National Biodiversity Network

The National Biodiversity Network Trust

Data Exchange Principles

A framework of principles for the exchange of wildlife information within the National Biodiversity Network

Version 3.1 – Working Document

October 2001

Version Control

VERSION	TITLE	DATE	DESCRIPTION
V1	Pre-consultation Draft	04.02.00	National Biodiversity Network Trust consultation
V2	Consultation Draft	04.03.00	Launched at National Federation for Biological Recording (NFBR). Released for wide consultation.
V3	Trial Version	30.07.01	This document is a working document, which may be revised in the light of practical experience. The principles are available to be used by anyone to inform the development of policy for data delivery.
V3.1	FInal Version	10.10.01	Same as V3 but edited for errors.

Contents

N.B.

This working document sets out the Seven Data Exchange Principles of the National Biodiversity Network. Each section of the document has been written to stand alone, enabling users to access and download specific sections from the Access Project page of the Networks website (www.nbn.org.uk).

Introduction to the Data Exchange Principles and their purpose

The Data Exchange Principles document sets out seven principles for the exchange of wildlife data.

Through work to develop the National Biodiversity Network, the National Biodiversity Network Trust has encountered significant barriers to the exchange of wildlife information in the UK. In consultation with data owners, managers and users, the Trust has identified a demand for guidance to help overcome these barriers.

The seven data exchange principles represent the Trusts first attempt to provide such guidance. This document is a working document, which may be revised in the light of practical experience. The principles are intended for use by anyone to inform access negotiations for individual datasets and/or the development of organisational policy for data delivery. Although the principles do not represent an approved standard in data access terms, the Trust is hopeful that they will help more organisations to exchange wildlife information.

Practical trial of the Data Exchange Principles

The National Biodiversity Network Trust has produced seven data exchange principles. The principles are intended to support organisations and individuals wishing to exchange wildlife information. The Trust would like to test whether the principles work practically, and invite any organisation to examine them.

Oliver Grafton, the Access Project Officer for the Trust, is the primary contact for this work. Oliver is happy to advise on the use of the principles and would be grateful to receive any advice on whether the principles are useful. Examples of access agreements and principles currently in use would help the Trust to build experience and extract best practice.

Oliver can be contacted by…

Telephone: 01733 455411

Email: o.grafton@nbn.org.uk

Address: NBN Trust Projects Officer
English Nature
Northminster House
Northminster
Peterborough
PE1 1UA

The Seven Data Exchange Principles

Principle One

Biodiversity data should be easily accessible to enable their use for not-for-profit decision-making, education, research and other public-benefit purposes.

Principle Two

Making biodiversity data available should reduce the risk of damage to the environment. If it is likely to have the opposite effect, availability may need to be controlled.

Principle Three

When biodiversity data are supplied, accompanying information (meta-data) on its ownership, methods and scale of collection and limitations of interpretation, should be provided. In general there should be sufficient metadata to allow biodiversity data users to assess the scope and potential users of their information holdings.

Principle Four

A clear transfer of authority should be made when a biodiversity data resource is put together, to allow biodiversity data managers to act on behalf of the biodiversity data owners.

Principle Five

Managers of biodiversity data should make their framework of terms and conditions publicly available, allowing biodiversity data owners to have confidence that control will be exercised in the management and use of their data.

Principle Six

Personal data must be managed in accordance with the principles of the Data Protection Act 1998 and/or any subsequent legal provisions.

Principle Seven

a)

Managers and funders of biodiversity data should make basic facts freely available (except for handling charges if needed) for not-for-profit decision-making, education, research and other public-benefit purposes.

b)

Biodiversity data suppliers should try to arrange resourcing of information provision so that charges for not-for-profit uses are minimal and charges for commercial uses are realistic but do not prevent the use of biodiversity data.

c)

Biodiversity data users should expect to contribute to sustaining the provision of biodiversity data through contributing either in kind or financially to the collection, collation and management of biodiversity data, or at the point of use.

The Data Exchange Principles, rationale and application

This section of the document provides the reasoning behind each of the seven principles. Statements of rationale attempt to provide the justification for the inclusion of each principle. Some guidance for the practical application of each principle is also provided.

The practical application of the principles may not always be clear. Much of the commitment and work required to comply with the principles will require some level of experimentation and testing of new approaches.

More detailed guidance on how to overcome the more contentious and uncertain issues surrounding access to wildlife data is provided in the associated annexes of the document. The guidance and advice provided in the annexes represents the National Biodiversity Network Trusts best interpretation of the issues as they currently stand. The scope and detail of this guidance and advice is likely to expand and mature as the development of the Network continues.

Principle One

Biodiversity data should be easily accessible to enable their use for not-for-profit decision-making, education, research and other public-benefit purposes.

