WEST LONDON ACTION FOR CHILDREN

WLAC GENERAL DATA PROTECTION & CARDHOLDER DATA SECURITY POLICY

There are three sections to the General Data Protection Policy

1. General introduction to Data Protection
2. Mobile data
3. Cardholder data

The policy forms part of the Induction Pack for all members of Team and for appropriate volunteers and will be signed accordingly.

1. Introduction

West London Action for Children strictly follows and acts in accordance with the UK General Data Protection Regulation (UK GDPR).
In accordance with UK GDPR West London Action for Children aims to comply with the law, prevent harm to individuals (clients, employees, persons affiliated with WLAC), follow good practice, and protect the organisation.
WLAC has taken all measures that it can to ensure compliancy and acknowledges that UK data protection law which includes the UK GDPR and the data protection act 2018 is intended to make the collection and retention of data about a person more transparent and that the organisation is more accountable for the safe keeping of that data.
Data will be held on subjects in four main areas: clients; staff; supporters; and other agencies. Each of these may be subject to different reasons for the data being held, including consent; legitimate interest; and legal necessity. Full details of the new requirements can be found on the Charity Commission website.

In addition to this General Data Protection Policy, there is now a Privacy Policy which is referred to on the website and on communications.

Policy Statement/Guidelines

All data/information collected and filed from clients is to remain strictly private and confidential in order to respect and protect the individual. This applies to text, photographic images, videos, and audio material obtained. The only exception to this rule is when it has been agreed that, as a matter of safeguarding, information pertaining to a client will be shared with another agency. It is obligatory for WLAC to share such information at this time in accordance with the WLAC policy on Child Protection.
Sensitive information must not be disclosed to outside parties without prior discussion with the individual and with the Employer.

All data must be accurate and up to date. When unsure about the criteria of information, it is necessary to be cautious.

Confidential data/information maybe kept securely for a maximum of six years. Access is restricted to only authorised members of the team at West London Action for Children who are obliged to maintain and regard the Confidentiality Policy. In a case where there has been any element of grievance, case notes must be kept for a period of 25 years. All information collected from supporters will be kept confidential. This information will not be passed on to a

third party. As per the UK GDPR, individuals have the right to opt out of receiving publicity from WLAC.

Offences in direct violation of the policy will result in disciplinary action deemed appropriate by the employer. Serious offences can result in legal action.
This policy is reviewed at least every three years and updated if there are any changes in business i.e. any changes in how you accept credit cards, whether it involves equipment or just procedure. The Chief Executive/ Administrator is held accountable for implementing an incident response plan.
General Data Protection Awareness training is given at the induction of all new employees and volunteers. Specific training is given to those who deal with processing card payments.

2. Mobile Data

Mobile devices provide enhanced opportunities and benefits for staff and clients. With these opportunities and benefits comes a corresponding duty to handle the processing of any personal information in accordance with UK GDPR
.
The use of mobile technologies falls in line with general data protection regulation identified above and must be observed. Mobile data protection is no different to data protection relating to IT security, data protection, retention of records, e-mail, acceptable use, and staff disciplinary procedures.

Some practical suggestions to aid compliance are:

- Audit current behaviours and practices to find out how and when mobile devices are being used and the current level of security being applied to mobile devices.
- Where not already implemented, ensure adequate technological measures are put in place to handle security of mobile devices. Encryption is required if data is shared, to adequately protect personal data processed using mobile devices
- Develop and apply an encryption policy to ensure DP compliance. This can be a separate policy or incorporated with current policies but should provide clear practice for staff (and students) to adopt when using mobile devices
- If encryption is necessary, staff will need to be competent in the use of encryption technology. Training will be provided with help on the application of the security measures. Security needs to be user friendly
- Ensure staff awareness of the institution's requirements through training, notices, and regular reminders. All staff should be privacy and security aware in their use of mobile devices
- Have a clear line of responsibility for information handling

Other Legal Considerations
There are other legal obligations to take into account including copyright and licences, e-safety, and accessibility all of which require consideration in relation to the use of mobile technologies.
The JISC Legal website has further information on the law in these areas.