Data Protection and Access to Information Policy

The Company is committed to fulfilling its obligations and will comply with all statutory requirements of the General Data Protection Regulation (Regulation (EU) 2016/679)(GDPR), Data Protection Act 2018 and the Freedom of Information Act 2000. This imposes legal obligations on the way in which the Company obtains, records and processes personal information about employees and third parties, whether this is done manually or electronically.

Personal data is information which relates to an individual who can be identified from that information.

Some information is classified as "Sensitive Personal Data" and there are special rules which apply when processing this type of data.

The Company processes personal data if it holds personal data and/or carries out any operation relating to that information, such as altering or deleting, accessing, downloading, reviewing or transferring it.

The ultimate responsibility for data protection within the Company lies with the Directors and they are supported by the Operational Manager to ensure compliance with the requirements of GDPR, Data Protection Act, the Freedom of Information Act and to give guidance in cases of doubt.

If you are a user of such information, you need to be sure that you are not breaching any data protection rules when you store or use information and when you write and send emails. This could include but is not limited to:

- using data which has not been kept up-to-date;
- passing on or processing personal information about an individual without their consent;
- keeping personal information for longer than necessary; and/or
- sending personal information outside the country.

The Company cannot comply with its legal obligations unless all employees ensure that they comply with this policy. Employees and officers of the Company may also face criminal liability in certain circumstances.

Each employee is required to:

- read and comply with this Policy and the Company Privacy and Confidentiality Policy; and
- when in doubt, seek guidance from the Directors/Operational Manager; and
- immediately notify their line Manager of all changes to their personal information to ensure that records are correct and up-to-date.

If any breach of data protection rules is discovered, such as the leaking or hacking of personal or sensitive data, this should be reported immediately to your line Manager, and any immediate action should be taken to close down such leaks. Your line Manager will ensure this is properly investigated in liaison with the Directors/Operational Manager and the appropriate reporting actions taken if necessary.

Employees can request access to the information held on them by the Company. All requests by employees to gain access to such records should be made in writing to their line Manager.

If an employee receives a subject access request, they should refer this immediately to their line Manager. The Company will endeavour not to keep information for any longer than is necessary for the purpose for which it is being processed. Employees must comply with any instructions of their line Manager/Operational Manager/Directors concerning the retention of data. If employees know that information is incorrect or misleading as to any matter of fact, or is out of date, they should arrange for it to be corrected as soon as possible.

January 2024

Personal data on employees is held in accordance with the provisions of the Company's Privacy Notices, a hardcopy of which is provided upon commencement of employment with the Company and is available for reference by employees if required within the nursery Office.

Data protection is a serious matter. A failure to comply with this policy may result in disciplinary action which could result in summary dismissal.