

DATA PROTECTION POLICY

Lakenheath Community Primary School



Version Number	6
Date of Policy	May 2023
Review Date	May 2024
Head Teacher's Signature	 22/5/23
Chair of Governors' Signature	 22/5/23

Document Change History

Version	Date	Change Details
1	May 2018	New Policy
2	May 2019	Policy review, amendment to Data officer contact details.
3	May 2020	Policy review, no changes.
4	May 2021	Policy review, no changes.
5	May 2022	Policy review, no changes.
6	May 2023	Policy review, Data Breach Form and Privacy Notices added as appendices. Process for handling Archive documents added to point 6.

1. Related Policies

The School also adopts the following policies that relate to the Data Protection Policy:

- CCTV Policy
- Computer/IT Policy
- Home Working Policy
- Clear Desk Policy
- Data Retention Schedule
- ICT policy for staff/ Acceptable use of ICT

2. Introduction

The school is committed to being transparent about how it collects and uses the personal data of its staff, children, parents and carers, 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. The school has appointed Schools Choice as its data protection officer. Their role is to inform and advise the school on its data protection obligations. They can be contacted at data.protection@schoolschoice.org and questions about this policy, or requests for further information, should be directed to them.

3. Definitions

Personal data – any information that relates to an individual who can be identified from that information.

Processing – 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.

4. Data Protection Principles

The school processes 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 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 the General Data Protection Regulation (GDPR).

The school will update personal data promptly if an individual advises that their information has changed or is inaccurate and data gathered is held in:

- the individual's personnel file (in hard copy or electronic format, or both)
- on HR systems
- in child files
- on CPOMS [Child Protection Online Management System – for all safeguarding information]
- on SIMS [School Information Management System]

The periods for which the school holds personal data are contained in its privacy notices/retention schedule and the school keeps a record of its processing activities in respect of personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

5. Privacy Notices

The school has a duty to check that staff, children, parents and carers information is accurate and up to date. It fulfils this by sending out a data collection form to parents/carers/staff on an annual basis.

This form will also include a privacy notice, which outlines:

- who we are (including our contact details);
- the contact details of our Data Protection Officer;
- the purpose of the school processing data;
- the legal basis for processing data; and
- who this data will be shared with.

The current privacy notices for each relevant category of data subjects can be found **as appendix 2**, on the school's website and in the office.

6. Data Retention

The school maintains a retention schedule, which can be found in the School Business Manager's office.

This retention schedule is based on guidance from the information and records management society:

<http://www.irms.org.uk/resources/information-guides/199-rm-toolkit-for-school> and it encompasses records managed by all types of school – some of the file descriptions listed may not be relevant to every school.

The school adopts and references the 'Protection of school archives under GDPR: Principles and Practice for Archivists and Bursars'. (The School Archives & Records Association, 2021)

<https://schoolarchivesandrecordsassociation.org/>.

For the correct procedure in the handling of the schools archive material.

7. Individual Rights

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

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 (i.e. e-recruitment software.)

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 agree otherwise.

To make a subject access request, the individual should complete the relevant form/send the request to head@lakenheath.suffolk.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.

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 legitimate grounds for processing data.

To ask the school to take any of these steps, the individual should send the request to admin@lakenheath.suffolk.sch.uk

8. Disclosure of Personal Information

Information Sharing with Professionals Working with Children

Information sharing between professionals is vital to ensure the wellbeing of Children.

The school will follow the “7 golden rules of Information Sharing” described by the DfE:

1. Remember that the DPA/GDPR is not a barrier to sharing information
2. Be open and honest with the person or family
3. Seek advice if you are in any doubt
4. Share with consent where appropriate
5. Consider safety and well-being
6. Necessary, proportionate, relevant, accurate timely, and secure
7. Keep a record of your decision and reasons

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/419628/Information_sharing_advice_safeguarding_practitioners.pdf

Access to Pupils Records

Parents have two distinct rights to access information about their child held by a school.

These rights are:

1. The parent's right of access to their child's educational record under The Education (Pupil Information) Regulations 2005. A link to this document can be found here. <http://www.legislation.gov.uk/ukxi/2005/1437/contents/made>
2. The pupil's right of subject access

A child or young person will always be the owner of their personal information however if a young person is incapable of making their own decisions which is generally accepted as under the age of 12, the primary carer or guardian would act on their behalf. This authority is only extended to functions that are in the 'best interests' of the child or young person.

