Charles Kingsley's CE Primary School



PART OF CKS GDPR 2018 COMPLIANCE

DATA PROTECTION POLICY

Reviewed by the Governing Body: Autumn Term 2026

Next Review: Autumn Term 2028

_____ _____

Headteacher **Date**

_____ _____

Chair of Committee **Date**

1. INTRODUCTION

Purpose

This policy sets out how Charles Kingsley's (CE) Primary School (the School) deals with personal information (referred to in the UK General Data Protection Regulation (UKGDPR) as personal data, and related legislation.

This policy applies to all personal data however it is collected, used, recorded and stored by the School.

Review

This Policy will be reviewed every 2 years or as required. The review will be undertaken by the Head Teacher, and a nominated Governor Representative.

Contacts

For Policy enquiries or subject access requests, contact the School Data Protection Officer.

2. The School and Personal Data

Personal Data & Sensitive Personal Data

Personal 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 typically includes (but is not limited to) an individual's name, address, date of birth, photograph, bank details etc.

Sensitive Personal Data in the School context includes information of an individual's racial or ethnic origin, religious beliefs or beliefs of a similar nature, whether they are a member of a trade union, their physical or mental health or condition, sexual life, the commission or alleged commission of an offence and associated proceedings.

The School and UKGDPR

The School collects and uses Personal Data about staff, pupils, parents/carers and others who come into contact with the School. This enables the School to pursue its legitimate interests, namely the provision of education and associated functions. The School may also be required by law to collect, use and share certain information.

With resepct to the terms of the UKGDPR:

The School is the **Data Controller.**

The School has a **Data Protection Officer** who is responsible for all aspects of Personal Data Management. At the time of writing, this is Sarah Turner - s.turner@charleskingsleys.hants.sch.uk.

The School issues **Privacy Notices** (also known as Fair Processing Notices) to all pupils/parents, staff, volunteers and Governors. These summarise:

- the general Personal Data held about pupils, staff, volunteers and Governors;
- the purpose for which it is held;
- who it is shared with;
- an individual's rights in respect of their Personal Data.

3. UKGDPR And Data Protection Principles

The School adheres to the six principles contained within the UKGDPR, as well as a number of additional duties that must be complied with at all times. Personal Data shall be:

1. Processed lawfully, fairly and in a transparent manner;
2. 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. Adequate, relevant and limited to what is necessary to the purposes for which they are processed;
4. Accurate and, where necessary, kept up to date;
5. Kept in a form that permits the identification of data subjects for no longer that is necessary for the purposes for which the Personal Data are processed;
6. Processed in a manner that ensures appropriate security of the personal.

4. Duties

Personal data shall not be transferred to a country or territory outside the UK unless that country or territory ensures an adequate level of data protection.

Data Controllers have a Gerenal Duty of accountability for personal data.

5. Commitment to the Principles

In its commitment to these principles, the School will:

Inform

- Inform individuals of the identity and contact details of the Data Controller and Data Protection Officer;
- Inform individuals of the purpose and basis for Personal Data being collected;
- Inform individuals when their information is shared, and why and with whom, unless the UKGDPR provides a reason not to do this;
- Inform individuals of their Data Subject rights;
- Inform individuals that they may withdraw consent (where relevant) and, if that 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;
- If 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;
- If the School plans to transfer Personal Data outside the UK, the School will inform individuals where they can obtain details of the safeguards for that information;

Accuracy

- Check the accuracy of the information it holds and review it at regular intervals.

Storage/Security

- Ensure that clear and robust safeguards are in place to ensure Personal Data is kept securely and to protect Personal Data from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded;
- Ensure that Personal Data is not transferred outside the UK without the appropriate safeguards;
- Ensure that only authorised personnel have access to the Personal Data whatever medium (paper or electronic) it is stored in;

Retention

- Provide details of the length of time Personal Data will be kept;
- Ensure that Personal Data is not retained longer than is needed;
- Ensure that when information is destroyed that it is done so appropriately and securely;

Sharing

- Share Personal Data with others only when it is legally appropriate to do so.

Access

- Comply with the duty to respond to requests for access to Personal Data (known as Subject Access Requests).
- All School staff and Governors involved with the collection, use, processing or disclosure of Personal Data will be aware of their duties and responsibilities and will adhere to this Policy.