Rationale

This is the basic overarching principle upon which the National Biodiversity Network is founded. It is based on the understanding that, for *wise choices to be made about the environment, the many viewpoints involved should use information about the environment.*

It is assumed that the majority of organisations and individuals likely to participate in the Network will be interested in promoting the availability and use of biodiversity data rather than private gain from its sale. This will allow greater use of wildlife information in more appropriately guiding the activities of UK society, safeguarding the interest of the environment. In this way communities will gain in many ways from greater understanding and protection of the environment in which they live. This constitutes public-benefit.

The principle reflects the view that *informed decisions are better than uninformed ones*. Given this, whilst respecting and acknowledging the rights of owners of biodiversity data, the viewpoint has been taken that if such biodiversity data are to be of practical benefit, they must be made more available. It is acknowledged that there are some problems with this approach, but none of these are insurmountable. In the long term, the benefits of making biodiversity data widely available will be great. What these benefits are, and which are most important, will depend upon the viewpoint and remit of individual organisations.

Ideally, biodiversity data from many different sources should be readily available. Given this, organisations and individuals will be able to balance different interests when reaching a decision (e.g. in a development case), taking into account their different remits. In effect, this is a move towards enabling sustainable decision-making. A network of biodiversity data holdings will set local biodiversity data in a broader context, allowing for better informed decision-making. Improved communications should lead to better knowledge of the existence of biodiversity data, which in turn should help reduce duplication of effort for biodiversity data collection.

Although it is true that a better educated public will ultimately result in better decision making, the main reason for including '…education, research and other public-benefit purposes.' in the wording of the principle is to recognise their intrinsic value and encourage the diversity of uses to which biodiversity data can be put.

Application

Many differently constituted organisations should be able to subscribe to the concept embodied by this principle. Indeed, as a result of the Environmental Information Regulations (EIR) or providing evidence for Public Inquiries, many already have to. The EIR are a statutory instrument that imposes a duty upon public bodies to provide information to anyone who asks for it. Whilst a request can be refused on a number of grounds, and a charge can be levied, there is a clear presumption in favour of release. Those making a request do not have to prove an interest. However, if sensitive data are requested it is not unreasonable for the body or individual holding the data to clarify the request to ensure that they do not contravene any of the restrictions on the release of data. In this case, a decision making process to determine what level of detail of information to release to whom, and for what purpose, can be applied. More information on the EIR is provided in Annex 2.

Some organisations may not have the resources or the remit to promote access for all of the purposes suggested in the principle. However, improving the management of biodiversity data

for its primary purpose will normally mean that the extra cost of providing it for other purposes is small. Similarly, although using biodiversity data more efficiently is likely to require changes in working practices by both individuals and organisations, these changes should be viewed positively - as an opportunity to work better.

Some concern has been expressed that allowing the use of biodiversity data by anyone means that those with a commercial interest will be able to exploit - for example - the voluntary sector. Whilst this is addressed in part by the application of principles 3, 4, 5 and 7, it is important to recognise that all participants in environmental decision-making should have an equal opportunity to find and use the same information. *The National Biodiversity Network will not work in practice if biodiversity data owners are over-restrictive about either who can use biodiversity data or what they can use biodiversity data for.* This could mean that organisations working to these principles may not be able to accept records if caveats are placed on their use.

Principle Two

Making biodiversity data available should reduce the risk of damage to the environment. If it is likely to have the opposite effect, availability may need to be controlled.

Rationale

There are risks inherent in making biodiversity data available. These range from; the misuse of biodiversity data; exposure of the locations of rare species; landowners not giving permission for survey work because they are not happy for the biodiversity data to be made widely available; and volunteers not submitting biodiversity data because they don't trust the control over its use. These risks can all be managed, providing a proactive approach is taken.

It is accepted that individual recorders may have concerns about how confidentiality will be assessed and managed. Internet technology enables secure access mechanisms (password based) to be implemented, and a number of levels of security are feasible. The concerns of landowners (whose permission is necessary to gain access to land for survey) can at least in part be allayed by ensuring that they are aware of the results of any survey.

Much of the biodiversity data collection which is carried out, either by volunteers (in the best tradition of such activity in the UK) or by professionals, is seen by those collectors as contributing to the conservation of habitats and species. The aims and objectives of conservation can only be achieved if biodiversity data is made available for use in decision-making. From a conservation perspective, what is needed is a cost-effective mechanism that makes the best possible contribution through applying science-based knowledge to underpin wildlife conservation.

