



Data Protection Policy

Policy approved and adopted: May 2020

Review date: May 2023

This document is a statement of the aims and principles of Cove Junior School for ensuring the confidentiality of sensitive information relating to staff, pupils, parents and governors.

Introduction

We collect and use personal information (referred to in the General Data Protection Regulation (GDPR) as personal data) about staff, pupils, parents, governors, volunteers, third party contractors and suppliers, and other individuals who come into contact with the school. This information is gathered to:

- Enable the provision of education to the pupils in the school
- Ensure their welling-being and safety
- Support their social, moral, cultural, spiritual, and economic development
- Make them secondary school ready
- Enable them to participate in and contribute to the wider community, and for other associated purposes

We also collect information for purposes associated with the provision of the above including administration of employment contracts, staff pay and performance, staff health and well-being, staff development, administration of third party contracts, and the provision of services to the school that support the main education function.

In addition, we are required by law to collect, use and share certain information, including, for example, pupil performance data, attendance data, and equalities data, with (amongst others) the Department for Education and our local education authority.

The school is the Data Controller, of the personal data that it collects and receives for these purposes.

The school has a Data Protection Officer, Mrs Zoe Fuller, who may be contacted at adminoffice@cove-jun.hants.sch.uk or via the school office on 01252 542941.

The school issues Privacy Notices (also known as Fair Processing Notices) to all parents and staff. These summarise the personal information held about pupils and staff, the purpose for which it is held and who it may be shared with. It also provides information about an individual's rights in respect of their personal data .

Purpose

At Cove Junior School, we aim to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR).

This policy sets out how the school deals with personal information correctly and securely and in accordance with the GDPR, and other related legislation.

This policy applies to all personal information however it is collected, used, recorded and stored by the school and whether it is held on paper or electronically.

What is Personal Information/ Data?

Personal information or data means any information relating to an identified or identifiable individual. An identifiable individual is one who can be identified, directly or indirectly by reference to details such as a name, an identification number, location data, an online identifier or by their physical, physiological, genetic, mental, economic, cultural or social identity. Personal data includes (but is not limited to) an individual's, name, address, date of birth, photograph, bank details and other information that identifies them.

Special Category Data

Special category data (formerly sensitive personal data) is personal information which is considered to be more sensitive and/or to require more protections. This includes information as to race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life or sexual orientation.

The GDPR prohibits the collection, use and sharing of such information, except on specified and limited grounds, including:

- To comply with employment and/or social security law
- If it is in the vital interests of the data subject
- Processing of the information has been disclosed publicly by the data subject
- It is necessary for preventive medical or occupational health needs
- The assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment
- Processing is necessary for archiving purposes in the public interest
- Scientific or historical research purposes
- Statistical purposes
- Where consent is given

Data Protection Principles

The GDPR establishes six principles as well as a number of additional duties that must be adhered to at all times:

1. Personal data shall be processed lawfully, fairly and in a transparent manner
2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (subject to exceptions for specific archiving purposes)
3. Personal data shall be adequate, relevant and limited to what is necessary to the purposes for which they are processed and not excessive
4. Personal data shall be accurate and where necessary, kept up to date
5. Personal data shall be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
6. Personal data shall be processed in a manner that ensures appropriate security of the individual

Duties

Personal data shall not be transferred to a country or territory outside the European Economic Area (EEA), unless that country or territory ensures an adequate level of data protection. Data Controllers have a General Duty of accountability for personal data.

Commitment

The school is committed to maintaining the principles and duties in the GDPR at all times. Therefore the school will:

- Inform individuals of the identity and contact details of the data controller
- Inform individuals of the contact details of the Data Protection Officer
- Inform individuals of the purposes that personal information is being collected and the basis for this
- Inform individuals when their information is shared, and why and with whom unless the GDPR provides a reason not to do this
- If the school plans to transfer personal data outside the EEA, the school will inform individuals and provide them with details of where they can obtain details of the safeguards for that information
- Inform individuals of their data subject rights
- Inform individuals that the individual may withdraw consent (where relevant) and that if consent is withdrawn, that the school will cease processing their data although that will not affect the legality of data processed up until that point
- Provide details of the length of time an individual's data will be kept
- Should the school decide to use an individual's personal data for a different reason to that for which it was originally collected, the school shall inform the individual and where necessary seek consent
- Check the accuracy of the information it holds and review it at regular intervals
- Ensure that only authorised personnel have access to the personal information whatever medium (paper or electronic) it is stored in
- Ensure that clear and robust safeguards are in place to ensure personal information is kept securely and to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Ensure that personal information is not retained longer than it is needed
- Ensure that when information is destroyed that it is done so appropriately and securely
- Share personal information with others only when it is legally appropriate to do so
- Comply with the duty to respond to requests for access to personal information (known as Subject Access Requests)
- Ensure that personal information is not transferred outside the EEA without the appropriate safeguards
- Ensure that all staff and governors are aware of and understand these policies and procedures

Photographs and videos

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

Uses may include:

- Within school on notice boards and in school newsletters.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website

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

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

Data security and storage of records

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

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key, or are password protected, when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- 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 we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected

Disposal of records

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

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

Breaches of GDPR

- The school will make all reasonable endeavours to ensure that there are no personal data breaches
- When appropriate, the school will notify the Information Commissioner's Office (ICO) within 72 hours of the breach occurring or within 72 hours of the school becoming aware of the breach
- If the breach represents a high data risk, for example, the publication of personal financial information to a non-authorised third party, the school will, in accordance with GDPR immediately notify the Data Subject of the breach
- The school will thereafter review its procedures to ensure that it minimises the risk of a future similar breach

Complaints

Complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to the handling of personal information may be referred to the Information Commissioner who can be contacted at Wycliffe House, Water Lane Wilmslow Cheshire SK9 5AF or at www.ico.gov.uk

Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years. The policy review will be undertaken by the Data Protection Officer, Headteacher, and the Governing Body.

Contacts

If you have any enquires in relation to this policy, please contact the Data Protection Officer via the school office.

Appendix 1: Personal data breach procedure

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

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
 - Lost
 - Stolen
 - Destroyed
 - Altered
 - Disclosed or made available where it should not have been
 - Made available to unauthorised people
- The DPO will alert the headteacher and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
 - Loss of control over their data
 - Discrimination
 - Identify theft or fraud
 - Financial loss
 - Unauthorised reversal of pseudonymisation (for example, key-coding)
 - Damage to reputation
 - Loss of confidentiality
 - Any other significant economic or social disadvantage to the individual(s) concerned

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

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school's computer system.
- Where the ICO must be notified, the DPO will do this via the ['report a breach' page of the ICO website](#) within 72 hours. As required, the DPO will set out:
 - A description of the nature of the personal data breach including, where possible:
 - The categories and approximate number of individuals concerned
 - The categories and approximate number of personal data records concerned
 - The name and contact details of the DPO
 - A description of the likely consequences of the personal data breach
 - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
 - The name and contact details of the DPO
 - A description of the likely consequences of the personal data breach
 - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
 - Facts and cause
 - Effects
 - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on the school's computer system.

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

Actions to minimise the impact of data breaches

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

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Other types of breach that may need to be considered could include:

- Details of pupil premium interventions, for named children, being published on the school website
- Non-anonymised pupil exam results or staff pay information being shared with governors
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- The school's cashless payment provider being hacked and parents' financial details stolen