Christleton Primary School

Be the best you can be

Data Protection Policy

Document Name		Reviewed by	
Data Protection Policy		Full Governing Body	
Author	Mr Mitchell	**Version number**	1.
Date of Policy	**Policy Reviewed**	**Next Review**	
September 2023		September 2025	
Signed Headteacher		Mr Mitchell	
Signed Chair of Governors		JLEaton	

Christleton Primary School

General Data Protection Regulation

Data Protection Policy

Statement of intent

Christleton Primary School is required to keep and process certain information about its staff members, pupils, their families, volunteers and external contractors in accordance with its legal obligations under data protection legislation.

The school may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, other schools and educational bodies, and potentially children's services.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the school complies with the following core principles of the UK GDPR.

Organisational methods for keeping data secure are imperative, and the school believes that it is good practice to keep clear practical policies, backed up by written procedures.

Applicable data

For the purpose of this policy, 'personal data' refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. an IP address. The UK GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

'Sensitive personal data' is referred to in the UK GDPR as 'special categories of personal data', and is defined as:

- Genetic data.
- Biometric data.
- Data concerning health.
- Data concerning a person's sex life.
- Data concerning a person's sexual orientation.
- Personal data which reveals:
    - Racial or ethnic origin.
    - Political opinions.
    - Religious or philosophical beliefs.
    - Trade union membership.
    - Principles.

'Sensitive personal data' does not include data about criminal allegations, proceedings or convictions. In the case of criminal offence data, schools are only able to process this if it is either:

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

The latter point can only be used if the conditions of the reason for storing and requiring the data fall into one of the conditions below:

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

In accordance with the requirements outlined in the UK GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals.
- 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 UK GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with" the above principles.

Introduction

Christleton Primary School will comply with the demands of the General Data Protection Regulation (GDPR) to be known as the Data Protection Act 2018.

Members of staff will gain familiarisation with the requirements of the GDPR either in a staff briefing or as part of their induction.

This policy follows guidance issued by the Information Commissioner's Office (ICO) and the Department for Education (DfE).

The school is a Data Controller as data is processed that is the personal information of pupils, families, staff, visitors and other school users.

The School is a Data Processor as it processes data on behalf of other public bodies such as the DfE.

Definitions

Data processing

The acquisition, storage, processing and transmission of data

Data subject

Any identifiable person whose data is processed

Consent

Must be freely given, specific and an unambiguous indication of the subject's wishes. It must be recorded and available to an audit. A person must be 13 years old in order to record their consent.

Cross-border processing

The GDPR covers all EU states and will remain part of UK law. Data cannot be stored beyond the EU and UK borders (the exact borders are those of the European Economic Area)

Sensitive data

The GDPR/ICO requires that particular care is taken with the following data

- Data regarding children
- Health (physical, mental, genetic)
- Ethnicity
- Religion
- Sexuality
- Performance management and trade union membership

Filing system

Any structured set of personal data, however stored in any format (physical or digital) that can be processed

Personal data breach

A breach of data security leading to the accidental or unlawful destruction, loss, theft, alteration, unauthorised disclosure, destruction, sale or access to any processed data. Data subjects affected by a data breach must be informed of the breach within 72 hours. Breaches must be reported to the ICO within 72 hours.

Pseudonymisation
The act of making data anonymous. There must be security between pseudonymised data and any data that could re-identify a person.

Password protection
The act of 'locking' a device or document. The information remains readable beyond the password.

Encryption
The act of encoding all the information beyond a password or code.

Legal basis
The school decides, and registers with the ICO, upon which legal basis it processes data. As a public body with set duties the school uses the following bases for processing and controlling data
Legal basis: **Public Task**

- Admissions
- Attendance
- Assessment
- Pupil and staff welfare
- Safe recruitment
- Staff training
- Performance Management

Legal basis: **Consent**

- Various uses of photographs and moving images
- Trade union membership
- Staff ethnicity, religion and health data (Note the Staff Privacy Statement)
- The use of data to promote the social life of the school community

Legal basis: **Contract**

- When processing is required to carry out the performance of a contract

Personal data
Anything that might lead to the identification of a person: name, number, characteristics, photograph, correspondence.

Data portability, data subject access request
Data subjects (or a child's parents) may request access to a copy of all their data. The school has established an efficient means of accomplishing this task which may not carry a charge and will be completed within 15 working days. Data subjects may request that data is brought up-to-date or made more accurate.[1]

Principles

- Personal data must be processed lawfully, fairly and transparently
- Personal data can only be collected for specific, explicit and legitimate purposes
- Personal data must be adequate, relevant and limited to what is necessary for processing
- Personal data must be accurate and kept up-to-date
- Personal data may identify the data subject only as long as is necessary for processing
- Personal data must be processed in a manner that ensures its security
- Any breaches in data security must be reported to the ICO within 72 hours
- The school must report any breaches caused by third parties who have access to school users' data within 72 hours.
- The school must inform any data subject (person identified in data) where a data breach may have led to the unauthorised access to their personal information [2]

Roles and Responsibilities

The school's Privacy Statements set out in detail how the school will maintain the security of school users' data. The Acceptable Use Policies set out the duties of the staff and other school users in supporting data security.