It is widely recognised that some biodiversity data, if released into the wrong hands, could lead to damage to the natural environment. The example often quoted is that of nesting locations of rare birds of prey. However, the assessment of what is sensitive is in many cases highly subjective. In addition, the attention given to exceptional cases tends to overshadow the potential benefit in terms of damage prevention arising from making such biodiversity data accessible. Understanding the probability and impact of risks allows them to be managed. *There must be a presumption in favour of allowing access to biodiversity data to ensure that availability is restricted only when it is truly necessary. Often the perceived level of risk can be reduced with improved trust between individuals.*

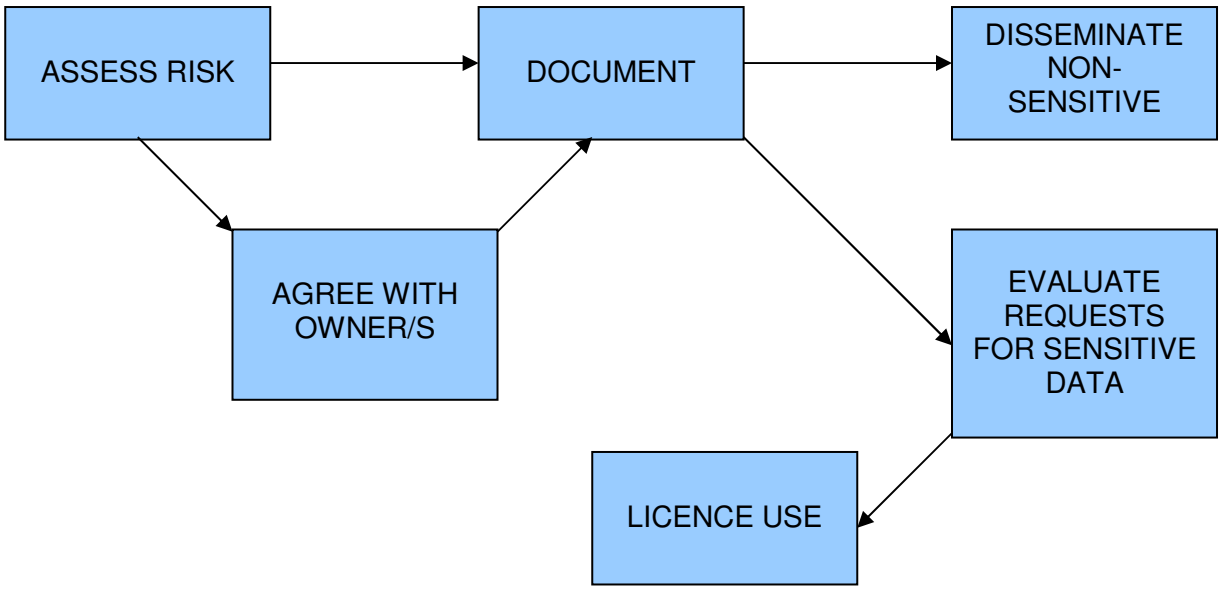
Application

To apply this principle it will be necessary to work out for any given biodiversity dataset which bits of it might be sensitive and which are not. Annex 1 of the Data Exchange Principles document provides some basic guidance for the management of sensitive wildlife data. *Sensitivity or risk of damage to the environment should be assessed according to defined criteria.* Anyone building a biodiversity data resource from multiple contributions will need to agree the criteria with their contributors. Any biodiversity data product should meet the needs of its users (i.e. be fit for purpose) while protecting 'sensitive' biodiversity. Having established how to distinguish between sensitive and non-sensitive biodiversity data, the latter can be made accessible immediately, whilst the sensitive biodiversity data should be made available only if the proposed use or user can be assessed and approved. As an example of the actual (rather than perceived) level of risk, it is perhaps worth mentioning that despite receiving over a hundred biodiversity data requests each year, Hampshire County Council have only had to refuse one such request (for locations of rare orchids) in ten years.

A process for determining risk and deciding when to release potentially sensitive biodiversity data is shown below in Figure 1. The objective of this process is to develop and document sensitive data management agreements. This provides an opportunity to define the criteria used to assess the risk of environmental damage occurring if data is made available. These agreements will help both the owners and managers of wildlife data gain a better understanding of how to manage sensitive data.

Figure 1.

Flow Model for handling sensitive data



Principle Three

When biodiversity data are supplied, accompanying information (meta-data) on its ownership, methods and scale of collection and limitations of interpretation, should be provided. In general there should be sufficient metadata to allow biodiversity data users to assess the scope and potential users of their information holdings.

Rationale

Much concern tends to be expressed about assuring the quality of observations and their validation. This can be a (largely unnecessary) barrier both to making biodiversity data available and to their use. The problem can be addressed by making more documentation on biodiversity data available. Thus biodiversity data should not be provided just on their own, but with accompanying meta-data setting out the methods used for their collection, the statistical limits of interpretation, how the data is held and to whom the data belongs.

