DRAFT Data Protection – Employee HR Data Policy

Formally adopted by the Governing Board/ Trust of:-	**Brooke Primary School**
On:-	**5th June**
Chair of Governors:-	**Rebecca Cole**
Signed:-	

This model has been subject to consultation with the recognised trade unions at County level.

Introduction

The General Data Protection Regulations enforced from 25 May 2018 strengthen data protection requirements across the EU. This policy focuses specifically on data protection from an HR employee data point of view.

1. Purpose

This school is committed to being transparent about how it collects and uses the personal data of its workforce, and to meeting its data protection obligations. This policy sets out the school's commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of job applicants, employees and former employees, referred to as HR-related personal data. [This policy does not apply to the personal data of clients or other personal data processed for business purposes.]

The school's data protection officer is part of an annually purchased service. Their role is to inform and advise the school on its data protection obligations. They can be contacted by obtaining their details from the school office Questions about this policy, or requests for further information, should be directed to the data protection officer.

2. Definitions

"Personal data" is any information that relates to a living individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

3. Data protection principles

The school processes HR-related personal data in accordance with the following data protection principles:

- The school processes personal data lawfully, fairly and in a transparent manner.
- The school collects personal data only for specified, explicit and legitimate purposes.
- The school processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- The school keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- The school keeps personal data only for the period necessary for processing.

- The school adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

The school tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons. Where the school relies on its legitimate interests as the basis for processing data, it will carry out an assessment to ensure that those interests are not overridden by the rights and freedoms of individuals.

Where the school processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with data protection legal requirements.

The school will update HR-related personal data promptly if an individual advises that their information has changed or is inaccurate.

Personal data gathered during the employment relationship, is held in the individual's personnel file (in hard copy or electronic format, or both), on HR systems and with Educator Solutions HR Services. The periods for which the school holds HR-related personal data are contained in its privacy notices to individuals.

The school keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

4. Individual rights

As a data subject, individuals have a number of rights in relation to their personal data.

4.1. Subject access requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, the school will tell them:

- whether or not their data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom their data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long their personal data is stored (or how that period is decided);
- their rights to rectification or erasure of data, or to restrict or object to processing;
- their right to complain to the Information Commissioner if they think the school has failed to comply with their data protection rights; and
- whether or not the school carries out automated decision-making and the logic involved in any such decision-making.

The school will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless they agrees otherwise.

If the individual wants additional copies, the school will charge a fee, which will be based on the administrative cost to the school of providing the additional copies.

To make a subject access request, the individual should send the request to head@brooke.norfolk.sch.uk In some cases, the school may need to ask for proof of identification before the request can be processed. The school will inform the individual if it needs to verify their identity and the documents it requires.

The school will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the school processes large amounts of the individual's data, it may respond within three months of the date the request is received. The school will write to the individual within one month of receiving the original request to tell them if this is the case.

If a subject access request is manifestly unfounded or excessive, the school is not obliged to comply with it. Alternatively, the school can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the school has already responded. If an individual submits a request that is unfounded or excessive, the school will notify them that this is the case and whether or not it will respond to it.

4.2. Other rights

Individuals have a number of other rights in relation to their personal data. They can require the school to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the school's legitimate grounds for processing data (where the school relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the school's legitimate grounds for processing data.

To ask the school to take any of these steps, the individual should send the request to head@brooke.norfolk.sch.uk

5. Data security

The school takes the security of HR-related personal data seriously. The school has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Where the school engages third parties to process employee personal data on its behalf (e.g. third party HR provider, Occupational Health), such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data. Further information regarding what is processed can be viewed in the school's privacy notice.

6. Impact assessments

Some of the processing that the school carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, the school will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

7. Data breaches

If the school discovers that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery (NB. The 72 hours includes weekends and holidays). The school will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

If an employee uncovers a data breach they must report it to the Headteacher immediately.

8. International data transfers

The school will not transfer HR-related personal data to countries outside the EEA.

9. Individual responsibilities

Individuals are responsible for helping the school keep their personal data up to date. Individuals should let the school know if data provided to the school changes, for example if an individual moves house or changes their bank details.

Individuals may have access to the personal data of other individuals in the course of their employment. Where this is the case, the school relies on individuals to help meet its data protection obligations to staff, pupils, parents and suppliers.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the school) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from the school's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
- not to store personal data on local drives or on personal devices that are used for work purposes; and
- to report data breaches of which they become aware to the Headteacher immediately.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the school's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

10. Training

The school will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

Appendix 1 – Table of changes

Date of change	Paragraphs affected	Summary of update
12/04/2018	All	New model policy uploaded to HR InfoSpace