The school will respond to a subject access request within 1 calendar month. If this request comes from someone other than the individual, the school will consider the capability of the individual and also must ensure the requester is acting in the best interests of the individual.

Requests for information from pupils, or parents, for information that contains, wholly or partly, an educational record must receive a response within 15 school days.

Under the Regulations, requests from parents to view their child's educational record will be dealt with by the Board of Governors. All other requests for personal information from the pupil, or someone acting on their behalf, will be dealt with by the Head Teacher on behalf of the school.

9. International Data Transfers

Personal data may be transferred to countries outside the EEA when their families move abroad due to relocation [e.g: USAF – familial postings] to reduce the risk of children missing education and to pass on relevant safeguarding information.

10. Biometric Data

Biometric technologies are those, which automatically measure people's physiological or behavioural characteristics. Examples include automatic fingerprint identification, iris and retina scanning, face recognition and hand geometry, and their use is becoming increasingly popular in educational settings.

Before the first processing of a child's biometric information, the school will notify each parent of the child:

- Of its intention to process the child's biometric information.
- That the parent may object at any time to the processing of the information.

11. Freedom of Information/Environmental Information Regulations

The school as a public authority is subject to The Freedom of Information Act 2000 (FOI) and Environmental Information Regulations 2004 (EIR) and all requests for information that is not personal information must be treated as a FOI or EIR. These requests must be fully responded within 20 (school) working days by law. The information will be provided unless the school can provide an exemption or exception under the FOI act or EIR respectively.

In line with FOI the school is required to have a publication scheme showing what information is held and how you can access this. The school's publication scheme can be found on the website and in the office.

12. Data Security

The school takes the security of 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.

- All paper copies are kept in locked filing cabinets or cupboards.
- Computers are password protected,
- Files are encrypted.
- Personal devices are discouraged but where staff access emails or other cloud based information these are password protected.
- School is protected by CCTV.
- Information transfers are encrypted.
- School is only accessible through a limited number of key holders and through an electronic entry system.
- Follow a clear schedule whereby information is only held for the necessary time period and is then safely destroyed.

Where the school engages third parties to process personal data on its behalf, 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.

An Information Risk Register will be created and maintained by the school which summarises each information asset the school maintains. Appropriate measures will be taken to mitigate the risk of disclosure of each information asset based on the impact level assigned. The information risk register can be found in the school manager's office and on the O:\drive.

13. Privacy 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 privacy 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.

14. Data Breaches

If the school discovers that there has been a breach of 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. The school will record all data breaches regardless of their effect. *Data Breach form appendix 1.*

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.

15. 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.

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.

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.

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 data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

16. 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.

17. Roles and Responsibilities

The senior information risk owner (SIRO) for the school is the Headteacher.

They are responsible for:

- *Owning and updating this policy*
- *Owning the risk register*
- *Advocating information risk management and raising awareness of information security issues*

All staff are responsible for ensuring that information is managed according to this policy.

Appendix 1

Data Breach Incident Form



Under the General Data Protection Regulation 2016 and the Data Protection Bill 2017, organisations which process personal data must take appropriate measures against unauthorised or unlawful processing and against loss, destruction of or damage to personal data. A data security breach can happen for a number of reasons:

- Loss or theft of data or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it

As soon as you are aware of a data breach you must notify Lyndsey Nobbs or Michael Tingey within 24 hours by completing this form.

Once you have notified Lyndsey Nobbs or Michael Tingey the form should be returned to Schools Choice at data.protection@schoolschoice.org

Information Management Leads

Lead	Contact Information
Lyndsey Nobbs Or Michael Tingey	01842 860256 or finance@lakenheath.suffolk.sch.uk 01842 860256 or head@lakenheath.suffolk.sch.uk
Schools Choice	01473 260700 or data.protection@schoolschoice.org