Meta-data make the appropriate use of wildlife data possible by providing context, facilitating a greater understanding of the limits within which a dataset can be applied. Meta-data can also record the extent to which the data has been checked, allowing the dissemination of some biodiversity data before all checking procedures have been completed (through version control). A single survey is only a snapshot in time. Multiple surveys build a picture of natural heritage changes and trends and are of more value for many purposes. Meta-data allows users to understand how and when biodiversity data have been collected. In short meta-data can be used to clearly inform a data manager or user as to how the information was obtained and how it should be used. This has close ties to the Data Protection Act, addressed under Principle Six and in Annex 2 of the Data Exchange Principles document.

Biodiversity data quality is not an absolute measure: it depends on the purpose for which the biodiversity data are to be used. Biodiversity data may be of high quality for one purpose but of very low quality for another. For example, a survey to determine butterfly population size could cope with much less rigorous identification quality than a taxonomic or distribution study. The latter might require a large number of very carefully checked observations to validate both the species determination and the location, but these observations would be of little use in estimating population size unless part of a sampling regime. Alternatively, an accurately determined species observation might be of little use in site management because it had a very imprecise geographical reference.

Once biodiversity data are broadly accessible it will be possible for many organisations and individuals to create their own interpretations of biodiversity data (which may challenge those produced by the collector(s) of the biodiversity data). Under this view of the world the skill of organisations in creating interpretations of biodiversity data (thereby creating added value) will form their competitive edge. In effect organisations will control their interpretation rather than the biodiversity data upon which they are based.

Application

Meta-data are essentially descriptions of the biodiversity data itself and how it was obtained. An important benefit of the National Biodiversity Network is that it should encourage meta-data to be produced. Metadata will probably be as valuable in the long run to those organisations currently holding the biodiversity data, as they will to the wider community. It will be important to have clear standardisation, whilst recognising that there are always practical problems with complex datasets in fitting the meta-data into standardised schemes. Where a dataset is drawn from a variety of sources it will be important to have meta-data that refer to the set as a whole, rather than simply to have meta-data for each of the component datasets making up the whole. This is particularly important in situations where the chain between the person making the

original observation and those making interpretations is a long one. It is also important that the meta-data makes it clear where biodiversity data are absent, that is to say, distinguishing between truly negative records and a lack of biodiversity data.

Standards for meta-data exist and a variety of tools are available to help people compile meta-data for their biodiversity datasets. It is important that users take responsibility for any interpretations of the biodiversity data that arise from how they have used them. This can be achieved through the use of disclaimers when providing biodiversity data and additionally, by making a condition of use (through a licence or other legal agreement), that the supplier does not accept any liability for how the biodiversity data may be used or interpreted.

The Network already has in place some of the features needed for people to provide access to biodiversity data with accompanying meta-data: The Network has an internet-based meta-data catalogue of biodiversity datasets; meta-data are part of the biodiversity data exchange format; and *Recorder 2000* allows meta-data to be compiled at the time of biodiversity data collection.

Early availability of biodiversity data is generally beneficial, especially where interpretation is straightforward. Exceptionally, availability may need to wait until context meta-data are available, while a method of analysing biodiversity data is being developed, or until a large enough sample has been collected to permit valid interpretation.

It is obvious that some species and habitats are a lot more difficult to recognise than others, and some survey methodologies are a lot harder to use than others. Using appropriate survey methods for the quality of biodiversity data required, understanding the competence of recorders, and ranking the species or habitats that need to be verified in particular ways, are all ways to increase confidence in the quality of observations and decrease the amount of validation necessary to manageable levels.

When biodiversity data are made available there is potential for them to be misused. This is a fact of life and occurs with all other forms of data in the public domain. However, supplying good meta-data can reduce this risk. A clear common understanding of the conditions under which biodiversity data are made available (e.g. by licence agreement) should also reduce the risk of misuse.

Principle Four

A clear transfer of authority should be made when a biodiversity data resource is put together, to allow biodiversity data managers to act on behalf of the biodiversity data owners.

Rationale

There are serious legal issues that impose constraints on the way that the National Biodiversity Network is able to operate. The Environmental Information Regulations and the Freedom of Information legislation both advocate and provide for (within limits) release of biodiversity data and information. These are balanced by the requirements of the laws of confidentiality, copyright and data protection, which provide for withholding information or delivering 'property rights' over the same data and information. Organisations cannot be expected to work in a way that will subject them to legal penalties, so these legal constraints cannot be ignored. Solutions that deliver what is needed within the legal constraints must be found. Some of the relevant areas of the law are not clear and it can be difficult to decide where the balance lies. There is also a real issue of technological advances running ahead of the law.

