



**DRAFT Version
Work In Progress**

Version 1.0 - Date Effective: 22-23/11/2000
Author: S.J. McWilliam
Change Ver.: 0.0 Change Date: 22/11

POLICY ON DATA SECURITY

1. Policy Statement:

All data lodged with **rECORD** is valuable, not directly in monetary terms, but in both the effort which has been expended by those who have donated the data and the time and resource expended by **rECORD** in the storage and management of said data but also in the potential the data has for education, research and for usage for wildlife and people.

Due to this inherent value, **rECORD** will put in place procedures to ensure, as far as is possibly practical, that all data lodged will be secure from theft, fire, flood, decay, computer failure and data corruption. This will be implemented via back-up procedures, off-site storage agreements, archival of paper records and the development of both building security measures and data access controls.

2. Background to the Policy:

Biodiversity data collected and collated by **rECORD** is a valuable resource for many differing reasons and as such there is a need to protect this data, to ensure its longevity and to prevent its loss or damage through theft, fire, flood, decay, computer failure, corruption or any other form of damage or loss, whether acts of God, disaster, malicious intent or otherwise.

To this end procedures will be put in place to protect the building housing the data from illegal access; weekly data back-ups on non erasable media (i.e. writable CD Rom) will be held within a fire-proof safe within the centre; monthly copies of the back-ups will be produced and will be lodged off-site with disaster recovery partners (e.g. other local record centres/museums with which such reciprocal agreements have been negotiated); paper data will be stored in filing cabinets and will be archived to Liverpool Museum on an agreed cycle (e.g. quarterly); all computer systems will be scanned for viruses at least weekly; hard-drives will be scan-disked on a weekly basis; all work-stations will require a password to enable log-in - each password being applicable to a single individual or group; all software relating to input or output of **rECORD** data will be password protected.

3. Links to other rECORD Policies:

Data Needs (All areas):

These policies provide the frame work within which **rECORD** identifies its users overall needs and which feed in to the process of defining the levels of service.

Building Security:

This policy details the means by unauthorised access to the building in which **rECORD** is housed is prevented.

Controlling Access to Data:

Access to the data holdings of **rECORD** must be controlled and managed in order to ensure that such access is not a means of tampering with and altering the data.

Confidentiality:

This policy defines which types of data are critical and which must remain confidential; these strictures may be imposed for various reasons. The consequences of confidentiality may impact some areas of data security in terms of how it is implemented and who has access to what data.

Data Entry Protocols:

The protocols for data entry must take account of data security requirements in terms of being able to understand what data has been entered/modified/alterd and by whom.

Internet:

As the InterNet operational capabilities of both **rECORD** and the National Biodiversity Network increase so there will be a requirement to ensure that data is secure from attack by malicious hackers or by accidental erase or alteration by non-malicious users.

Satellite Management:

There will be a need to raise data security awareness with satellite users and also to determine what are each individual satellite's security issues. Addressing these issues in terms of physical security and also access security will be more difficult than at **rECOrd** but will need to be explored.

4. Activities Supporting this Policy:

4.1 **rECOrd** will establish a basis upon which all data held is protected and its longevity, viability, continuing validity and non-corrupted nature is maintained.

4.2 The **rECOrd** Building Security policy will be implemented along with all detailed unauthorised access constraints therein noted.

4.3 **rECOrd** will enter into, and complete, negotiations with Liverpool Museum with regard to the placement of all paper-based records (including naturalists' notebooks) in an archive at the Museum. This should include the paper being managed to archival standards.

4.4 **rECOrd** will develop relationships to engender off-site storage of regular back-ups of data on non-erasable computer media (i.e. writable CDs) in order to allow for Disaster Recovery procedures to be employed with at least two, and preferable more, local record centres and/or museums. Deposits of CD copies of the data with these partners will be on a monthly or quarterly basis depending upon the volume of data being added to the **rECOrd** database. Requests will be made within the agreements for **rECOrd** data to be stored at the recipients site in a fire-proof data safe. Similar services will be offered to recipient partners for **rECOrd** to act as off-site storage for their own data back-ups. The potential will be explored, with at least one of the off-site storage partners, to provide a minimal processing service for **rECOrd** during their normal down-time periods (e.g. over-night) on their own machines in the event of a disaster at **rECOrd** which negates all processing capability (e.g. following a fire which destroys building and computers).

4.5 Back-ups of all **rECOrd** databases will be undertaken onto non-erasable computer media (i.e. CD-Rom) and stored in an on-site fire proof safe on a weekly basis.

4.6 Back-ups of all **rECOrd** databases will be undertaken to the network server hard-drive each and every evening and duplicated under another directory.

4.7 The **rECOrd** network server will operate within a physically locked area.

4.8 All **rECOrd** computer systems will be virus scanned over-night on one evening per operational week.

4.9 All **rECOrd** computer hard-disks will be scan-disked, over-night, on one evening per operational week.

4.10 All **rECOrd** computer systems, whether networked or stand-alone, will be password protected with that password being changed, by the Manager, on a regular basis - maximum period between password changes being 6 months.

4.11 All work-stations connected to the **rECOrd** network, or stand-alone computers, will be required to have a log-on password - further work will be needed to determine whether it will be feasible to have individual log-on identities created.

4.12 All software relating to **rECOrd** databases (the database itself, and any ancillary data-entry or enquiry software) will be password protected.

4.13 The main **rECOrd** biodiversity information database (Recorder-2000) will have security levels set to ensure that data can not be deleted or amended by personnel other than bona fide and specific staff members.