

## **Data Protection Policy Statement**

Data Protection Act 1998

The Data Protection Act 1998 sets out rules for processing personal information, and it applies to some paper records as well as those held on computer and some automatically processed data, for example, document image processing, audio/video, photographs and CCTV. The Act gives individuals certain rights, and imposes obligations on those who record and use personal information to be open about how information is used and to follow eight data protection principles:

### **Data Protection Principles**

Personal data must be processed following these principles so that data are:

1. processed fairly and lawfully
2. obtained for specified and lawful purposes
3. adequate, relevant and not excessive
4. accurate and, where necessary, kept up-to-date
5. not kept for longer than necessary
6. processed in accordance with the subject's rights
7. kept secure
8. not transferred abroad without adequate protection

All users of personal information, including the Board of Management and the Board of Trustees are obliged to comply with the 1998 Data Protection Act (DPA).

The Museum of Technology is a 'not for profit' charity and thus is exempt from registration requirements for Data Protection with the Information Commissioner's Office.

### **Your rights**

You are entitled to have access to information held about you, except where releasing that information would breach another person's privacy. You also have rights to prevent data processing likely to cause substantial and unwarranted damage and distress, and to prevent processing for direct marketing. If you wish to exercise these rights, you should contact the Museum of Technology and request to speak to the Chairman of the Board of Trustees.

### **Your responsibilities**

Any personal data must be collected, processed and held according to the data protection principles

Data will not be kept for longer than necessary

### **Security**

All reasonable steps should be taken to ensure that personal data is secure, the following steps are suggested:

- Access to computer files should be restricted using privilege levels and passwords.
- Regular password changes should be enforced and the number of attempted logins limited.
- Equipment should be sited in a secure location where access can be restricted - the public should not be able to view terminal screens.
- Terminals should not be left unattended and should be logged-off at the end of a session: "log-off, switch off, lock up".
- Redundant data should be wiped or overwritten.
- Ensure appropriate back-up and storage for data
- Storage media should be locked up after use.
- For large amounts of sensitive data, consider keeping a copy in a fire-proof safe at a separate location.
- Network systems should be considered to be insecure. Data must be kept as secure as possible, using encryption, de-personalisation and password-protection if possible. Consider storing highly sensitive data on stand-alone machines.
- Computer printout containing personal information should be shredded before disposal; it should not be used as scrap paper.
- Review manual files and store securely. Sensitive data should be stored in locked filing cabinets.

### **Review date**

May 2012

### **SIGNATURE**

Chairman of the Board of Trustees

Date of Signature

Approved: 28.4.2009  
Reviewed: 11.3.2010  
Reviewed: 12.5.2011