1.09 Use Of Tapestry

Safeguarding and Welfare Requirement: Child Protection.

The safeguarding policy and procedures must include and an explanation of the action to be taken in the event of an allegation being made against a member of staff and cover the use of the EYFS learning Tapestry.

Policy Statement

We use the wealth of information gathered about individual children to create a Learning Tapestry file, which contains detailed individual observations of self-initiated activity in a particular context, photos and special moments as well as pieces of children's work. These are to be used to document and monitor the individual learning and development progress of each child in Preschool The information contained within each learning file is to relate to an individual, identifiable child; therefore it is to be treated as personal data. This means that such information is to be stored securely when not in use. The aim will be to avoid unauthorised access to potentially sensitive data.

Consent must be obtained from parents and carers should their child be photographed amongst a group of children; and where consideration is to be given to including that image in a learning file belonging to another child. It will be anticipated that this will be a regular occurrence, as group activity shots are to be encouraged.

Where possible, therefore, 'blanket' consent will be requested from parents and carers for group images to be included in the learning files of other children. Parents and carers must be given the option to view any images before they are to be included in any learning story, should they request to do so. Parents and carers will also be permitted to restrict their consent. This may mean that group images can only be included in specified learning stories, for example, those which are to belong to close friends. Should it not be possible to obtain consent, the relevant image must not be shared across learning files of other children.

Individual learning files are provided for the benefits of the individual child and their parents or carers. Parents and carers are therefore to be given the responsibility for choosing what to do with any personal data contained in the learning file, once it is to be in their possession. However parents must be made aware that they are not permitted to 'publicise' another child without the express agreement of the parent or carer concerned. Parents and carers must therefore be reminded that they must not share, distribute or display said images without relevant authorisation and consent from the parents and carers of all children and young people captured in any of the photographs.

All new admissions to our preschool will be asked to sign a letter, stating that they will not upload images of any children at St John's Preschool.

Early years practitioners training portfolios

During training, early years practitioners may be required to compile portfolios which will be used to document and evidence their own learning. Part of this documentation may include images of the early years practitioner working alongside children and young people participating in various activities. Should such evidence be required, parent or carer consent will be requested.

Storage and disposal

Images are to be stored and disposed of securely. The aim will be to prevent unauthorised access, ensure confidentiality and protect identity. All images are to be stored and disposed of in line with the Data Protection Act 2018 and GDPR regulations.

Images will not be kept for longer than is to be considered necessary. The Senior Designated Person for Safeguarding is to ensure all photographs are to be permanently wiped from memory cards, computer hard and portable drives or other relevant devices once the images will no longer be of use. Should images need to be kept for a short period of time, they must be protectively stored and password protected on the computer hard drive or other appropriate storage device. Such equipment will be stored securely and access will be restricted.

Photographs must be disposed of should they no longer be required. It must be ensured that they will be returned to the parent or carer, deleted and wiped or shredded as appropriate. Copies are not to be taken of any images without relevant authority and consent from the Senior Designated Person for Safeguarding and the parent or carer.

A record of all consent details are to be kept on file. Should permission be withdrawn at any time, all relevant images will be removed and disposed of. The record will be updated accordingly.

Security

All images are to be handled as personal data and deemed to be of a sensitive and confidential nature. It is to be recognised that damage or distress could be caused if security is to be breached. The responsibility of being in a position of trust in handling such data must therefore be taken seriously. The Senior Designated Person for Safeguarding is to be responsible for ensuring all information is handled appropriately and securely. Should there be any concerns over breaches of security, the Senior Designated Person for Safeguarding and/or the registered person will be required to undertake an investigation as is to be deemed appropriate. All such incidents are to be recorded and where necessary reported to the relevant authorities. Any actions which are to be identified as a result of any investigations must be implemented with immediate effect.

Under the Data Protection Act 1998, reasonable steps must be taken to ensure the reliability and suitability of any individual who is to have access to personal data. Staff are therefore considered to be in a responsible position of trust. To this effect, effective safer recruitment procedures are to be applied. Rigorous and regular checks are also to be undertaken to ensure the on-going suitability of all new and existing early years practitioners and their managers. All relevant checks must be completed before any new employee, volunteer or student is to be given access to children and/or their personal data. All early years practitioners are to be required to follow confidentiality and information sharing procedures, which must be agreed to at the time of induction.

Physical security – effective measures are to be put in place to ensure physical security and to protect against theft, including that of laptops, computers, cameras, and any personal data, including photographic images.

Computer security – stringent measures are to be implemented to ensure computer security. Awareness will be raised in respect of technological advancements which could put online systems at risks. Security will be updated as and when it is to be required. Security procedures are to be proportionate to the potential risks involved and must be subject to constant monitoring and review.

Legislative framework

Data Protection Act 2018 Freedom of Information Act 2000, Human Rights Act 1998, GDPR Regulations and other relevant Acts regarding the taking and use of photographic images of children.

Date to be reviewed – by end of March 2023