**DATA PROTECTION and PRIVACY POLICY**

**09/23**

**The Wilderness Grove Forest School Data Protection and Privacy Policy**

The Wilderness Grove collects and uses personal information about staff, children, parents, and other individuals who come into contact with the provision. This information is gathered to enable TWiG to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the forest school complies with its statutory obligations.

This Code of Practice has been issued to give guidance to employees, volunteers and any other person delivering services to customers/participants/beneficiaries of TWiG, so that any data which TWiG holds is stored safely, processed correctly and not unlawfully disclosed to any other person, and that such processing of data complies with Data Protection Law, namely the UK GDPR (2021) and its implementation of the UK GDPR Regulations 2021. TWiG management and staff should also familiarise themselves with TWiG’s Data Protection Policy.

TWiG’s data protection officer is Cate Regi (see contacts below).

**Purpose**

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 2018, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored, and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

**What is Personal Information?**

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held.

**Application of this Code of Practice**

This Code of Practice applies to “Personal Data”, which is defined as: information (including opinions and intentions) which relates to an identified or identifiable natural person.

**Identity**

An “identifiable natural person” is an individual who can be identified, directly or indirectly, by information such as: a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person. If, by looking solely at the information you are processing you can distinguish an individual from other individuals, that individual will be identified (or identifiable). Identifiers are wide ranging, for example, a name or number, an Internet Protocol (IP) address or an image.

**Sensitive Personal Data**

TWiG recognizes that sensitive personal data (including “Special Category Data” as defined in Data Protection legislation) is likely to be of a very personal nature and that it may only be processed with the \*express consent of the individual concerned. In accordance with legislation and KE’s Data Protection Policy, TWiG treats the following information about a person as sensitive personal data:

Racial or ethnic origin  
Political opinions  
Religious or philosophical beliefs  
Trade Union membership  
Physical or mental health or condition  
Genetic data  
Biometric data  
Sexual life and sexual orientation  
Alleged or actual commission of a criminal offense

Examples of the type of sensitive personal data that TWiG may hold include details of an individual’s health, medication, physical needs and criminal convictions. TWiG strives to collect, process, and hold only data that is necessary and appropriate for the Forest School to provide its services and comply with any contract or legislation. Employees and volunteers working with participants should only request and process sensitive personal data if requested to do so in the forms provided for the course, or specifically by their line manager.

**Data Protection Principles**

TWiG has adopted the following principles to govern its collection, use, retention, transfer, disclosure, and destruction of personal data.

Processes have been put in place at TWiG (for example the use of specific forms to capture participant information) to ensure compliance with appropriate legislation and these principles. Employees and volunteers should ensure that they follow these processes and if in doubt they ask the for clarification.

## Lawfulness, Fairness and Transparency

Personal data shall only be processed lawfully, fairly and in a transparent manner. This means, TWiG must tell participants what processing will occur (transparency), the processing must match the description given to the participant (fairness), and it must be for one of the purposes specified in the applicable Data Protection legislation (lawfulness).

## Purpose Limitation

Personal data shall only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means TWiG must specify exactly what the personal data collected will be used for and limit the processing of that personal data to only what is necessary to meet the specified purpose.

## Minimisation

Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes. This means TWiG must not collect, process, or store any personal data beyond what is strictly required.

## Accuracy

Personal data shall be accurate and kept up to date. (More on keeping personal data up to date, below.)

## Online Storage

TWiG holds computerised files and folders in Famly, an online data storage system and communication platform.

## Limitation

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

## Integrity & Confidentiality

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, and against accidental loss, destruction, or damage.

## Accountability

Each person responsible for personal data at TWiG should be able to demonstrate compliance. This means they must demonstrate that the six data protection principles (outlined above) are met for all personal data for which they are responsible.

## Handling Personal data

Personal data should only be collected in accordance with questions on the appropriate online and hard copy forms approved for the processing of information.

Information collected from course participants manually at indoor or outdoor locations should be always kept out of sight of participants and stored at the end of the same working day in the filing cabinet in the pod.

Forest School staff and others working with participants should pass all completed participant paperwork to the administrator at the very earliest opportunity, who will ensure it is stored electronically and hard copies destroyed.

At NO time leave participant paperwork unsupervised during the working day or left unsecured during out of work hours

**TWiG Policy**

Personal data being displayed on computer screens should be closed when unattended.

Photography and film: Photographs and other forms of picture capture, eg video, are permitted to be taken on personal mobile phones. At the end of the same working day ALL participant photographs and videos MUST be transferred to the secure Famly App or sent via Whats App to Cate Regi. All participant photographs on mobile phones MUST then be deleted at the end of each working day and removed from Google access accounts.

Only photographs or videos that contain individuals with known written consent for internal and external media use should be uploaded to Famly.

Media and social media: Under NO circumstances should photographs or videos be shared with the press, on our website, on social media, or in any other publication, unless those involved have given written consent. Under NO circumstances should any other personal data be shared through social media.

Sharing personal data with third parties: in some circumstances, we are required to share certain data with referring organisations or authorities. If identifying personal data is to be shared, you should check with the office administrator whether sharing is permitted in the circumstances and ensure any method of transfer is secure. (More on sharing personal data, below.)