During the collection of biodiversity data, work is undertaken by a chain of individuals and organisations. Copyright will exist in each of the individual pieces of work. The copyright of the separate pieces may potentially be different. Many biodiversity data resources are based on collations of original observations, which might have been made by thousands of people. If each person had to be asked each time for permission to use their copyright material, a substantial proportion of biodiversity data would effectively be inaccessible. The solution is for biodiversity data managers who are providing access to multiple biodiversity datasets, or to biodiversity datasets based on any individual contributions, to agree with the holders of copyrights to act on their behalf. It is important to remember that agreements are no substitute for trust between the individuals involved. However, formally approved agreements are likely to be beneficial (so long as they are written in plain English). A summary of what copyright is and how it applies to biodiversity data is provided in Annex 2 of the Data Exchange Principles document.

During the process of creating biodiversity data products, for example summaries or interpretations of raw biodiversity data, value is added in various stages to the raw data, potentially by different organisations or individuals. It is important to understand who owns the rights to which parts, as this controls how the biodiversity data may be used. An audit trail of who owns the copyright to which biodiversity data is therefore essential.

The JNCC[1] and the country conservation agencies have sought legal advice on the implementation of the environmental information regulations and their interaction with copyright and data protection. A summary of this work is provided in Annex 2 of the Data Exchange Principles document. For example, advice was sought to help devise agreements for the transfer of authority to use information collected by volunteers. Unfortunately, the wording of the documents created was so legalistic that it threatened to put off many of those who might be asked to sign them. Despite explaining the problems caused by such documents, the lawyers were not able to draft an agreement in the right spirit and in plain English. It is understood that other organisations have had similar experiences when they have sought legal advice on these issues.

Based on this experience and the recognition that there is very little relevant case law, JNCC have come to the conclusion that all we can try to do is be as reasonable and clear as possible. Some

1 Joint Nature Conservation Committee

organisations may feel that this is not good enough, but it boils down to a balance between the (very low) probability of legal action being taken and the risk and costs of what might happen if such action did take place.

Application

The key point in implementing access to biodiversity data is that *providing access to other peoples' biodiversity data can only be done on the basis of trust.* Licences are legal agreements which can help clarify the parties' shared understanding, but they can also be very inflexible and may frighten off some biodiversity data providers if the documents used are perceived to be worded in an obscure manner. Licences could thus effectively prevent rather than facilitate use of biodiversity data. Having stated this, the most practical way to implement this principle will be through the preparation and use of a series of biodiversity data agreements between biodiversity data providers and users. *Biodiversity data access agreements* need not be viewed as measures to limit access to biodiversity data. Rather they *are measures to build trust and fair dealing between the providers and users of biodiversity data.* An important aspect of implementing such agreements in practice is that *biodiversity data should be accessed only through the dataset custodian, rather than through any secondary source.*

Licensing will be difficult to introduce unless there is a common understanding of why it is necessary. These principles should help to foster a common approach, allowing organisations to create straightforward policies and operational procedures. For instance, the application of Principle 5 in itself goes some way to achieving implementation of Principle 4. Managers of biodiversity data should make sure that all licences for use require users to acknowledge the original copyright holders; this will ensure appropriate recognition of the efforts of individuals.

It is likely that there will remain (at least initially) situations in which it will be necessary to seek the permission of the originators of biodiversity data to release information. However, forward planning and implementation of measures now should aim to minimise this in the future to avoid a crippling administrative burden.

Principle Five

Managers of biodiversity data should make their framework of terms and conditions publicly available, allowing biodiversity data owners to have confidence that control will be exercised in the management and use of their data.

Rationale

This principle addresses issues about the control of biodiversity data, such as recordings provided by volunteers to a Local Record Centre (LRC) or to a national recording scheme and society.

An understanding of the processes used by managers of biodiversity data to validate new biodiversity data and to manage the release of sensitive biodiversity data should reassure biodiversity data owners that controls exist. Intellectual property rights provide the legal basis for the control of biodiversity data. The right to exploit a monopoly, which forms the basis of intellectual property rights law, is given because a resource (in this case biodiversity data) is made available. Biodiversity data licences can be used to impose contractual conditions. Copyright and contract law allow these to be enforced. A brief summary of copyright law is provided as part of Annex 2 of the Data Exchange Principles document. While the electronic publication of biodiversity data does lead to some loss of control, the same is also true of conventional publication, for example in a book.

Application

The fieldworkers who originally collect biodiversity data (most of whom are volunteers) may have concerns about their biodiversity data being misused or falling into the wrong hands. It is important that the National Biodiversity Network is able to demonstrate good control over access to biodiversity data. Organisations working to these principles need to work hard to give feedback to volunteer fieldworkers and to build their trust. The organisations responsible for collating biodiversity data and putting them into the NBN need similar reassurances.

