

DATA PROTECTION POLICY

1. Leisure & Culture Dundee (hereinafter referred to as "the Organisation") supports the objectives of the Data Protection Act, 1998 (hereinafter referred to as "the Act") and intends to retain its present policy of maintaining the confidentiality of personal information processed automatically (on computers etc) and held on manual files which are considered to be "relevant filing systems" in terms of the Act.
2. The Organisation expects all Trustees and employees to comply fully with this policy and the Date Protection Principles (Appendix I).
3. The Organisation will hold the minimum personal information necessary to enable it to perform its functions, and the information will be erased once the need to hold it has passed. Every effort will be made to ensure that information is accurate and up-to-date, and that inaccuracies are corrected without unnecessary delay.
4. Personal information is confidential. Automated systems and relevant filing systems will be designed to comply with the Date Protection Principles. Personal information will be disclosed only for registered purposes to:
 - Organisation staff where such information is vital to their work;
 - others as detailed in the Registration;
 - the Court under the direction of a Court Order.
5. It is the responsibility of the Managing Director and Service Managers to ensure compliance with this policy. All systems within the Service Section or Organisation containing information about individuals must be identified, made secure, and notified to the Data Protection Officer for notification purposes. It is the responsibility of all employees to co-operate in this task. Upon discovering that the Organisation's Policy on Data Protection is not being complied with, the Managing Director, after consultation with the Finance Director, shall have full authority to take such immediate steps as considered necessary.
6. The Organisation will provide to any individual who requests it in the proper manner a written copy in clear language of the current information **held about themselves**. The Organisation shall fix a fee for this service which in appropriate circumstances may be waived by the Managing Director. Employees of the Organisation will not be required to pay any such fee when requesting access to information regarding their employment.
7. In cases where the Organisation acts as a bureau providing services to outside organisations, no disclosure will be made without the written consent of the third party except under the direction of a Court Order checked by the Managing Director.
8. All employees of the Organisation must comply with the requirements specified in the Organisation's e-mail/internet **guidelines and should avoid storing Personal Information on lap tops, home PC's etc. If this is unavoidable then the lap tops etc. must be encrypted and staff must ensure the security of such devices at all times.**
9. Disciplinary action may be taken against any Organisation employee for deliberate or reckless breach of any instructions contained in, or following from this Date Protection Policy.

APPENDIX 1

DATA PROTECTION ACT 1998

THE DATA PROTECTION PRINCIPLES

1. Personal data shall be processed, fairly and lawfully and, in particular, shall not be processed unless:
 - at least one of the conditions in ***schedule 2 of the Act*** is met, and
 - in the case of sensitive personal data, at least one of the conditions ***in schedule 3 of the Act*** is also met.
2. Personal data shall be obtained for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data held for any purpose or purposes shall be adequate, relevant and not excessive in relation to that purpose or those purposes.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data held for any purpose or purposes 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 this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
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 protection for the rights and freedoms of data subjects in relation to the processing of personal data.