1.	Name of the person who identified the breach	
2.	Job title and contact details	
3.	School Name	
4.	Date incident occurred	
5.	Is this a breach of data by a supplier or partner organisation? (If the breach has been notified to you by a supplier or a partner organisation who you share your data with, name of the supplier/partner, date notified, contact should be completed)	The breach originated in school: Yes/No We have been notified of the breach by a supplier / Partner Organisation. Name: Name Contact: Date Notified:
5.	Who has been notified of the breach to date? (e.g. Headteacher, DPO, ICO, Parents, Teachers, Governors etc.)	
6.	Type of data involved and how sensitive is it? (Some data is sensitive because of its very personal nature e.g. social services and health records. Other data types are sensitive because of what might happen if it is misused e.g. bank account details.)	
7.	If the data has been lost or stolen, were there any protections in place such as encryption?	
8.	What Type of Data Breach is it? A Confidentiality Breach has occurred if the data was unauthorised or accidentally disclosed. An Availability Breach has occurred if the data was unauthorised or accidentally lost. An Integrity Breach has occurred if the data was unauthorised or accidentally altered.	Delete as applicable: Confidentiality Breach: Yes/No Accidental/Unauthorised Availability Breach: Yes/No Accidental/Unauthorised Integrity Breach: Yes/No Accidental/Unauthorised
9.	What could the data tell a third party (individual or organisation) about the school/pupil/teacher? For example, sensitive data could disclose an individual's medical condition, details of their finances.	
10.	How many individuals' personal data are affected by the breach?	Approx. Number individuals impacted: Who are they (staff, children etc.):

		Approx. Number of data records impacted:
12.	What harm could be caused by the breach, consider whether there is: Any risks to physical safety as a result of the breach? Any risks of the data being used to discriminate against an individual? Any risks to the reputation of any individual being impacted by the breach? Any risks of financial loss through identity theft?	The ICO will need to be notified within 72 hours of all data breaches where a risk to individual's rights and freedom exists. If you have answered yes to any of the questions on the left-hand side, it is likely that you will need to notify the breach to the ICO.
13.	Are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service you provide?	

Signature: _____

Print Name: _____

Job Title: _____

Date: _____

To be completed by the DPO

Date received and logged:

Date ICO notified:

Actions taken to recover in full or partially the data:

Does this represent a 'High Risk' to the rights and freedoms of those impacted individuals? If yes details of the communication plan:

Future mitigating actions identified:

Date added to the General Data Protection Compliance Action Plan:

Signature: _____

Print Name: _____

Job Title: _____

Date: _____

Appendix 2

Lakenheath Community Primary School

EMPLOYEE PRIVACY NOTICE



Privacy Notice - General Data Protection Regulation (GDPR) 2018

We (Lakenheath Community primary School) collect and process personal data relating to its employees to manage the employment relationship. We are committed to being transparent about how we collect and use that data and to meet our data protection obligations.

Who We Are

Under Data Protection legislation, we are a data controller.

The contact details for the school are as follows:

Lakenheath Community Primary School

Mill Road

Lakenheath

Suffolk

IP27 9DU

Tel: 01842 860256

Our Data Protection Officer

The school's data protection officer is:

Schools' Choice Data Protection Team

Beacon House

Whitehouse Road

Ipswich

Suffolk

IP1 5PB

Tel: 01473 260700

Categories of Information

The school collects and processes a range of information about its employees. This includes:

- your name, address and contact details, including email address and telephone number, date of birth and gender;
- the terms and conditions of your employment;
- details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the organisation;
- information about your remuneration, including entitlement to benefits such as pensions;
- details of your bank account and national insurance number;
- information about your marital status, next of kin and emergency contacts;
- information about your nationality and entitlement to work in the UK;
- information about your criminal record;
- details of your schedule (days of work and working hours) and attendance at work;

- details of periods of leave taken by you, including holiday, sickness absence and family leave, and the reasons for the leave;
- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence;
- assessments of your performance, including appraisals, performance reviews and ratings, performance improvement plans and related correspondence;
- information about medical or health conditions, including whether or not you have a disability for which the organisation needs to make reasonable adjustments; and
- equal opportunities monitoring information including information about your ethnic origin, sexual orientation and religion or belief.

The school may collect this information in a variety of ways. For example, data might be collected through application forms or CVs; obtained from your passport or other identity documents such as your driving licence; from forms completed by you at the start of or during employment (such as benefit nomination forms); from correspondence with you; or through interviews, meetings or other assessments.

In some cases, the school may collect personal data about you from third parties, such as references supplied by former employers, information from employment background check providers and information from criminal records checks permitted by law.

