



Privacy Policy

At Potential Kids we respect the privacy of the children attending the Club and the privacy of their parents or carers, as well as the privacy of our staff. Our aim is to ensure that all those using and working at Potential Kids can do so with confidence that their personal data is being kept secure.

Our lead person for data protection is Peter Lowe. The lead person ensures that Potential Kids meets the requirements of the GDPR, liaises with statutory bodies when necessary, and responds to any subject access requests.

Confidentiality

We respect confidentiality in the following ways:

- We will only ever share information with a parent about their own child.
- Information given by parents to Potential Kids staff or volunteers about their child will not be passed on to third parties without permission unless there is a safeguarding issue (as covered in our **Safeguarding Policy**).
- Concerns or evidence relating to a child's safety, will be kept in a confidential file and will not be shared within Potential, except with the appointed safeguarding Officer and the trustees.
- Staff only discuss individual children for purposes of planning and group management.
- Staff are made aware of the importance of confidentiality during their induction process.
- Issues relating to the employment of staff, whether paid or voluntary, will remain confidential to those making personnel decisions.
- All personal data is stored securely in a lockable file / on a password protected computer at The Galleria
- Students on work placements and volunteers are informed of our Data Protection policy and are required to follow it.

Information that we keep

The items of personal data that we keep about individuals are documented on PK personal data base. Personal data is reviewed annually to ensure that any new data types are included.

Children and parents: We hold only the information necessary to provide a childcare service for each child and young person. This includes child registration information, medical information, parent contact information, attendance records, incident and accident records

and so forth. Our lawful basis for processing this data is fulfilment of our contract with the child's parents. Our legal condition for processing any health-related information about a child, is so that we can provide appropriate care to the child. Once a child leaves our care we retain only the data required by statutory legislation and industry best practice, and for the prescribed periods of time. Electronic data that is no longer required is deleted and paper records are disposed of securely or returned to parents.

Staff: We keep information about employees to meet HMRC requirements, and to comply with all other areas of employment legislation. Our lawful basis for processing this data is to meet our legal obligations. Our legal condition for processing data relating to an employee's health is to meet the obligations of employment law. We retain the data after a member of staff has left our employment for the periods required by statutory legislation and industry best practice, then it is deleted or destroyed, as necessary.

Sharing information with third parties

We will only share child information with outside agencies on a need-to-know basis and with consent from parents, except in cases relating to safeguarding children, criminal activity, or if required by legally authorised bodies (eg Police, HMRC, etc). If we decide to share information without parental consent, we will record this in the child's file, clearly stating our reasons.

We will only share relevant information that is accurate and up to date. Our primary commitment is to the safety and well-being of the children in our care.

Some limited personal information is disclosed to authorised third parties we have engaged to process it, as part of the normal running of our business, for example in order to take online bookings, and to manage our payroll and accounts. Any such third parties comply with the strict data protection regulations of the GDPR.

Subject access requests

- Parents/carers can ask to see the information and records relating to their child, and/or any information that we keep about themselves.
- Staff and volunteers can ask to see any information that we keep about them.
- We will make the requested information available as soon as practicable and will respond to the request within one month at the latest.
- If our information is found to be incorrect or out of date, we will update it promptly.
- Parents /carers can ask us to delete data, but this may mean that we can no longer provide care to the child as we have a legal obligation to keep certain data. In addition, even after a child has left our care, we have to keep some data for specific periods so won't be able to delete all data immediately.
- Staff and volunteers can ask us to delete their data, but this may mean that we can no longer employ them as we have a legal obligation to keep certain data. In addition, even after a staff member has left our employment we have to keep some data for specific periods so won't be able to delete all data immediately.
- If any individual about whom we hold data has a complaint about how we have kept their information secure, or how we have responded to a subject access request, they may complain to the Information Commissioner's Office (ICO).

GDPR

We comply with the requirements of the General Data Protection Regulation (GDPR), regarding obtaining, storing and using personal data.

Data Protection Act Information

We keep a file in the office for all learners and volunteer assessors. The learner files have details of enrolment and registration with OCN. These details are also stored on computer. We also keep copies of learner action plans, feedback sheets and records of certification and internal quality assurance. This information is required and seen by Centre staff, internal and external quality assurers.

All assessors have a file in the centre in which information required by IQA and EQA is kept.

Freedom of Information Act

The right to know: From 1/1/2005 anyone can request information held by public authorities including Central Government, Local Authorities, NHS, Schools and Police.

Citizens' Rights under the Act: Right to request information and the public authority has a duty to confirm or deny information held by them, and 20 days to communicate the information. There is a right of appeal. There are exemptions to the law. Further information and guidance available from www.informationcommissioner.gov.uk

When personal data is stored on any mobile device or removable media the:

- **data must be encrypted and password protected.**
- **device must be password protected.** (be sure to select devices that can be protected in this way)
- **device must be protected by up to date virus and malware checking software**
- **data must be securely deleted from the device, in line with school/academy policy (below) once it has been transferred or its use is complete.**

Reviewed 6/5/25 To be reviewed:7/5/26	Signed:  Angela Gaughan Founder & CEO
This policy was adopted by: Potential kids	Date:1/12/2019