BEAMINSTER PLAYGROUP

INTERNET POLICY

AIM

To outline safe and effective practice in the use of the internet.

PROCEDURES

The Manager is responsible for ensuring the online safety within the Playgroup.

All staff will be made aware of the procedures that must be followed in the event of a potentially unsafe or inappropriate online incident taking place.

All Playgroup ICT will be password protected. Access to sensitive and personal data will be restricted.

All ICT users must 'log-out' if they need to leave the computer unattended. If password security is compromised this must be reported to the Manager.

Internet access will be monitored by the Manager.

Control measures will be implemented to manage internet access and minimise risk, such as a secure broadband service, a secure, filtered and managed internet provider, secure email accounts, regularly monitored and updated virus protection, a secure password system, agreed list of authorised users and effective audit, monitoring and review procedures.

The computer is situated in a highly visible place to ensure children and adults can be closely supervised.

If a child accidentally accesses inappropriate material it must be reported to the Manager immediately. The page should be minimised or hidden, but should not be closed down, to allow an investigation to take place. Safeguarding procedures will be considered and applied if appropriate.

Staff are not permitted to connect personal mobile devices to the Playgroups ICT systems unless with explicit authorisation from the Manager.

All email correspondence is subject to scrutiny and monitoring.

All staff are expected to write online communications in a polite, respectful and non-abusive manner.

If children are allowed to use online technologies they will always be relevant to their age and development.

Staff are not permitted to use the Playgroups computer for personal access to social networking sites.

September 2014