6. General Staff Guidelines

- The School will provide training to all employees to help them understand their Data responsibilities;
- The only people able to access Personal data will be those who need it for their work;
- Data will not be shared informally. When access to confidential information is required, staff may request it from the Head teacher, SLT member or the Data Protection Officer;
- Employees will keep all data secure, by taking sensible precautions and following the guidelines below: -
    - Strong passwords must be used and never shared.
    - Personal Data will not be disclosed to unauthorised people.
    - Data will be regularly reviewed and updated if it is found to be out of date. If no longer required, it will be deleted and/or disposed of.
    - Employees will request help from the Head Teacher or the School Data Protection Officer if they are unsure about any aspect of Data Protection.

7. Data Storage

Questions about storing data safely can be directed to the Head Teacher or the Data Protection Officer.

Paper

Data stored on paper, or where printed from electronic sources, will be kept in a secure place where unauthorised people cannot see or access it.

- Paper or files will be kept in a locked drawer or filing cabinet when not in use.
- Staff will make sure paper and printouts are not left where unauthorised people could see or access them.
- Data printouts will be shredded and disposed of securely when no longer required.

Electronic

When data is stored electronically, it will be protected from unauthorised access, accidental deletion and malicious hacking attempts by:

- The use of strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these are be kept locked away securely when not in use.
- Data is only stored on designated School drives and servers and may only be uploaded to approved cloud computing services.
- Data is never be saved directly to laptops or other mobile devices like tablets or smart phones.
- Servers containing Personal Data are sited in a secure location, away from general office space.
- Data is backed up frequently. Those backups are tested regularly, in line with the School's standard backup procedures.
- All servers and computers containing data are be protected by approved security software and a firewall.

8. Data Use

It is when Personal Data is accessed and used that it can be at the greatest risk of loss, corruption or theft. Therefore:

- Staff will ensure the screens of their computers are always locked when left unattended;
- Personal Data will not be shared informally;
- Personal Data will be risk assessed before being transferred electronically through any secure system;
- Personal Data will never be transferred outside of the UK;
- Employees will not save copies of Personal Data to their own computers and will always access and update the central copy of any data.

9. Data Accuracy

- All staff who work with Personal Data will take reasonable steps to ensure it is accurate and up to date as possible.
- Staff will take every opportunity to ensure data is updated, as appropriate.
- Data will be held in as few places as necessary. Staff must not create any unnecessary additional data sets.
- The School will make it easy for Data Subjects to update the information held about them via the Data Protection Officer
- Data will be updated as inaccuracies are discovered.

10. Disclosing Data to Third Parties

Data may be also disclosed to the certain third parties without consent: -

- **Other Schools** - When a child transfers schools, their academic records and health and welfare data will be forwarded onto the new school. This supports a smooth transition and ensures that the child is provided for correctly.
- **Health authorities** - In the interest of public health, the School may share information regarding the health of a child to monitor and avoid the spread of contagious diseases.
- **Police & Courts** - For a criminal investigation, the School may have to forward information onto the Police. Under these circumstances, the School will disclose the requested data. However, the School Office will ensure the request is legitimate, seeking assistance from the Hampshire County Council and their legal advisers, where necessary.
- **Support agencies** - In order to protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass Personal Data on to social workers or other support agencies.

11. Data Breaches

If a breach is detected, this is to be reported immediately to the Data Protection Officer by completing a 'Data Breach Reporting Form'.

The Data Protection officer will record the information on the 'internal breach register' before conducting a full investigation.

Breaches that are deemed likely to result in an individual suffering damage, will be subject to the mandatory reporting requirements to the ICO (Data Protection Authority) within 72 hours of the breach detection.

12. Subject Access Requests

All individuals whose Personal Data is held by the School are entitled to:

- Ask what information the School holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the School is meeting its Data Protection obligations.

Such a request is called a Subject Access Request (SAR). These must be made in writing (including email) and be addressed to the School Data Protection Officer. (Details are available on the School website and obtainable from the School office.)

The identity of the requestor will be established before the disclosure of any information, and checks carried out regarding proof of relationship to the child.

The GDPR allows exemptions as to the provision of some information; therefore, all information will be reviewed prior to disclosure.

Third party information is that which has been provided by another, such as the police, Local Authority, Health Care professional or another school. Before disclosing third party information, the School might need to obtain further consent.

The following information will not be disclosed as part of an SAR:

- Information which may cause serious harm to the physical or mental health or emotional condition of an individual
- information that would reveal that the individual is at risk of abuse;
- information relating to court proceedings.

13. Complaints

Complaints about how the School captures and processes Personal Data will be dealt with in accordance with the School's Complaints Policy.

If the complaint cannot be resolved, it may be referred to the Information Commissioner who can be contacted at Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF or at https://ico.org.uk/make-a-compliant