Children First Learning Partnership

Inspiring Excellence Together

Data Protection Policy

Policy reviewed and agreed

Signed……Board of Directors

Date……16/07/19

Next review date….July 2020

Contents

1. Aims

Our school aims 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) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. The data controller

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

Our school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

4. Roles and responsibilities

This policy applies to all staff employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

4.1 Governing board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

4.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

DPO responsibilities may be delegated. They are as follows:

- Keeping the board updated about data protection responsibilities, risks and issues
- Ensuring all data protection procedures and policies are reviewed on a regular basis
- Arranging data protection training and advice for all staff members and those included in this policy
- Providing support and advice on data protection from staff, board members and other stakeholders
- Responding to individuals such as regulated individuals, employees and members of the public who wish to know which data is being held on them by the organisation
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing

Our DPO is Tracy Thorley and is contactable via dpo.schools@staffordshire.gov.uk.

4.3 Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis.

4.4 All staff

All employees (including those temporary and permanent, under contract, work experience and agency staff) and anyone processing data on the Trusts / schools behalf have the responsibility to comply with this policy and related guidance documents.
Deliberate unauthorised use and access to copying, destruction or alteration of or interference with any personal information is strictly forbidden.

5. Data protection principles

The GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles.

6. Collecting personal data

6.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)

- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

  For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

- Obtained for a specific, explicit and legitimate purpose

  We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

- Adequate, relevant and limited to what is necessary
  Staff must only process personal data where it is necessary in order to do their jobs.

- Accurate and up to date

- Not kept longer than is necessary

  When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's record retention schedule.

- Handled ensuring appropriate security

7. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
  - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
  - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
  - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

8. Subject rights

8.1 The right to be informed

Data subjects have the right to obtain confirmation if data is being processed and then have a copy of their personal data, together with an explanation of the categories of data being processed, the purposes of such processing, who the data will be shared with as well as details of the period for which the data will be retained.

8.2 The right of access (Subject access requests)

The Trust / School has one calendar month in which to respond to a Subject Access Request (SAR), provided all information required to carry out the request has been received from the applicant and suitable proof of identification has been supplied. The Office Manager co-ordinates the processing of SAR requests.

8.3 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it individuals also have the right to:

- The right to rectification
- The right to erasure
- The right to restrict
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling
- Withdraw their consent to processing at any time
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

9. CCTV – see also the school CCTV code of conduct.

We use CCTV in various locations around the school site to:

- assist in providing a safe and secure environment for the benefit of those pupils attending and visiting the school, for those who work and volunteer in the school, and for those who visit the school, such as members of an outside agency or contractors
- deter and detect anti-social behaviour and crime
- provide the Police, Health and Safety Executive and the School with evidence upon which to take criminal, civil and disciplinary action respectively
- protect employees from undue threats and violence
- obtain evidence for use in the investigation of criminal actions, breaches of health and safety legislation and breaches of pupil and staff disciplinary procedures

Note: The School will only investigate images for use in a staff disciplinary case when there is a suspicion of gross misconduct and not to generally monitor staff activity. In these situations the Headteacher / Executive Headteacher will approve their use. Where access is given, the confidentiality of these images and who is able to access them will be closely controlled.

Note: A member of the school leadership team will approve the use of images for matters of pupil discipline. Where access is given, the confidentiality of these images and who is able to access them will be closely controlled.

We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the Headteacher / Executive Headteacher.

10. Privacy by design and Data Impact Assessments

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing Data Protection impact assessments (DPIA) where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

11. 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.

12. 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 or incinerate paper-based records, and overwrite or 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.

13. Personal data breaches

All members of staff have an obligation to report actual or potential data protection incidents. This allows us to:

- Investigate and take remedial steps where necessary.
- Maintain a register of incidents as part of the responsibility to monitor all incidents to ensure lessons learnt can be made and future prevention be enabled.
- Comply with the mandatory requirement of notifying the Information Commissioners Office (ICO) with 72 hours of any breaches which hit the threshold as outlined by data protection legislation.

14. Training

All staff and Local Advisory Boards are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

15. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if any changes are made to our school's practice. This policy will be reviewed **every year** and shared with the local advisory board.

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 / Executive Headteacher and the chair of the Local Advisory Board.
- 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.
- 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 by the DPO.
- The DPO and Headteacher / Exec 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 (including safeguarding records)

- *If special category data (sensitive information) is accidentally made available to unauthorised individuals, the sender must attempt to recall the data 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 data for any reason, the DPO will ask appropriate members of staff to recall it, including ICT support staff if the data is in electronic form*
- *In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the data, explain that the information was sent in error, and request that those individuals return the information, or in the case of electronic data they delete it, and that they 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*
- *In the case of electronic data, 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*

Details of pupil premium interventions for named children being published on the school website

- *Pupils are not to be identifiable in named interventions, such as by name or photograph*
- *Postings to the school web site are to be reviewed and authorised by a member of the Senior Leadership Team to ensure compliance*
- *DPO to be alerted of breach*

Non-anonymised pupil exam results or staff pay information being shared with the Local Advisory Board

- *Only anonymised information to be given to the Local Advisory Board*
- *Headteacher / Executive Headteacher to review all data given to the Local Advisory Board*
- *DPO to be alerted of breach*

A school laptop containing non-encrypted sensitive personal data being stolen or hacked

- *Member of staff who identifies the theft or hacking to alert a member of the Senior Leadership Team and DPO immediately*
- *If theft, report the incident to the Police*
- *If hacking, report the incident immediately to ICT support staff, who will amongst other things, reset your password and block all access to network resources. If there was a potential compromise of sensitive information or exposure of network resources, the DPO may confer with appropriate school members to coordinate notification to affected individuals and report the incident to the necessary agencies (see 'sensitive information being disclosed' actions)*

Appendix 2

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.