Use of biodiversity data without the permission of the owner is a breach of copyright law. There has been a great deal of uncertainty as to how to manage biodiversity datasets collated before the transfer of authority was included in the collation process. Pragmatically the way to deal with this is to *show that 'reasonable' steps have been taken to obtain authorisation for use from originators of biodiversity data.* Documentation of the process undertaken, and, from now on, ensuring that the biodiversity data owner(s) have given permission for their biodiversity data to be used in particular ways, safeguards both those who collect and those who use biodiversity data.

For small numbers of casual records it may be sufficient to add a note on the collection form telling the person completing it how the biodiversity data will be used; submitting the form then gives implicit permission for the biodiversity data to be used in that way. For larger collections of biodiversity data, advertising that a collation is being created, making it clear how the biodiversity data manager intends to use the resource and allowing time for people to express an interest or withdraw their biodiversity data, would probably be wise. Where a large quantity of biodiversity data originate from a single source, a one-off agreement may be sufficient. This should include the provision of appropriate feedback - illustrating that the biodiversity data supplied represent a valued resource.

Some suggestions of things to include in a set of terms and conditions are listed below:

- an assurance that the procedures for documenting biodiversity datasets will be made available by the biodiversity data manager;
- a statement of policy on the sorts of uses the biodiversity data manager would like to promote for the biodiversity data;
- the criteria for evaluating sensitive biodiversity data and a procedure for agreeing with biodiversity data owners how they apply;
- the procedures for evaluating requests for sensitive biodiversity data;
- the working practices in place to physically safeguard the biodiversity data;
- an explanation of the circumstances under which the biodiversity data manager may charge for providing access services and what happens to any income.

It should be adequate in many cases simply to release biodiversity data with a copyright statement, thereby creating an implied agreement. It is important for all parties to be both pragmatic and reasonable when implementing a legal agreement.

Principle Six

Personal data must be managed in accordance with the principles of the Data Protection Act 1998 and/or any subsequent legal provisions.

Rationale

The Data Protection Act 1998 provides the legislative basis for registering the use and dissemination of personal data. It covers all use of personal data, regardless of whether the user needs to be registered under the Act or not. An important change between the previous (1984) and replacement legislation is that, whereas under the 1984 Act the only personal data that were covered were those stored electronically, under the 1998 Act this has been extended to include structured manual filing systems. The Act is based on a number of principles that provide a very useful framework for the management of biodiversity data. A brief summary of data protection is provided in Annex 2 of the Data Exchange Principles document.

Data about people and biodiversity data generally need to be managed alongside each other for three main purposes:

1. to record who the copyright holder is so that they can be properly acknowledged when the personal data are used;
2. for the purposes of administering recording schemes;
3. to provide contact data for use when others need to confirm details of the observation.

Application

While personal data may be important in validating biodiversity data, once that has been done, *personal data need only be exchanged where it will significantly improve the interpretation of biodiversity data* (e.g. for critical taxa where the skill of the observer is a significant factor in the accuracy of the records). If people are happy to be acknowledged as the original observers then of course there is no problem in disseminating that information.

If the provision of personal data does not assist interpretation of the biodiversity data, and the original contributors do not want to be individually acknowledged, then normal working practice should be not to disclose personal data when biodiversity data are made available. If personal data are subsequently needed as context to the observations in particular circumstances, for example when biodiversity data have been challenged in a Public Inquiry, the personal data should be disclosed only if permission is subsequently obtained from the originator.

The exact data protection notification that organisations will need to make will depend upon their remit and activities. However, a biodiversity manager can provide data as outlined in the three scenarios above under the Data Protection Act. Under the 1998 Act, a data manager requires permission from all data contributors for any intended use of personal data associated with biodiversity data. It is illegal for biodiversity data managers to hold personal details about fieldworkers if they object to them being held. In this case a judgement will have to be made as to whether the personal data are integral to the quality of the record. If they are, the records will have to be refused, as they will be substantially incomplete. The administrative burden that formal management of personal data entails may cause some concern, but none of the three uses is particularly controversial, and it is therefore expected that only a small minority of potential fieldworkers will be put off by the increased formality required.

Principle Seven

A

Managers and funders of biodiversity data should make basic facts freely available (except for handling charges if needed) for not-for-profit decision-making, education, research and other public-benefit purposes.

B

Biodiversity data suppliers should try to arrange resourcing of information provision so that charges for not-for-profit uses are minimal and charges for commercial uses are realistic but do not prevent the use of biodiversity data.

C

Biodiversity data users should expect to contribute to sustaining the provision of biodiversity data through contributing either in kind or financially to the collection, collation and management of biodiversity data, or at the point of use.

Rationale

Charges (including the level at which they are set, what they cover, and who benefits from them) are probably the most contentious part of this framework of principles. There is no intention that this charging principle should undermine the funding basis of local records centres, national schemes and societies or any other biodiversity data provider.

