Blackpool Council

Schools Data Protection Policy

(GDPR)

Kincraig Primary School

and

Nursery

Contents

1. Introduction

Kincraig Primary School and Nursery collects, holds and processes personal data about pupils, staff, parents/carers, governors, visitors and other individuals who have contact with the school. It therefore has a number of legal obligations under the General Data Protection Regulation (GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018).

Within this policy (and procedures – appendix 1) we will set out how we seek to protect personal data and ensure that employees understand the rules governing their use of personal data to which they have access to in the course of their employment. This policy applies to all personal data, regardless of whether it is held in paper or electronic format.

The school is a registered data controller with the Information Commissioner and will continue to abide by the new registration arrangements. All members of staff have responsibility for how the school collects, holds and processes personal data. The policy therefore applies to all staff as well as external organisations or individuals processing data on behalf of the school. Staff who do not comply with this policy may face disciplinary action.

This policy also commits that the school will also comply with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, the Protection of Freedoms Act 2012 when referring to use of biometric data and Article 8 of the Human Rights Act 1998.

2. Definitions

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR refers to sensitive personal data as 'special categories of personal data'. Special category data is personal data which the GDPR says is more sensitive, and so needs more protection. For example, information about an individual's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics, health, sex life or sexual orientation, are all 'special categories of personal data'.

The GDPR applies to 'controllers' and 'processors'. The school is a data controller who determines the purposes and means of processing personal data. A processor is responsible for processing personal data on behalf of the school.

3. Data Protection Principles

Under Article 5(1) of the GDPR, the data protection principles set out the main responsibilities for organisations. It states personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) 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;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) 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;

e) 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 GDPR in order to safeguard the rights and freedoms of individuals; and

f) 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."

Article 5(2) requires that:

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

4. Lawful Processing

The first principle requires that organisations process personal data in a lawful manner. The school/nursery will only process personal data if it can meet one of the following lawful bases set out under Article 6(1):

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

In addition, if the school/nursery wishes to process 'special category data', it will identify an additional condition for processing as set out under Article 9(2).

5. Consent

Where a need exists to request and receive consent of an individual prior to the collection, use or disclosure of personal data, the school is committed to seeking such consent. In all cases consent must be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's wishes. The school/nursery are therefore committed to obtaining consent in the following manner:

- consent is presented in a manner clearly distinguishable from other matters
- the request is made in an intelligible and easily accessible form using plain language
- is freely given (i.e. not based on the need to conduct another processing activity)
- the date, method, validity and content of the consent is documented
- a simple method is provided for the data subject to be able to withdraw consent at any time

Once consent is withdrawn by the data subject, the school will cease processing data for the specified purpose without undue delay.

If the school wishes to offer information Society Services (ISS) to pupils it will gain parental consent for any pupil below the age of 13.

6. Accountability and Governance

6.1. Data Protection Officer (DPO)

Under the GDPR it is mandatory for Local Authorities (as defined by the FOIA) to designate a Data Protection Officer (DPO). The DPO's minimum tasks are defined in Article 39:

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments, train staff and conduct internal audits
- To be the first point of contact for the Information Commissioner's Office

The contact details for the School's designated DPO are as follows:

Data Protection Officer, Information Governance Team
Blackpool Council, Number One, Bickerstaffe Square, Blackpool, FY1 3AH
SchoolsDPO@blackpool.gov.uk

Staff can contact the DPO if they have any queries about this policy, data protection law, data retention or the security of personal data. The DPO can also be contacted directly if members of staff have any concerns that this policy is not being adhered to.

6.2. Register of Processing Activities (RoPA)

The school/nursery are required to maintain records of activities related to higher risk processing of personal data. The school and nursery can confirm it maintains a Register of Processing Activities and this is held by the school office in conjunction with the DPO. All members of staff are required to notify the relevant persons before they embark on any new processing activities so they can be adequately recorded on the RoPA.

