National Guidance
oeapng.info

Participant Information and Data Protection

This document is about the need to securely gather and use information about visit participants. For guidance on parental consent, and on the provision of information to parents, see OEAP National Guidance document 4.3d "Parental Consent and Informing Parents".

Participant Information

It is essential that the visit leadership team has access to up-to-date information in order to manage the welfare of young people. This typically includes emergency contact details and medical, dietary and other considerations such as confirmation of swimming ability.

Establishments should have a mechanism in place for obtaining this information, updating it, and communicating it to those who need it. Where the information is transcribed to a summary sheet, or where a database such as the Student Information Management System is used to provide a summary, there must be a process to ensure the accuracy and currency of the information. Information may be gathered in any way that is effective and secure, such as an annual form, visit-specific form, tear-off reply slip, website portal, email etc.

See OEAP National Guidance Document
8.1e "Model Parental Consent and Information Form"

You should ensure that parents are made aware of the importance of disclosing information. You should inform them that disclosure is unlikely to affect the opportunities for their child to participate in off-site visits and activities, but that the information may be essential to allow the Visit Leaders, and possibly specialist activity leaders, to manage their child's participation safely.

There should be a robust arrangement for keeping welfare, medical and emergency information up to date. Sensitive information should be kept secure but accessible and understood by those who need it, including relevant leaders from other organisations. Consideration should be given to how that information is carried. This might include copies of medical forms, a printed summary sheet or electronic data storage. You should ensure that individuals' confidentiality can be protected, and personal information securely disposed of when it is no longer needed.

Data Protection

Processing of personal data, which is defined below, must comply with the Data Protection Act 2018 (DPA) which includes the General Data Protection Regulation (GDPR). 'Processing' covers a wide range of operations on data including collecting, recording, storing, adapting, retrieving, consulting, using, disclosing and deleting.

This document does not attempt to give detailed guidance to employers or establishments about their overall responsibilities for data protection. It simply highlights aspects of data protection that are relevant to visits. Visit Leaders and establishments must follow their employer's policies about the processing and retention of personal data.

Data protection law does not apply to photographs taken for personal use. It does not prevent, for example, parents or teachers from taking photos during activities and visits. However, you need permission to take photos if you are in a private place: schools are normally regarded as private places.

In some circumstances there may be safeguarding reasons to avoid taking or using photos of children: see OEAP National Guidance document 4.3e "Safeguarding".

Personal Data

Personal data is data that includes information from which an individual can be identified, such as their name or a recognisable photograph. Records that are commonly used for managing visits and which could hold personal data include:

- Parental consent forms;
- Emergency contact details;
- Medical and dietary information;
- Information about individuals' behaviour, attitude, etc.;
- Care plans;
- Photographs in which individuals can be identified;
- Group summary sheets.

You must not process personal data unless you have a legal basis for doing so. Valid legal grounds for using an individual's personal data include:

- They (or their parent if they are under 18) have given their consent, based on the establishment's privacy policy;
- They (or their parent) have contracted to allow their data to be used (the contract must be compliant with the DPA);
- You need to use the data to protect someone's life.

See OEAP National Guidance documents 3.2i "Contracts and Waivers" and 4.3d "Parental Consent and Informing Parents".

Personal data:

- Must be stored securely;
- Must be kept only if there is a clear reason for keeping it;
- Must not be kept for longer than is strictly necessary;
- Must be accurate and up to date.

For further information about the retention of personal data and other records, see "Record Keeping" below.

The law does not prevent establishments from taking on a visit the necessary records, such as parents' contact details and participants' medical information. However, they must be kept secure irrespective of how the data is shared or carried.

Sometimes it is necessary for an establishment to share personal data with another organisation. For example, an activity provider may require medical or other information about participants so that they can take care of their health and safety. The establishment should obtain assurances that the provider is compliant with the DPA – this can be done by checking that it has a privacy policy which explains how participant data is shared, used, stored, secured, and eventually deleted or returned to the establishment.

If ever there is any doubt about whether it is acceptable to share personal data with another organisation, the safeguarding and wellbeing of children must take priority. The law allows personal data to be shared for the protection of life, even if there is no consent.

Images may be taken and used for safety and security (e.g., through CCTV), if this is explained (e.g., in a notice or privacy policy), but they may not be used for other purposes (such as marketing) without explicit consent. Such consent must involve specifically opting-in, and not be part of other terms or conditions.

Record Keeping

Personal data can be retained as long as there is a legal basis for having it (e.g., parental consent), that it is secure and the reasons for keeping it are clearly stated.

There are many reasons for retaining records of visits and outdoor learning experiences, for example:

- To record the range of opportunities that you provide for the young people in your care;
- To record staff experience in leading visits and outdoor learning;
- To demonstrate effective planning and evaluation of visits and outdoor learning;
- To build a history for sharing learning and good practice;
- To inform future visits in order to improve both safeguarding and learning;
- For public interest, research or statistical purposes;
- When there has been an accident or incident that may result in an insurance claim or legal action (see below).

Electronic visit planning systems, which create searchable databases, are particularly useful for record keeping.

Whatever system you use, if the records contain personal data:

- The system itself must be secure;
- Access to the system must be strictly controlled;
- You must have a legal basis for having the data (e.g. parental consent);
- The purposes for keeping the data must be clear and be recorded;
- You must be able to justify how long you keep the data;

- There should be a policy setting standard retention periods wherever possible;
- Consent for the use of personal data (which includes photographs) should be kept for the duration that the data is retained;
- If copies are made (on paper or electronically), e.g., to take on a visit or activity, they must also be kept securely, and deleted when no longer needed;
- The data should be periodically reviewed, and erased or anonymised (e.g., by removing personal data from a visit record) when no longer needed.

Record Keeping Following an Accident/Incident

Whenever there has been an accident or incident on a visit, the Visit Leader must follow their establishment's and employer's reporting procedures, including reporting to HSE if required by the Reporting of Injuries, Diseases and Dangerous Occurrence Regulations (RIDDOR).

Establishments and employers should consider whether the nature of any accident or incident might, in the future, give rise to an insurance claim or a civil claim for damages. Where this is a possibility, or where an incident was reported under RIDDOR, it is advisable to retain sufficient information about the visit and incident to allow the employer to investigate fully and, if necessary, defend their actions:

- Full details of the incident and any related report/witness statements/follow-up actions;
- The plan for the visit (including risk management plan);
- Names of the young people and adults on the visit;
- The programme of activities that took place on the visit;
- Policies current at the time of the visit (e.g., educational visits policy; health and safety policy);
- A copy of the information about the visit sent to parents prior to the visit;
- A copy of the completed parental consent and personal/medical information form(s) for anyone directly involved in the accident/incident.

A reasonable policy, taking into account the Limitation Act 1980, would be to retain such records until a young person reaches age 25, or for 7 years following the incident in the case of an adult. This allows the legal maximum of 3 years for making a personal injury claim from the date a young person becomes 18, or from the date of the incident, or from the date a person knows that the facts of the incident give grounds for a claim, whichever is latest. It also allows an additional 4 years, which can be regarded as a period sufficient for a person to become aware that the facts of the incident give grounds for a claim, if they had not previously known these facts. In certain types of incident (e.g., where the nature of the incident means that it could be many years before latent personal injury becomes apparent) a longer period might be allowed.