Leas Park Junior School Privacy Notice

Leas Park Junior School respects you and your child's privacy when you use the Organisation's services and is committed complying with privacy legislation.

The information below is what is referred to as a 'Privacy Notice' which explain how the Organisation uses and protects your personal information.

Leas Park Junior School has a Data Protection Officer whose role it is to ensure that any personal information processed by the Organisation is processed fairly and lawfully (respecting your rights and ensuring we follow the law). If you have any concerns or questions regarding how we look after your personal information, please contact the Data Protection Officer Marie Irving, at office@sherwood.notts.sch.uk or by calling 01623 842545.

Why we use your personal information

Why we use personal information

We may need to use some information about you to:

- deliver services and support to you;
- manage those services;
- train and manage the employment of our workers who deliver those services;
- help investigate any worries or complaints you have about your services;
- keep track of spending on services;
- check the quality of services; and
- to help with research and planning of new services.

What are our legal reasons for processing personal information?

There are a number of legal reasons why we need to collect and use personal data. Each privacy notice from the menu on the left explains for each service which legal reason is being used. Generally we collect and use personal information in the following circumstances:

- Where you, or your legal representative, have given consent
- Where you have entered into a contract with us
- Where it is necessary to perform our statutory duties
- Where it is necessary to protect someone in an emergency
- Where it is required by law
- Where it is necessary for employment purposes
- Where you have made your data publicly available
- Where it is necessary to establish, exercise or defend a legal claim
- Where it is in the substantial public interest
- Where it is necessary to protect public health
- Where it is necessary for archiving public interest material, research, or statistical purposes

Where we are using your consent to process your personal data, you have the right to withdraw that consent at any time. If you wish to withdraw your consent, please contact office@leaspark.notts.sch.uk. so that your request can be dealt with.

What is Personal Information?

Personal information is often records that can identify and relate to a living person. This can also include information that when put together with other information can then identify a person.

What are Special Categories of Information?

This is personal information that needs more protection due to its sensitivity. This information is likely to include:

- sexuality and sexual health
- religious or philosophical beliefs
- ethnicity
- physical or mental health
- trade union membership
- political opinion
- genetic/biometric data

How we limit the use of personal information

Where necessary Leas Park Junior School processes personal data to deliver our services effectively; but wherever possible, the data that we process will be anonymised, pseudonymised or de-personalised. This means the information can no longer identify a person.

When using personal data for research purposes, the data will be anonymised/pseudonymised to avoid the identification of a person, unless you have agreed that your personal information can be used for the research project.

We do not sell personal data to any other organisation for the purposes of selling products.

Your privacy rights

The law provides you with a number of rights to control the processing of your personal information:

Accessing the information we hold about you

You have the right to ask for all the information we have about you. When we receive a request from you in writing, we must normally give you access to everything we have recorded about you. However, we will not let you see any parts of your record which contain:

Confidential information about other people; or

- Data an information professional thinks will cause serious harm to your or someone else's physical or mental wellbeing; or
- If we think that the prevention or detection of crime may be adversely affected by disclosing data to you.

This applies to paper and electronic records. If you ask us, we will also let others see your record (except if one of the points above applies). If you cannot ask for your records in

writing, we will make sure there are other ways you can apply. If you have any queries regarding access to your information please contact office@leaspark.notts.sch.uk.

.Changing information you believe to be inaccurate

You should let us know if you disagree with something written on your file. We may not always be able to change or remove the information; however, we will correct factual inaccuracies and may include your comments in the records. Please use the contact details above to report inaccurate information.

Asking for your information to be deleted (right to be forgotten)

In some circumstances you can request the erasure of the personal information used by the Organisation, for example:

- Where the personal information is no longer needed for the purpose for which it was collected
- Where you have withdrawn your consent to the use of your information (where there is no other legal basis for the processing)
- Where there is no legal basis for the use of your information
- Where erasure is a legal obligation

Where personal information has been shared with others, the Organisation shall make every reasonable effort to ensure those using your personal information comply with your request for erasure.

Please note that the right to erasure does not extend to using your personal information where:

- Is required by law
- It is used for exercising the right of freedom of expression
- It is in the public interest in the area of public health
- It is for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes where it would seriously affect the achievement of the objectives of the processing
- It is necessary for the establishment, defense or exercise of legal claims.

Restricting what your information is used for

You have the right to ask us to restrict what we use your personal data for where one of the following applies:

- You have identified inaccurate information, and have notified us of this
- Where using your information is unlawful, and you wish us to restrict rather than erase the information
- Where you have objected to us using the information, and the legal reason for us using your information has not yet been provided to you

When information is restricted it cannot be used other than to securely store the data, and with your consent, to handle legal claims, protect others, or where it is for important public interests of the UK.

Where restriction of use has been granted, we will inform you before the use of your personal information is resumed.

You have the right to request that the Organisation stop using your personal information for some services. However, if this request is approved this may cause delays or prevent us delivering a service to you. Where possible we will seek to comply with your request, but we may need to hold or use information in connection with one or more of the Organisation's legal functions.