6.3. Workforce Training

The school/nursery are committed to providing data protection training to all staff as part of their induction process and will issue regular refresh training throughout the course of their employment or in the event of any changes in data protection law. The school will retain a record of this training programme and this will be made available to the Information Commissioner's Office on request.

6.4. Data Protection Impact Assessments (DPIA's)

Data protection impact assessments (DPIAs) are a tool which can help the school identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA allows organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.

The school/nursery will complete a DPIA for certain listed types of processing, or any other processing that is likely to result in a high risk to individuals' interests. Therefore, staff must consult the relevant persons or DPO before they embark on any new processing that could be regarded as being high risk to an individuals' interests. If required, the Information Governance Team will assist members of staff completing the school's DPIA template.

6.5. Contracts

Whenever a controller uses a processor, it needs to have a written contract in place. This is important so that both parties understand their responsibilities and liabilities. The school commits to including the following compulsory details in its contracts:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of data subject; and
- the obligations and rights of the controller.

7. Individual Rights

7.1. Right to be informed

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR. We call this 'privacy information' and the school will issue privacy notices in relation to pupil data, workforce data and governor data. The school will endeavour to issue these notices on induction and also make them available on the school's website throughout the data subject's school life.

7.2. Right of Access

Individuals have the right to access their personal data (commonly known as subject access) and supplementary information about the processing of their data. The right of access allows individuals to be aware of and verify the lawfulness of the processing of their personal data. The information that can be requested 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
- 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

'Subject access' requests can be submitted to the school office and should contain the name of the data subject, a correspondence address and a description of the information requested. The school will provide the information without delay and at the latest within one month of receipt of the request. The school will not apply a fee to requests unless the request is manifestly unfounded or excessive. The school will take reasonable steps to verify the identification of the applicant and if the applicant wishes to request a review of the school's decision, the process for doing so will be clearly outlined in the response issued.

7.3. Individual rights

GDPR also empowers individuals with the right to rectification, erasure, right to restrict processing, data portability, right to object and rights in relation to automated decision making or profiling. The school will carefully consider any requests under these rights and requests can be submitted to the school office.

8. Data Security

Principle f) states data should be processed in a manner that ensures appropriate security of the personal data. This means the school must have appropriate security to prevent the personal data it holds being accidentally or deliberately compromised. Particular attention will be paid to the need for security of sensitive personal data.

Manual data will be stored where it is not accessible to anyone who does not have a legitimate reason to view or process that data. Staff should carefully consider whether they need to take any manual data offsite before doing so and record instances where any 'special categories of data' is taken offsite. The following measures must be taken by staff in relation to electronic data:

- portable electronic devices, such as laptops, ipads and hard drives that contain personal data are stored in a locked cupboard or draw
- encryption software is used to protect all portable devices and removable media that contain personal data, such as laptops and USB devices
- passwords must meet appropriate security standards, be changed at regular intervals and must not be divulged to any other persons

- where personal data is shared with a third party, staff should carry out due diligence and ensure the data is sent in a secure manner or appropriate measures are taken to mitigate the risk of individuals being identified
- when sending personal data to a third party, staff must carefully check the recipient and their contact details
- where personal devices are used to access organisational email accounts, staff should ensure appropriate passwords are applied to the device
- staff should not open links when emails are received from unknown recipients or the emails appear suspicious
- personal data must be stored in a secure and safe manner, with careful consideration made to who can access the data

9. Breach Reporting

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. Where feasible, the school must do this within 72 hours of becoming aware of the breach, it is therefore essential that **all members of staff make the relevant persons aware of any potential breaches of data protection without undue delay.** This includes all losses, thefts or inadvertent disclosures of personal data. It also includes the loss or theft of any device that holds personal data.

The relevant persons will then follow the breach procedure in conjunction with the DPO. An investigation will be conducted to confirm whether or not a personal data breach has occurred. If a breach has occurred the DPO will advise the school on whether it is required to notify the Information Commissioner and the data subjects affected.