## Mobile phones, tablets, laptops, and other portable electronic data storage units:

Any portable device, whether owned by an individual or TWiG, used for receiving, processing or sending any information containing personal data of employees, volunteers, participants, service users, family, friends or associates of those individuals and any TWiG supporters, donors, suppliers, contractors or consultants, should be secured and kept out of public view if left unattended (e.g. kept in a locked box in the locked shed). Access to the device should also be password protected.

Preferably, all personal data should be stored on TWiG’s Famly Account and not be stored  
directly on portable equipment hard drives or USB devices unless it is entirely necessary, in which case it should be encrypted, or password protected.

## Protecting personal data about course participants (both children in Tribes and Candidates of training courses)

In the course of their work, staff, volunteers, and associates may have access to personal information. This document outlines company policy regarding privacy and data protection.

Personal data that TWiG may collect, use, store, and share (when appropriate) about children includes, but is not restricted to:

* Contact details, contact preferences, date of birth, identification documents.
* Records
* Characteristics or special educational needs
* Exclusion information
* Details of medical conditions, including physical and mental health
* Attendance information
* Safeguarding information
* Details of support received, including care packages, plans and support providers.
* Photographs   
  TWiG may also hold data about children that has been supplied from other organisations such as schools, local authorities and the Department for Education.   
  Purpose   
  TWiG uses this data to:

• Support children / adults to learn

• Monitor and report on progress

• Provide appropriate care

**Data Protection Principles**

The Data Protection Act 2018 establishes eight enforceable principles that must be adhered to at all times:

1. Personal data shall be processed fairly and lawfully.

2. Personal data shall be obtained only for one or more specified and lawful

purposes.

3. Personal data shall be adequate, relevant, and not excessive.

4. Personal data shall be accurate and where necessary, kept up to date.

5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data

subjects under the Data Protection Act 2018.

7. Personal data shall be kept secure i.e., protected by an appropriate degree of security.

8. Personal data shall not be transferred to a country or territory outside the

European Economic Area unless that country or territory ensures an adequate level of data protection.

**General Statement**

The Wilderness Grove is committed to maintaining the above principles at all times.

Therefore, we will:

* Inform individuals why the information is being collected and when it is collected.
* Inform individuals when their information is shared, and why and with whom it was shared.
* Check the quality and accuracy of the information it holds.
* Ensure that information is not retained for longer than is necessary.
* Ensure that when obsolete, information is destroyed and that it is done so appropriately and securely.
* Ensure that clear and robust safeguards are in place to protect personal information from loss, theft, and unauthorised disclosure, irrespective of the format in which it is recorded.
* Share information with others only when it is legally appropriate to do so.
* Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests
* Ensure our staff are aware of and understand our policies and procedures.

**Complaints**

Complaints will be dealt with in accordance with the complaints policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

**Review**

This policy will be reviewed as it is deemed appropriate, but no less frequently than every year. The policy review will be undertaken by the Managing FSL, or another nominated representative.

**Contacts**

If you have any enquiries in relation to this policy, please contact Cate Regi or Thomas Wild, The Wilderness Grove, Aylesbury Cottage, Fritton Norfolk, NR31 9AB who will also act as the contact point for any subject access requests.

Further advice and information is available from the Information Commissioner’s Office, www.ico.gov.uk or telephone 01625 545745 3

**Appendix 1**

Procedures for responding to subject access requests made under the Data

Protection Act 2018

**Rights of access to information**

There are two distinct rights of access to information held by the Forest School about children.

1. Under the Data Protection Act 2018 any individual has the right to make a

request to access the personal information held about them.

2. The right of those entitled to have access to curricular and educational records as defined within the Education Pupil Information (Wales) Regulations 2004. These procedures relate to subject access requests made under the Data Protection Act 2018.

**Actioning a subject access request**

1. Requests for information must be made in writing, which includes email, and be addressed to The Wilderness Grove. If the initial request does not clearly identify the information required, then further enquiries will be made.

2. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:

* passport
* driving licence
* utility bills with the current address
* Birth / Marriage certificate
* P45/P60
* Credit Card or Mortgage statement

*This list is not exhaustive*.

3. Any individual has the right of access to information held about them. However, with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Forest School leader or Director should discuss the request with the child and take their views into account when deciding. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

5. The response time for subject access requests, once officially received, is 40 days **(not working or school days but calendar days, irrespective of school holiday periods)**. However, the 40 days will not commence until after receipt of fees or clarification of information sought.

6. The Data Protection Act 2018 allows exemptions as to the provision of some information; **therefore, all information will be reviewed prior to disclosure**.

7. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school.

Before disclosing third party information consent should normally be obtained.

There is still a need to adhere to the 40-day statutory timescale.

8. Any information which may cause serious harm to the physical or mental health or emotional condition of the child, or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

9. If there are concerns over the disclosure of information then additional advice should be sought.

10. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained so that if a complaint is made, it can be established what was redacted and why.

11. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

12. Information can be provided at The Wilderness Grove with a member of staff on hand to help and explain matters if requested or provided at face-to-face handover.

The views of the applicant should be considered when considering the method of delivery. If postal systems have to be used, then registered/recorded mail must be used.

**Contact**

If you have any queries or concerns regarding these policies / procedures, then please contact the Managing Partners of The Wilderness Grove.

Further advice and information can be obtained from the Information.

Commissioner’s Office, www.ico.gov.uk or telephone.