Data will be stored in a range of different places, including in your personnel file, in the school's HR management systems and in other IT systems (including the school's email system).

Why We Collect and Use This Information

The school needs to process data to enter into an employment contract with you and to meet its obligations under your employment contract. For example, it needs to process your data to provide you with an employment contract, to pay you in accordance with your employment contract and to administer benefit, pension and insurance entitlements.

In some cases, the school needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check an employee's entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled.

In other cases, the school has a legitimate interest in processing personal data before, during and after the end of the employment relationship. Processing employee data allows the organisation to:

- run recruitment and promotion processes;
- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights;
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace;
- operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes;
- operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled;
- obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled;
- operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the organisation complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled;
- ensure effective general HR and business administration;

- provide references on request for current or former employees; and
- respond to and defend against legal claims.

Some special categories of personal data, such as information about health or medical conditions, is processed to carry out employment law obligations (such as those in relation to employees with disabilities).

Where the school processes other special categories of personal data, such as information about ethnic origin, sexual orientation or religion or belief, this is done for the purposes of equal opportunities monitoring. This is to carry out its obligations and exercise specific rights in relation to employment. Employees are entirely free to decide whether or not to provide such data and there are no consequences of failing to do so.

Who has access to data?

Your information may be shared internally, including with members of the HR and recruitment team (including payroll), your line manager, senior managers and IT staff if access to the data is necessary for performance of their roles.

The school shares your data with third parties in order to obtain pre-employment references from other employers, obtain employment background checks from third-party providers and obtain necessary criminal records checks from the Disclosure and Barring Service. In those circumstances the data will be subject to confidentiality arrangements.

The school also shares your data with third parties that process data on its behalf, in connection with payroll, HR, the provision of benefits and the provision of occupational health services.

- our local authority - we are required to share information about our employees with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.
- the Department for Education (DfE) - we share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding/expenditure and the assessment educational attainment.

The school will not transfer your data to countries outside the European Economic Area.

How Does the School Protect Data?

The school takes the security of your data seriously. The school has internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties. Staff details are kept in Staff folders, which are stored in a locked filing cabinet. They are also stored within our electronic systems which are accessed with secure passwords.

Where the school engages third parties to process personal data on its behalf, they 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.

For How Long Does the School Keep Data?

The school will hold your personal data for the duration of your employment.

The periods for which your data is held after the end of employment are for 6 years after contract ends, for purposes of references and safeguarding.

Data Collection Requirements

The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools

including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.

The department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit:

<https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

To contact the department: <https://www.gov.uk/contact-dfe>

Requesting Access to Your Personal Data

As a data subject, you have a number of rights. You can:

- access and obtain a copy of your data on request;
- require the school to change incorrect or incomplete data;
- require the school to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing; and
- object to the processing of your data where the school is relying on its legitimate interests as the legal ground for processing.

If you would like to exercise any of these rights, please contact Schools' Choice Data Protection Team Tel: 01473 260700 Email: data.protection@schoolschoice.org

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at <https://ico.org.uk/concerns/>

What If You Do Not Provide Personal Data?

You have some obligations under your employment contract to provide the school with data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. You may also have to provide the school with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights.

Certain information, such as contact details, your right to work in the UK and payment details, have to be provided to enable the school to enter a contract of employment with you. If you do not provide other information, this will hinder the school's ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

Automated decision-making

Employment decisions are not based solely on automated decision-making.

Further information

If you would like to discuss anything in this privacy notice, please contact:

Schools' Choice Data Protection Team Tel: 01473 260700 Email: data.protection@schoolschoice.org

Lakenheath Community Primary School

JOB APPLICANT PRIVACY NOTICE

Privacy Notice - General Data Protection Regulation (GDPR) 2018



As part of any recruitment process, we (Lakenheath Community primary School) collect and process personal data relating to job applicants. We are committed to being transparent about how we collect and use that data and to meet our data protection obligations.

Who We Are

Under Data Protection legislation, we are a data controller.

The contact details for the school are as follows:

Lakenheath Community Primary School

Mill Road

Lakenheath

Suffolk

IP27 9DU

Tel: 01842 860256

Our Data Protection Officer

The school's data protection officer is:

Schools' Choice Data Protection Team

Beacon House

Whitehouse Road

Ipswich

Suffolk

IP1 5PB

Tel: 01473 260700

What Information Does the School Collect?