10. Data Retention

Principle e) states data must be 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. Data will only be retained for the specified period outlined in the records management schedule that the school has adopted and will be destroyed in a secure manner thereafter. A copy of the records management schedule is available on request from the school office.

11. Data Accuracy and Limitation

Principle (d) states data shall be accurate and, where necessary, kept up to date The school will issue regular reminders to staff and parents/carers to ensure that personal data held is up to date and accurate. Any inaccuracies discovered will be rectified and if the inaccurate information has been disclosed to a third party; the recipients will be informed of the corrected data.

The school will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals in the school's privacy notices. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary. Staff must only process personal data where it is necessary to do so in their jobs.

12. Information Requests

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. The school will adhere with 'subject access' requests as outlined in Section 7.2 of this policy.

Personal data will only be disclosed to third party organisations or individuals for whom consent has been given to receive the data, or organisations that have a legal right to receive the data without consent being given e.g. examination boards.

Requests for personal data by the Police or other bodies with law enforcement powers (e.g. HMRC), will usually only be considered when accompanied by an appropriate data protection. This form typically contains details of the applicant, the purpose of the request and the section of the legislation the information is being requested under. This will allow the DPO to make an informed decision as to whether the request is proportionate for the purpose requested, against the rights of the data subject

If requests are received from parents/carers for the names of pupils in their class (e.g. for Christmas card or birthday invites), only first names will usually be released, however the school reserves the right to refuse any request in its entirety.

13. CCTV and Biometric Data

The school uses CCTV in various locations around the school site; as such it adheres to the ICO's code of practice for the use of CCTV. We do not need to ask individuals' permission, but cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use. Any enquiries about the CCTV system or requests for footage should be directed to the school office.

Where we use pupils' biometric data as part of an automated biometric recognition system, we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it. Parents/carers and pupils have the right to choose not to use the school's biometric system(s) and we will provide alternative means of accessing the relevant services for those pupils. Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will ensure that any relevant data already captured is deleted.

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service should they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

Policy last updated 18/09/18

Schools Data Protection Policy at Kincraig Primary School and Children's Centre will be reviewed and modified bi-annually, or before if there are any changes in legislation.

It is possible to add amendments to this document prior to a review and these will be incorporated into the next issue. To add comments please complete the information on this sheet adding the date and signing where indicated.

Name of person responsible for policy – Mrs Karen Appleby

Policy adopted by the Governing Body – ***September 2018***

Signed: _____ Date: _____

Date	Proposed Amendment	Signed

APPENDIX 1

KINCRAIG PRIMARY SCHOOL AND NURSERY GDPR – PROCEDURES

MANAGEMENT:

- All staff complete a consent to share/ Privacy Notice
- All staff who use school iPads and lap tops sign/agree the acceptable usage policy
- All staff informed that USB drives are blocked on all school devices. Additional passwords put in place for older devices where there is no TMP chip/bitlocker
- All staff advised to have the Outlook app installed on their mobile phones to enable additional passcode protection
- Door codes changed when there is knowledge that the code has been breached
- Blackpool council email addresses are deleted by Comptechit/DPO when staff/governors leave

STAFF:

Emails:

- System in place to delete staff emails after 2 years
- Staff advised to use BCC to send emails to multiple recipients when no consent to share has been given
- Staff advised to use the terms, secure/confidential /ENCRYPT in the subject title to impose an additional layer of security on the recipient

Device security:

- Staff advised to use **windows and L** on their keyboard when they leave their screen, particularly when working on personal/sensitive information
- Inactivity lock screen policy in place: -
  *5 minutes for administrators
  *30 minutes for classroom devices when teaching
- Password protection to be a minimum of 6 digits
- Password to be changed every 90 days
- Password to be a minimum of 8 characters (upper and lower case characters and a minimum of 1 number)
- No passwords to be used that relate to school
- No passwords to be left on desks/on view
- Scan addresses specific to user
- System in place where scans are automatically deleted after 2 weeks

GOVERNORS:

- Governors advised to use their Blackpool Council email address for school related communication/documentation and to delete all emails relating to school from their personal email addresses.