Restricting the availability of biodiversity data is seen by some biodiversity data holders as important in order to protect their business, placing them in a monopoly position. However, managing and making biodiversity data available is expensive and business models are changing. Once this is recognised the question that has to be answered is: who pays and for what? The challenge for the National Biodiversity Network is to recognise and acknowledge the risks to existing biodiversity data suppliers and to help to manage transitions. While suppliers should not expect to be artificially supported, it is in no-one's interest to create gaps by forcing existing biodiversity data suppliers out of business.

It is important that in the development of the wider use of biodiversity data, that biodiversity data providers and users avoid attaching monetary value to biodiversity data directly. This is for three reasons: firstly, this is a dangerous and slippery slope when the majority of biodiversity data collection is by volunteers, whose effort and goodwill are paramount to making the system work; secondly, this is counter to the internet trend of making more information more easily available; and thirdly, charging is mostly about services not data anyway.

This principle has been split into three parts to clarify the interests of the different players in biodiversity data provision and use. The value of biodiversity data lies in its appropriate use. It should be expected that some summary or overview level of access to information will be available free to anyone, to act as a 'shop window'. Individuals and organisations will feel more or less comfortable with allowing access to greater or lesser amounts of detail according to how open they feel able to be (which will depend partly on their status - public bodies are likely to be more open, owing to the Freedom of Information legislation, than private bodies or charities, which may feel they have to protect their assets). The more widely it is known that biodiversity data exist, the more likely it becomes that new revenue sources will be discovered.

A clear distinction has been made between commercial and non-commercial uses of biodiversity data. It is expected that commercial users will be more likely to want to pay at point of use than contribute to core costs for biodiversity data collection and management. The intention of proposing that charges 'do not prevent the use of biodiversity data' is to avoid *excessive* charging, such as attempts to recover the full cost of biodiversity data collection from each user.

Given that the resources which may become available from pay-per-use are less certain (i.e. it is difficult to predict the amount of use that an organisation may make of a biodiversity data resource unless they enter into some sort of agreement), organisations that pay in this manner should expect to be charged at a higher rate than those that are willing to enter into a service-type agreement with biodiversity data providers. It is important that the main funders of a biodiversity data provision service do not feel disadvantaged by the access arrangements for other users - another reason for higher charges for those who contribute on a 'pay-per-use' basis. However, some funders may wish to subsidise other uses, for example, public funders may wish to discount the costs of provision of biodiversity data to the general public.

One of the major benefits of improved access to biodiversity data is the ability to influence the decisions of others. Some biodiversity data owners may be concerned that greater availability of biodiversity data will make it easier for others to increase their influence at little cost to themselves. However, since biodiversity data are unlikely to be collected except for a good reason, *wider use of those biodiversity data should be regarded as an added benefit.* In addition, if the biodiversity data have been collected with public funds then the principles of open government and wise use of public resources demand that the biodiversity data be made widely available. Indeed, the Environmental Information Regulations (EIR) *require* public bodies to make information available to whoever asks for it. It is very important that all requests for biodiversity data are handled by the agreed biodiversity data custodian to ensure consistency in biodiversity data and information, access and charging, and to provide the ability to log the nature of the requests received, which can provide important market research type information.

There is very little evidence of significant income generation from supplying biodiversity data unless a) a near monopoly exists and b) there is great demand for the biodiversity data. Neither of these is likely to apply to the bulk of biodiversity data. It is a common misconception that local records centres and other biodiversity data managers 'make a profit' from providing access to biodiversity data. This is quite simply not true. Whilst the demand for biodiversity data is increasing exponentially, available evidence suggests that the resources available from information provision are likely to be considerably less than the costs of making biodiversity data available. This is because it is very expensive to collect, manage and disseminate biodiversity data. However, the income that *is* generated can be used to offset the costs of running a recording scheme, to offset the cost of supplying biodiversity data to those who, for public-benefit reasons, may only be asked to pay at nominal rates, or to enable work that would otherwise not be undertaken.

Application

For those organisations whose remit is the supply or procurement of biodiversity data, it should be noted that the trend for increased provision of biodiversity data is likely to both continue and increase. The National Biodiversity Network should therefore be seen not as a threat, but as an opportunity to develop and access high quality biodiversity data services, using biodiversity data managed both directly by an organisation and indirectly by others. Within a partnership network such as the National Biodiversity Network, creating unreasonable or inconsistent cost barriers to the use of biodiversity data is more likely to hinder than help biodiversity data exchange.

