Organisations which provide school photographs (such as Aperture)
- Organisations which provide sign in systems (such as e-Reception Book)
- Organisations which provide Information Management Services (such as SIMs)
- Organisations which provide data collection, integration with Management Information Services and reporting services (such as Wonde)
- Organisations which provide learning tools (such as Mymaths, Spell Shed)
- Organisations which provide school pupil tracking systems (such as Insight Tracking, Early Excellence)
- Organisations which provide payment systems – (such as Parentpay)
- Organisations which provide communication services (such as PS Connect)
- Other local authorities if they have responsibility for a child has SEN/LAC
- Daily attendance will be shared with the local authority's commissioned service for all 'Looked After Children' attending The Coppice Primary

The School routinely shares employee information with:

- Our Local Authority (LA)
- The Department for Education (DfE) including through GIAS (Edubase)
- Office for National Statistics (ONS)
- Teacher Pensions
- Local Government Pension Scheme (LGPS)
- Companies House
- Organisations which provide staff absence insurance (such as SAS)
- Organisations which provide quotes for medical insurance (such as Gallaghers)
- Organisations which provide motor insurance to enable staff to drive the school mini bus (such as AON)
- Organisations which provide communication services (such as PS Connect)

Accuracy

The School will endeavour to ensure that all personal data held in relation to an individual is as up-to-date and accurate as possible. Individuals must notify the DPO of any changes to information held about them.

Timely Processing

The School will not keep personal data longer than is necessary for the purpose or purposes for which they were collected and will take all reasonable steps to destroy, or erase from its systems, all data which is no longer required. Retention details will be included in the Pupil Data Consent forms.

Enforcement

If an individual believes that the School has not complied with this Policy or acted otherwise than in accordance with the Act, they should utilise the School's complaints procedure and should also notify the DPO.

Data Security

The School will take appropriate technical and organisational steps to ensure the security of personal data about individuals, and to ensure that members of staff will only have access to personal data relating to pupils, their parents or guardians where it is necessary for them to do so. All staff will be made aware of this Policy and their duties under the Act.

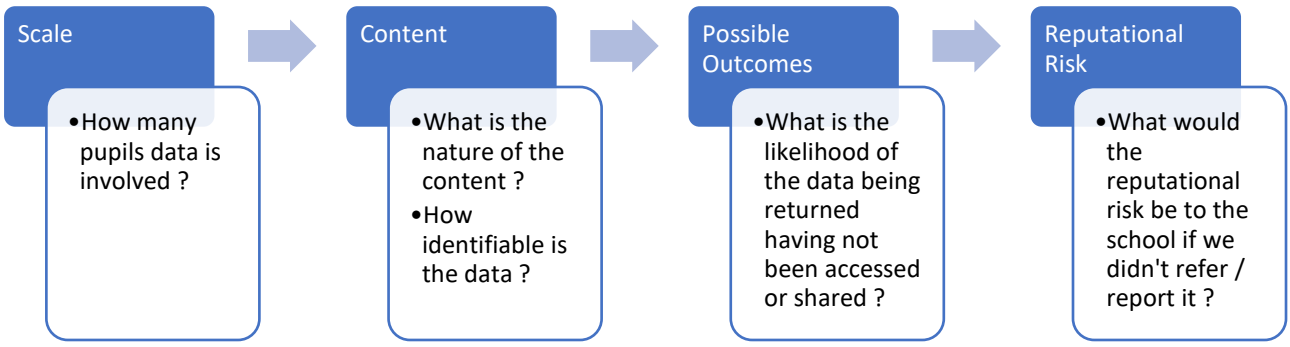
The School must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of or damage to, personal data. Members of staff are only permitted to remove electronic personal data from School premises on an encrypted memory stick. Paper forms are allowed to be taken offsite with regard to safeguarding eg for trips and then is shredded when no longer needed.

Data Breaches

The School takes seriously any data breach and will, through its policy and practice endeavour to minimise the risk of a breach. To minimise the risk of a data breach, staff will follow the confidential system procedures in place to protect personal data and student records and if a breach in data security occurs, it shall be reported to the DPO immediately.

In the rare circumstances surrounding a data breach a process will be followed (appendix A).

The GDPR states that breaches should be referred to the Information Commissioners Office (ICO) within 72 hours of disclosure. However, it is appropriate for our School to consider the following factors before referring to the ICO:



Complaints

Complaints related to the management of data in our School will be handled through our existing Complaints Procedure. Copies of which are available on the School website or from the School office upon request.

Transparency and Accountability

To ensure that the School is open and transparent about what data it holds and how it will be managed, the School will bear in mind the following eight principles in all that it does:

The School will provide every parent with information in relation to their data rights. In addition, it will also provide every new parent with a privacy notice. This notice will outline the aspects of data that the School will gather and use, as well as stating their purpose, their 'shelf-life' and where it may be shared. Parents will be asked to acknowledge their understanding of this information and accept the reasoning and processing that may occur.

School Website

The School will establish a page on its website to ensure that its approaches, policies and practices in relation to data are transparent. It will provide parents with information that may be relevant to their data concerns. It will include:

- Information about the School's Data Protection Officer (name, contact details etc)

- Copies of relevant policies
- Data review and amendment request forms
- Process flowcharts
- Complaints Policy

Introducing a new Initiative or project

The GDPR requires schools to undertake an evaluation of the data management impact resulting from new initiatives.

The School's rights to refuse a request

The School reserves the right to refuse a request to view or amend data held. This would be rare and only on the following basis:

- Vexatious requests
- Where information held maybe required by future legal processes e.g. Child Protection
- The request would lead to inaccurate and misleading information being recorded
- The request has come from an individual who has no rights of access

Where the School decides not to adhere to a request it will notify the person who requested:

- The reason why the request has been refused
- Their legal rights of appeal or complaint
- Their legal rights of referral to the ICO

Charges

The School will not usually make a charge in relation to data viewing or amendment requests. However, it reserves the right to do so where the request is proven to be:

- Vexatious
- Excessive
- Unfounded

Generic Policies

The School will undertake to review all of its policies (curriculum, safety, statutory etc) to ensure that any potential data management issues are identified and resolved. The review statement will accompany the relevant document.

Transitional Period

The introduction of the GDPR has required the School to undertake a significant review of policy and practice in relation to data. Throughout this period we will keep the implementation under regular review. This will be undertaken by:

- Termly data protection audits
- Termly reports to Trustees by the School's DPO
- An annual data statement

Appendix A – Data Breach Process Flowchart