The school collects a range of information about you. This includes:

- your name, address and contact details, including email address and telephone number;
- details of your qualifications, skills, experience and employment history;
- information about your current level of remuneration, including benefit entitlements;
- medical details, N.I. number;
- your ethnicity, nationality, religion, gender, sexual orientation, whether or not you have a disability for which the school needs to make reasonable adjustments during the recruitment process; and
- information about your entitlement to work in the UK.

The school may collect this information in a variety of ways. For example, data might be contained in application forms or CVs, obtained from your passport or other identity documents, or collected through interviews or other forms of assessment, including online tests.

The school may also collect personal data about you from third parties, such as references supplied by former employers, information from employment background check providers and information from criminal records checks.

Data will be stored in a range of different places, including on your application record, in HR management systems and on other IT systems (including email).

Why Does the School Process Personal Data?

The school needs to process data to take steps at your request prior to entering into a contract with you. It may also need to process your data to enter into a contract with you.

In some cases, the school needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check a successful applicant's eligibility to work in the UK before employment starts.

The school has a legitimate interest in processing personal data during the recruitment process and for keeping records of the process. Processing data from job applicants allows the school to manage the recruitment process, assess and confirm a candidate's suitability for employment and decide to whom to offer a job. The school may also need to process data from job applicants to respond to and defend against legal claims.

The school may process special categories of data, such as information about ethnic origin, sexual orientation or religion or belief, to monitor recruitment statistics. It may also collect information about whether or not applicants are disabled to make reasonable adjustments for candidates who have a disability. The school processes such information to carry out its obligations and exercise specific rights in relation to employment.

For some roles, the school is obliged to seek information about criminal convictions and offences. Where the school seeks this information, it does so because it is necessary for it to carry out its obligations and exercise specific rights in relation to employment. If your application is unsuccessful, the school may keep your personal data on file in case there are future employment opportunities for which you may be suited. The school will ask for your consent before it keeps your data for this purpose and you are free to withdraw your consent at any time.

Who Has Access to Data?

Your information may be shared internally for the purposes of the recruitment exercise. This includes members of the HR and recruitment team, interviewers involved in the recruitment process, managers in the area with a vacancy and IT staff if access to the data is necessary for the performance of their roles.

In keeping in line with keeping children safe in education guidance, the school will obtain references from your former employers prior to interview. If your application for employment is successful and it makes you an offer of employment, the school will then share your data with employment background check providers to obtain necessary background checks and the Disclosure and Barring Service to obtain necessary criminal records checks.

The school will not transfer your data to countries outside the European Economic Area.

How Does the School Protect Data?

The school takes the security of your data seriously. It has internal policies and controls in place to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by our employees in the proper performance of their duties. Unsuccessful job applicant's data is held in a temporary staff folder in our locked Archive room.

For How Long Does the School Keep Data?

If your application for employment is unsuccessful, the school will hold your data on file for 1 year after the interview date. At the end of that period or once you withdraw your consent, your data is deleted or destroyed.

If your application for employment is successful, personal data gathered during the recruitment process will be transferred to your personnel file and retained during your employment. The periods for which your data will be held will be provided to you in a new privacy notice.

Your Rights

As a data subject, you have a number of rights. You can:

- access and obtain a copy of your data on request;
- require the school to change incorrect or incomplete data;
- require the school to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing; and
- object to the processing of your data where the school is relying on its legitimate interests as the legal ground for processing.

If you would like to exercise any of these rights, please contact Schools' Choice Data Protection Team Tel: 01473 260700 Email: data.protection@schoolschoice.org

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at <https://ico.org.uk/concerns/>

What If You Do Not Provide Personal Data?

You are under no statutory or contractual obligation to provide data to the school during the recruitment process. However, if you do not provide the information, the school may not be able to process your application properly or at all.

Automated decision-making

Recruitment decisions are not based solely on automated decision-making.

Further information

If you would like to discuss anything in this privacy notice, please contact:

Schools' Choice Data Protection Team Tel: 01473 260700 Email: data.protection@schoolschoice.org

Lakenheath Community Primary School

PUPIL PRIVACY NOTICE

Privacy Notice - General Data Protection Regulation (GDPR) 2018



Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

We (Lakenheath Community primary School) collect and process personal data relating to its pupils in order to successfully carry out our functions. We are committed to being transparent about how we collect and use that data and to meet our data protection obligations.

