

## Information Security & Data Protection Policy

### Information Security Provisions

WSUP regards the protection of its information and that of its partners and clients as of vital importance to the continued success of delivering its business plan. As such we will:

- Invest in an IT infrastructure that allows our staff to receive, store and transmit information securely, where hard copies of information are retained we will ensure the appropriate physical security measure are in place and staff are trained and equipped to use them.
- Develop a culture where our staff operate ethically and responsibly in the receiving, storing and transmitting of information.

### Data Protection Provisions

WSUP needs to gather and use certain information about individuals. These can include customers, funders, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact. We recognise our obligations under The Data Protection Act (1998). To that end we will ensure that all personal data collected will:

- Be processed fairly and lawfully
- Be obtained only for specific, lawful purposes
- Be adequate, relevant and not excessive
- Be accurate and kept up to date
- Not be held for any longer than necessary
- Processed in accordance with the rights of data subjects
- Be protected in appropriate ways
- Not be transferred outside the European Economic Area (EEA), unless the recipient in that country or territory also ensures an adequate level of protection

The policy will be reviewed and revised as necessary at regular intervals (at least annually) in consultation with the Risk Committee of Board.

Responsibility for adherence to this policy is delegated by the WSUP Board to the CEO of WSUP.



Neil Jeffery  
Chief Executive, WSUP



Will Day  
Chairman, WSUP