Computer based decisions about you and if you are 'profiled'

You have the right to object about decisions being made about you by automated means (by a computer and not a human being), unless it is required for any contract you have entered into, required by law, or you have consented to it. You also have the right to object if you are being 'profiled'. Profiling is where decisions are made about you based on certain things in your personal information. If and when the Organisation uses your personal information to profile you, you will be informed.

If you have concerns regarding automated decision making, or profiling, please contact the Data Protection Officer who will be able to advise you about how your information is being used.

Who will we share your personal information with?

We use a range of companies and partners to either store personal information or to manage it for us. Where we have these arrangements there is always a contract, memorandum of understanding or information sharing protocol in place to ensure that the organisation complies with data protection law. We complete privacy impact assessments before we share personal information to ensure their compliance with the law.

Sometimes we have a legal duty to provide information about people to other organisations, e.g. Child Protection concerns or Court Orders.

We may also share your personal information when we feel there is a good reason that is more important than protecting your confidentiality. This does not happen often, but we may share your information:

- For the find and stop crime or fraud; or
- if there are serious risks to the public, our staff or to other professionals; or
- to protect a child.

The law does not allow us to share your information without your permission, unless there is proof that someone is at risk or it is required by law.

This risk must be serious before we can go against your right to confidentiality. When we are worried about physical safety or we feel that we need to take action to protect someone from being harmed in other ways, we will discuss this with you and, if possible, get your permission to tell others about your situation.

We may still share your information if we believe the risk to others is serious enough to do so.

There may also be rare occasions when the risk to others is so great that we need to share information straight away. If this is the case, we will make sure that we record what information we share and our reasons for doing so. We will let you know what we have done and why as soon as or if we think it is safe to do so.

How do we protect your information?

We will do what we can to make sure we hold personal records (on paper and electronically) in a secure way, and we will only make them available to those who have a right to see them. Our security includes:

Encryption allows information to be hidden so that it cannot be read without special knowledge (such as a password). This is done with a secret code or cypher. The hidden information is said to be encrypted.

- Pseudonymisation allows us to hide parts of your personal information from view so only we can see it. This means that someone outside of ECC could work on your information for us without ever knowing it was yours.
- Controlling access to systems and networks allows us to stop people who are not allowed to view your personal information from getting access to it.
- Training for our staff allows us to make them aware of how to handle information and how and when to report when something goes wrong.
- Ways for us to access your information should something go wrong and our systems not work, including how we manage your information in event of an emergency or disaster.
- Regular testing of our technology and processes including keeping up to date on the latest security updates (commonly called patches).

Description of Security Measures employed to safeguard the processing of Personal Data

1. **Organisational**
   a. **Policies & Documented Procedures**
      Policies relating to information governance issues are drafted by employees with detailed knowledge of legal requirements and the Organisation's processes. All policies have documented review dates and ownership is assigned. Reviews are held ahead of the expiry date or sooner where there is an identified issue. All policies follow a governance route for approval. Key policies are published to the organisation's website for transparency.
   b. **Roles**
      The organisation has a named Data Protection Officer who is Marie Irving. This Officer executes the role by reporting the outcome of statutory process to Helen Atkins who acts as the organisation's Senior Information Risk Owner.
   c. **Training**
      The organisation regularly reviews our employee roles to ensure that training and awareness messages are appropriate to the nature and sensitivity of the data processing undertaken. Induction processes ensure new employees receive appropriate training before accessing personal data, and all other employees receive refresher training annually. All training received is documented for evidence purposes.
   d. **Risk Management & Privacy by Design**
      The organisation identifies information compliance risks on its risk register. Risks are assigned clear ownership, rated against a consistent schema; appropriate mitigations are identified and are annually reviewed.
   e. **Contractual Controls**
      All Data Processors handling personal data on behalf of the organisations have given assurances about the compliance of their processes; either through

procurement assurances/ evidence, contractual agreement controls, risk assessments or supplementary statements.

f. Physical Security

All employees or contractors who have access to our premises where personal data is processed are provided with Identity Cards which validate their entitlement to access. The organisation operates processes which ensure only those individuals who have an entitlement to access premises are able to. Access to physical storage holding sensitive personal data is further restricted either through lockable equipment with key or code control procedures or through auditable access to specific rooms/ areas of buildings.

g. Security Incident Management

The organisation maintains a security incident process which, with the support of appropriate training, defines what constitutes a breach of these security measures to facilitate reporting of incidents. The process covers investigation of incidents, risk rating and decisions over whether to notify an incident to the Information Commissioner's Office (ICO) within the statutory timescale. Incidents are reported to senior leaders and actions are consistently taken and lessons learned implemented.

