Confidentiality & Data Protection Policy

Aims

To ensure that the setting treats all confidential and personal information and data (whether written or verbal) in an appropriate way and in line with the Data Protection Act 2018 and the United Kingdom General Data Protection Regulation (UK-GDPR) as follows:

- To ensure that all information is stored, shared, archived and deleted according to the regulations and guidance of the UK-GDPR
- To ensure that the staff team are aware of the implications of the UK-GDPR in connection with their roles and responsibilities within the setting.
- To ensure there is a Privacy Notice for parents and employees.
- To ensure there is an Information Audit/Record of processing activity.
- To ensure that parents/carers are able to access the setting's policies and procedures.
- To ensure that parents/carers are able to access records kept about their child.

Procedure

The setting will comply with the seven principles of the UK-GDPR which state that data processing must be:

- lawful, fair and transparent;
- only used for the purpose for which it was originally requested (unless with further consent) and the setting will be clear about the purpose of the data processing;
- limited to what is adequate to fulfil its purpose and relevant;
- accurate and kept up to date;
- retained for no longer than necessary and deleted appropriately;
- processed in a secure way, with integrity and responsibility, to protect the data and avoid loss or damage.
- accountability. The data controller is responsible for and needs to show compliance with the principles listed above.

- The setting will appoint a 'data controller' and, if required, will register with the Information Commissioner's Office (ICO).

- There is a legal requirement for the setting to keep certain information in order to register a child, such as a child's date of birth and parents' contact details. There is also a statutory requirement to keep some record of the learning progress of each child. There will be other information which the setting may request, based on consent; the setting will indicate which data requests are consent based in order that parents/carers can

make an informed choice, for example, taking photographs of a child. Parents/carers have the option to refuse or withdraw consent at any time.

- When requesting consent-based data for children under 13 years, the setting will obtain consent from whichever adult holds parental responsibility for that child. The setting will make reasonable effort to verify that the person giving consent for the child does have parental responsibility for that child.

- In line with the EYFS, the setting will liaise with parents/carers to keep them updated about their child's well-being and progress. Parents/carers have the right to see any information that is held on them as well as that of their children. The Parents' Privacy notice will detail this and the "lawful basis" for holding this data.

- In line with the EYFS and Employment Law, the setting will keep records on employees and volunteers to ensure suitability, good practice and well-being. Employees and volunteers have the right to see any information that is held on them.

- The setting will store all personal records in a secure location. Paper records will be kept in lockable storage. Electronic records will be password protected. Security measures will be implemented for all portable electronic equipment.

- The management, staff, volunteers and any other individual associated with the running or management of the setting will respect confidentiality by:

  - not discussing confidential matters about children with other parents/carers;
  - not discussing confidential matters about parents/carers with children or other parents/carers;
  - not discussing individual children outside of the setting;
  - not discussing confidential information about staff members.

- Any child protection concerns will be handled in line with the setting's Child Protection Policy – please see Child Protection Policy for details.

- Parents/carers will be made aware that the setting has a duty to share and/or pass on child protection/safeguarding information to relevant agencies and the next education provider.

- Parents/carers will have, on request, access to their own child's records only, unless subject to an exemption. If for any reason an access request is refused by the setting, this decision, and an explanation, will be communicated to the parents/carers in writing within a month.

- Staff will only discuss individual children with other relevant members of staff for the purposes of planning/reviewing, group management or safeguarding.

- Personal information about a child will not be released to external agencies without the prior permission of parents/carers. The setting will seek active consent from parents/carers to share information with health, education and inclusion professionals. The exception to this is for safeguarding reasons, where doing so would put the child at significant risk of harm.

- Parent/carer information may be shared with the HMRC and other providers of funded places, where necessary, e.g. a child accessing two or more settings.

- Staff, management, students and volunteers failing to show due regard for confidentiality will be liable to disciplinary action under the provisions of the Disciplinary Procedure.

- This setting will not share data with any third party unless specified above.

Data Protection Impact Assessment (DPIA)

In line with UK-GDPR, the setting will undertake a DPIA for any new project or system when the type of processing is likely to result in high risk and the project involves using personal data. Guidance on how to do this will be sought from the Information Commissioner's Office (ICO) website.

Data Breach

If a data breach occurs, i.e. personal data is lost, destroyed, shared inappropriately or if someone accesses the information without permission, the setting will investigate the breach within 72 hours including:

- informing the individuals involved;
- promptly addressing the breach;
- identifying the severity of the breach;
- reporting the breach to the ICO, if required. Failure to notify may result in a fine.

If it is decided not to report the breach the setting will justify this decision and record it as an incident in the Log of Data Breaches. The setting will then identify what needs to be implemented to ensure this breach doesn't not occur again.

Parents have the right to complain to the ICO.

Retention of Records

- When a child leaves, the setting will hand over educational records (learning diary) and photographs to the parents/carers and delete any copies. Other records will be retained

by the setting and destroyed as appropriate according to the setting's Retention of Records Policy.

- If the setting closes, records will be kept securely according to the Retention of Records Policy.

- Paper documents will be destroyed by being cross-shredded or burnt. Information stored on digital storage devices will be deleted when it is no longer required.

- Staff records will be retained throughout their employment and when an individual leaves, some records will be retained in line with the setting's Retention of Records Policy or destroyed as above.

For further information see:

- Data Protection:
  Information Commissioner's Office (ICO) - https://ico.org.uk/
  Gov.UK: https://www.gov.uk/data-protection

- Guidance on the Transfer of a Child Protection Safeguarding File to another Education Setting: https://bristolsafeguarding.org/media/n0nlf1ue/kbsp-transfer-of-cp-and-safeguarding-file-update-final-version.pdf