Within school the security of data is coordinated by **Mrs Lisa Bowes (Bursar)**

The governor with special responsibility for data security is **Mrs Emma Binns**

The school has appointed a **Data Protection Officer** who has responsibility for overseeing the implementation of this policy and all GDPR related documents. The DPO will monitor compliance, report to the school leadership and support the school with updates and interpretations as the GDPR develops.

The DPO will liaise between the school and the ICO and must be informed as soon as is practicable of any personal data security breach.

The DPO will support the school in its communication with schools users (pupils, families, parents, governors, contractors and visitors) about the school's GDPR procedures. This will include the drafting of privacy statements, acceptable use policies and data subjects rights.

Data subject requests should be made in writing to the DPO. The DPO might have to respond to any or all of the following

- Why the data a is processed
- On which basis
- Who has seen it
- How long it will be stored for
- Where the data was sourced
- Whether decisions have been based on the data

Children below the age of 13 do not have the right to make a subject access request, so requests must be made by parents. The school may take into account the views of a pupil.

The school's DPO is provided by Edsential

schoolDPO@cheshirewestandchester.go.uk
07990786929

The DPO's duties are set out in greater detail in the service level agreement and contract held between the school and Edsential. Staff should contact the DPO should they believe that this policy and/or the privacy statements and/or the acceptable use policies are not being followed.

Data Audit

The school will carry out a data audit with support from Edsential and their technical support company. Within the audit the school will record all third parties' compliance with the GDPR if those third parties process data for any school users. Such confirmation will, from now on, be an essential part of any contract with third parties when the processing of school users' data is involved. The school will not share data, or have any data processed, by any third parties who do not confirm their compliance with GDPR requirements.
Preferably companies that process school users' data will have certification to ISO27001.
The audit will also check the security of physical and digital records and devices.

Processing Records

To meet the ICO's recommendation that 'scrupulous records' are developed the school will record its processing of data and the results of its data audit. It will record the ongoing security measures for physical and digital filing systems. Confirmation of compliance by third parties accessing any school user data will be recorded.
In broad terms the school will record which data has been processed (including deletions when data should no longer be stored) on which legal basis.
Consent replies are recorded within the system.

Sharing Data

Personal data may be shared with third parties to

- Protect the vital interests of a child
- Protect the vital interests of a member of staff
- To prevent or support the detection of fraud or other legal proceedings
- When required to do so by HMRC

CCTV

CCTV is used to support the safety and security of school users. We adhere to the ICO's code of practice* for its use. Although consent is not required for its use prominent notices inform school users that CCTV is used within the school site.
**In the picture: A data protection code of practice for surveillance cameras and personal information*

Photographs and moving images

Consent is requested from parents and staff for the use of images. Letters requesting consent outline the choices that pupils and staff may make for the use of their images.

The school may seek consent to use photographs for the following purposes:

- To support school user welfare (identity and security)
- To celebrate achievement within the classroom
- To celebrate achievement within the school
- To celebrate achievement in the printed press
- To celebrate achievement online

The school's specific data security measures - data protection by design

A. All IT systems - mobile devices, laptops, tablets, mobile phones and any device capable of processing data, will be password protected.
B. All IT systems will be kept securely; the server and hard disks will be in a locked cabinet and the server room locked when the school is closed and at other times of reduced security; desktop computers and portable devices will be sited/stored in secure places.
C. Staff are expected to ensure the safety of their allocated school devices: devices may not be let unattended in cars at any time and they must be kept out of sight if taken home.
D. All passwords must be 'strong;' (at least 8 characters with a mixture of upper and lower case letters, numbers and symbols), the school will require regular changing of passwords (annually).
E. No passwords will be written down or shared; advice is available on the safe storage of passwords.
F. The school will devise granulated levels of access as appropriate to staff responsibilities for access to personal data.
G. Devices that are used to process sensitive data and/or are vulnerable to theft will be secured with encryption (BitLocker).
H. All emails containing personal data will use school systems and be encrypted and only school email accounts will be used (personal emails will not be permitted for use by staff or governors).
I. All delated data will be deleted in a secure manner: physical data will be shredded and digital data will fully deleted with trash / junk emptied regularly. Hard disks no longer required will have the data on them deleted and the deletion certified by a suitably accredited company.
J. Only data that is necessary for the effective performance of the school will be processed.
K. Data protection will be integrated into all appropriate policies and procedures (e.g. staff induction).
L. Staff will be updated with any significant interpretations or developments of the GDPR.
M. The school will have data impact assessments in place to protect vulnerable data subjects and sensitive data.
N. Data contained within an email, or attached to an email, will be transferred to a secure folder and the email deleted.
O. Physical data will be kept securely, having regard to the sensitivity of the data and the vulnerability of the data subject e.g. medical data will be accessible to those who need to support a school user's needs, but not to others