Who We Are

Under Data Protection legislation, we are a data controller.

The contact details for the school are as follows:

Lakenheath Community Primary School

Mill Road

Lakenheath

Suffolk

IP27 9DU

Tel: 01842 860256

Our Data Protection Officer

The school's data protection officer is:

Schools' Choice Data Protection Team

Beacon House

Whitehouse Road

Ipswich

Suffolk

IP1 5PB

Tel: 01473 260700

Categories of Information

The school collects and processes a range of information about its pupils. This includes, but is not restricted to:

- Personal information (such as name, gender, date of birth unique pupil number, NHS number and address)
- Characteristics (such as ethnicity, religion, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Medical and Dietary Information
- Educational Information (such assessment information, special education needs information, exclusions/behavioural information)
- Safeguarding Information

- Photographs
- CCTV images captured on school grounds

We may also hold data about pupils that we have received from other organisations, including other schools, local authorities and the Department for Education.

Why We Collect and Use This Information

We use the pupil data:

- to support teaching and pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to comply with the law regarding data sharing
- to safeguard and promote the welfare of pupils
- to fulfil our contractual and other legal obligations
- to provide additional activities for pupils, for example, activity clubs and educational visits
- to protect and promote our interests and objectives - this includes fundraising

The Lawful Basis On Which We Use This Information

We only collect and use pupils' personal data when the law allows us to. Most commonly, we process it where:

- We need to comply with a legal obligation
- We need it to perform an official task in the public interest

Less commonly, we may also process pupils' personal data in situations where:

- We have obtained consent to use it in a certain way
- We need to protect the individual's vital interests (or someone else's interests)

Where we have obtained consent to use pupils' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

Some of the reasons listed above for collecting and using pupils' personal data overlap, and there may be several grounds which justify our use of this data.

Collecting Pupil Information

While the majority of information we collect about pupils is mandatory, there is some information that can be provided voluntarily. Whenever we seek to collect information from you or your child, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

Storing Pupil Data

We keep personal information about pupils while they are attending our school. We may also keep it beyond their attendance at our school if this is necessary in order to comply with our legal obligations. We hold pupil data until the child turns 24 years old.

Who We Share Pupil Information With

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about pupils with:

- schools that the pupils attend after leaving us
- our local authority

- the Department for Education (DfE)
- school nursing team
- school photographer
- online based software companies (Schoolcomms, test base, target tracker, mathletics, SATs companion etc)
- Residential trip venues (Eaton Vale, Burwell House)

Data Collection Requirements

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.

The National Pupil Database (NPD)

We are required to provide information about pupils to the Department for Education as part of statutory data collections such as the school census.

Some of this information is then stored in the [National Pupil Database \(NPD\)](#), which is owned and managed by the Department and provides evidence on school performance to inform research.

The database is held electronically so it can easily be turned into statistics. The information is securely collected from a range of sources including schools, local authorities and exam boards.

The Department for Education may share information from the NPD with other organisations which promote children's education or wellbeing in England. Such organisations must agree to strict terms and conditions about how they will use the data.

For more information, see the Department's webpage on [how it collects and shares research data](#).

You can also [contact the Department for Education](#) with any further questions about the NPD.

Transferring data internationally

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Parents and pupils' rights regarding personal data

Individuals have a right to make a '**subject access request**' to gain access to personal information that the school holds about them.

Parents/carers can make a request with respect to their child's data where the child is not considered mature enough to understand their rights over their own data (usually under the age of 12), or where the child has provided consent.

Parents also have the right to make a subject access request with respect to any personal data the school holds about them.

If you make a subject access request, and if we do hold information about you or your child, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you or your child
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

Individuals also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request please contact our data protection officer.

Schools' Choice Data Protection Team Tel: 01473 260700 Email: data.protection@schoolschoice.org

Parents/carers also have a legal right to access to their child's **educational record**. To request access, please contact Sally Esom, Head Teacher.

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance. Please refer to our Complaints Procedure which can be found on our school's website or our school office.

Further information

If you would like to discuss anything in this privacy notice, please contact:

Schools' Choice Data Protection Team Tel: 01473 260700 Email: data.protection@schoolschoice.org