2. Technical

a. Data at Rest

i. Use of Hosting Services

Some personal data is processed externally to the organisation's managed environment by third parties in data centres under agreed terms and conditions which evidence appropriate security measures.

ii. Firewalls

Access to the Organisation's managed environment is protected by maintained firewalls. Business needs to provide access through the firewall go through a strictly documented change control process which include risk assessment and approval.

iii. Administrator Rights

Enhanced privileges associated with administrator accounts are strictly managed. Administrator activities are logged and auditable to ensure activity can be effectively monitored.

iv. Access Controls

Access permissions to personal data held on IT systems is managed through role based permissions. Managers of appropriate seniority inform IT professionals of additions, amendments and discontinuation of individual accounts within permission groups. Managers are periodically required to confirm that current permissions for which they are the authoriser and employees associated with these permissions are accurate.

v. Password Management

The organisation requires a mandatory password complexity combination of minimum length and characters, plus a required change of password after 90 days.

vi. Anti-Malware & Patching

The organisation has a documented change control process which facilitates the prompt implementation of any security updates provided by the suppliers of active software products.

vii. **Disaster Recovery & Business Continuity**

As part of the organisation's business continuity plan, there is provision to ensure effective processes are in place to both safeguard personal data during a service outage incident and to re-establish secure access to the data to support data subject rights in ongoing service provision.

b. Data in Transit

i. **Secure email**

The organisation has access to secure email software for communicating with some third parties where licensing agreements permit this. Sensitive data will be sent using such tools where available. Where software is not available a system of password protecting sensitive data in email attachments is employed.

ii. **Secure Websites**

The organisation has access to third party websites which allow for secure upload of personal data. The organisation uses these facilities to fulfil statutory obligations to report personal data to other public authorities.

iii. **Encrypted Hardware**

Devices which store or provide access to personal data are secured by password access. Removable media such as memory sticks are encrypted.

iv. **Hard-Copy Data**

The removal of personal data in hard-copy form is controlled by organisational policy which requires employees to take steps to conceal the data and appropriately secure the data during transport.

These security measures are reviewed annually and approved as accurate and appropriate by the organisation's governance process.

If your information leaves the country

Sometimes, for example where we receive a request to transfer Organisation records to a new Organisation, it is necessary to send that information outside of the UK. In such circumstances additional protection will be applied to that data during its transfer, and where the receiving country does not have an adequacy decision from the European Commission, advice will be sought from the Information Commissioners Office prior to the data being sent.

How long do we keep your personal information?

For each reason why we use your personal information there is often a legal reason for why we need to keep it for a period of time. We try to capture all of these and detail them in what's called a 'retention schedule'. This schedule lists for each service how long your information may be kept for; a copy of the retention schedule is available on request.

Where can I get advice?

You can contact our Data Protection Officer, Marie Irving at office@sherwood.notts.sch.uk or by calling 01623 842545.

For independent advice about data protection, privacy and data sharing issues, you can contact the Information Commissioner's Office (ICO) at:
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

Tel: 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate number

Alternatively, visit ico.org.uk or email casework@ico.org.uk.

Cookies (not the edible ones) & how you use this website

To make this website easier to use, we sometimes place small text files on your device (for example your iPad or laptop). These are known as 'cookies'. Most big websites do this too.

They improve things by:

- remembering the things you've chosen, so you don't have to keep re-entering them whenever you visit a new page
- remembering data you've given (for example, your address) so you don't need to keep entering it
- measuring how you use the website so we can make sure it meets your needs.

By using our website, you agree that we can place these types of cookies on your device.

We do not use cookies on this website that collect information about what other websites you visit (often referred to as privacy intrusive cookies).

Our cookies aren't used to identify you personally. They're just here to make the site work better for you. Indeed, you can manage and/or delete these files as you wish.

To learn more about cookies and how to manage them, visit AboutCookies.org or watch a video about cookies.

How you use this website (something called 'Google Analytics')

We use Google Analytics to collect information about how people use this site. We do this to make sure it's meeting peoples' needs and to understand how we can make the website work better.

Google Analytics stores information about what pages on this site you visit, how long you are on the site, how you got here and what you click on while you are here. We do not collect or store any other personal information (e.g. your name or address) so this data cannot be used to identify who you are.

Name	Typical Content	Expires
_utma	randomly generated number	2 years
_utmb	randomly generated number	30 minutes
_utmc	randomly generated number	when you close your browser
_utmx	randomly generated number	2 years
_utmxx	randomly generated number	2 years
_utmz	randomly generated number and data on how the site was reached (e.g. direct or via a link, organic search or paid search)	

We also collect data on the number of times a word is searched for on the site and the number of failed searches. We use this information to improve access to the site and to identify gaps in the content and see if it is something we should add to the site.

Unless the law allows us to, we do not:

- share any of the data we collect about you with others, or
- use this data to identify individuals.

Other people's cookies

We use videos from YouTube and feeds from other websites such as Facebook and Twitter. These websites place cookies on your device when watching or viewing these pages.

Below are links to their cookie policies:

- Google and YouTube
- Facebook
- Twitter

Turning off cookies

You can stop cookies being downloaded on to your computer or other device by selecting the appropriate settings on your browser. If you do this, however, you may not be able to use the full functionality of this website.

There is more information about how to delete or stop using cookies on AboutCookies.org. If you wish, you can also opt out of being tracked by Google Analytics.

Further guidance on the use of personal information can be found at ico.org.uk