P. All school users will handle personal data with care: it will not be left unattended (unattended computers must be locked), school users will not allow others to oversee personal data (screens must be positioned with care); papers must not be left where others can see them.
Q. All computers that might be used to process data will be set to lock (a screensaver will activate) after 10 minutes of inactivity.
R. The Headteacher and/or the DPO will approve who and how personal data is stored on mobile devices.
S. All digital data that is stored will be backed up on at least password protected devices
T. Personally owned devices will not be used for the storage of school personal data.

Data breaches

All staff must report to a member of the SLT or the DPO any suspected data breaches (the loss, theft, unauthorised access to data etc.) immediately. It will be for the SLT/DPO to decide whether to the suspected data breach warrants reporting to the ICO. NB a data breach would include the accidental sharing of personal data via a wrongly addressed email.

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

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

Training

All staff will receive basic training in the requirements of the GDPR. The training will be recorded in the data audit and/or the data processing records. Governors will also receive a briefing. Data protection will form a part of pupils' e-safety education. The school will keep staff and governors up to date with guidance, changes and interpretations to data protection law.

Data Protection Impact Assessment

For the school's most sensitive data processing activities the school will have completed a DPIA to ensure that the risk to individuals of a data breach is minimised, as should be the risk to the school's reputation. Staff involved in processing the school's most sensitive data will have to record their reading and understanding of the relevant DPIA.

Monitoring

The DPO will lead the formal monitoring of the school's compliance with the GDPR. Every member of staff and governor shares a responsibility to monitor compliance and to report any suspected failures to comply.

Footnotes

1. Data subjects' rights include
   - The right to be informed
   - The right of access
   - The right to object
   - The right to be forgotten (this might prove impossible in the school context)
   - The right of rectification (any inaccurate data must be corrected)

2. In deciding whether to pass on a suspected data breach to the ICO the DPO will consider whether the data breach might affect a person's
   - Reputation
   - Confidentiality
   - Financial wellbeing
   - A loss of control over their data
   - Make them vulnerable to discrimination
   - Their rights and freedoms

Consent

Consent must be a positive indication expressly confirmed in words. It cannot be inferred from silence, inactivity, a positive action without words or pre-ticked boxes. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes. Consent can be withdrawn by the individual at any time.

Where consent is given, a record will be kept documenting how and when consent was given, and what the data subject was told.

The school ensures that consent mechanisms meet the standards of the UK GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease. Consent accepted under the DPA will be reviewed to ensure it meets the standards of the UK GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

When pupils and staff join the school, the staff member or pupil (or, where appropriate, pupil's parent) will be required to complete a consent form for personal data use. This consent form deals with the taking and use of photographs and videos, amongst other things. Where appropriate, third parties may also be required to compete a consent form.

Where the school opts to provide an online service directly to a child, the child is aged 13 or over, and the consent meets the requirements outlined above, the school obtains consent directly from that child; otherwise, consent is obtained from whoever holds parental responsibility for the child, except where the processing is related to preventative or counselling services offered directly to children. In all other instances with regards to obtaining consent, an appropriate age of consent is considered by the school on a case-by-case basis, taking into account the requirements outlined above.

The right of access
Individuals, including children, have the right to obtain a copy of their personal data as well as other supplementary information, including confirmation that their data is being processed, and the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing. The school will verify the identity of the person making the request before any information is supplied.
A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual requests further copies of the same information.
Requests will be responded to without delay and at the latest, within one month of receipt. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

The right to rectification
Individuals, including children, are entitled to have any inaccurate or incomplete personal data rectified.
Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.
Requests for rectification will be investigated and resolved, where appropriate, free of charge; however, the school may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual makes multiple requests at once. The school reserves the right to refuse to process requests for rectification if they are manifestly unfounded or excessive or if exemptions apply.
The school will take reasonable steps to ensure that data is accurate or is rectified if inaccurate, implementing a proportional response for data that has a significant impact on the individual, e.g. if significant decisions are made using that data. The school will restrict processing of the data in question whilst its accuracy is being verified, where possible.

The right to erasure
Individuals, including children, hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing. Individuals, including children, have the right to erasure in the following circumstances:

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

The school will comply with the request for erasure without undue delay and at the latest within one month of receipt of the request.
The school has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

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

The school has the right to refuse a request for erasure for special category data where processing is necessary for:

- Public health purposes in the public interest, e.g. protecting against serious cross-border threats to health.
- Purposes of preventative or occupational medicine, the working capacity of an employee, medical diagnosis, the provision of health or social care, or the management of health or social care systems or services.