Most biodiversity data-rich organisations add value to the biodiversity data through some sort of interpretation of those data. The collection and management of biodiversity data are thus a means to an end rather than the end itself. The costs of collecting and managing such biodiversity data certainly have to be covered; developing a broad enough funding base that supports this work in a sustainable fashion - perhaps as part of a service agreement - is one of the changes and challenges that biodiversity data managers face. Ideally, finance for the provision of information products should be available from within core or programme funding rather than expecting external users to pay. In practice this ideal may be difficult to achieve. As the trend of making

information more available continues biodiversity data managers will have to ensure that their biodiversity data are organised in ways which make it efficient to enter, validate and retrieve data. It should be noted that *poor data management is not an excuse for high charges.*

There are a number of issues around the subject of service agreements; for example what costs should be included, what the agreement should cover and how long it should run. Nevertheless, they provide a means by which the costs of biodiversity data management can be shared between organisations, with the benefits of access to a wider pool of information than would otherwise be available. They are therefore an attractive proposition to many organisations. They also offer a means by which the funding base of a biodiversity data provider can be broadened, and for stakeholders to support an on-going biodiversity data collection, collation and management process.

Biodiversity data services are not cost-free. Doing anything costs money, as in any other sphere of life, and this includes re-supplying of donated biodiversity data to their originator. However, using at least part of any revenue from the provision of biodiversity data to create a fund to pay for requests for help from biodiversity data suppliers is likely to be a good way of keeping such suppliers happy. *The challenge for biodiversity data managers is to create a charging regime under which providers are willing to supply biodiversity data and users are willing to pay for the services provided.*

For commercial uses of biodiversity data it is likely that negotiations on charges will be on a case-by-case basis. *For non-commercial applications,* charges should not be set with the aim of recovering data collection or management costs; rather, *biodiversity data managers should aim to minimise or discount the costs of providing biodiversity data, or even waive them.* This applies particularly to setting charges for those who provided the biodiversity data in the first place, especially if they did so in a voluntary capacity. For both commercial and non-commercial applications, *consistency and transparency in the Application of any charges made is very important.*

The UK Biodiversity Steering Groups report recommended, 'collect once, use many times'. This can best be done by keeping charges low, reducing the incentive for users to re-create the biodiversity data resource. The challenge of implementing a charging policy in the electronic information era is that the greatest part of the costs involved are in capturing, verifying and managing biodiversity data rather than in its dissemination. Views on how this challenge can be met are invited.

Annex 1 Managing Sensitive Wildlife Data

Background

The National Biodiversity Network hopes to provide a transparent and safe environment within which a diverse range of organisations can readily and confidently exchange their information. To achieve this the National Biodiversity Network Trust hopes to help overcome the many barriers currently preventing the ready exchange of wildlife information in the UK. Reduced data exchange due to concerns over the sensitivity of wildlife information is one of these barriers.

Evaluating Requests for Information

The decision whether to release non-sensitive biodiversity data is relatively easy. All that is required is to decide whether a fee should be charged (for example to cover the work involved in finding and processing information), as discussed under Principle 7.

Only if the information is sensitive for some reason is further information required before a judgement can be made about whether to release biodiversity data, or a subset thereof.

Types of use of environmental information

Assigning a request for information to one of the following categories may help decide whether, how much, or what sort of biodiversity data to release.

Will the release of biodiversity data:

- support conservation action and priority setting?
- further scientific understanding?
- promote public understanding and enjoyment of the environment?
- build the capacity of voluntary groups to collect valuable environmental information?
- allow the provision of sound professional advice?

What extra information might be needed?

- Who are the proposed users of the information?
- To what use is it going to be put?
- Have appropriate referees been named?
- Where will the information be used and what measures will be in place to prevent its accidental disclosure?
- For how long will the information be used?

Once this information has been provided the criteria in Figure 2 below can be applied; release of sensitive biodiversity data could then be by licence, with a balance struck between the needs of those requesting biodiversity data, the sensitivity of the organisms to which the biodiversity data refer, and the use(s) to which the biodiversity data are to be put.

Basic questions that should be answered by the biodiversity data manager or data owner:

- Do we own this information?
- If the information contains personal data, are we registered for its release to those making the request?
- Do the benefits of release outweigh the risks?
- Can I defend my action as reasonable?

If the answer to all these questions is '*Yes*' then the biodiversity data should be released.

Identifying 'sensitive' biodiversity data

A presumption of access to biodiversity data should be made to ensure that access to biodiversity data is restricted only when it is truly necessary. Generally, increased availability of biodiversity data is likely to decrease the risk of damage to the environment. Exceptionally, availability may

significantly increase this risk. There are genuine reasons why it may be necessary to refuse to supply information requested. The Environmental Information Regulations (EIR) provide some guidance regarding this. A summary of the EIR is provided in Annex 2 of the Data Exchange Principles document.

The criteria proposed below are intended to allow an objective assessment of the potential risk and to give authority to any decision to restrict the release of biodiversity data. In particular, they should provide a means of documenting the nature of the anticipated harm, the mechanism(s) by which it would be anticipated to occur, and why the harm would be sufficiently substantial to justify refusal of the request for biodiversity data. This will then allow the holder of the biodiversity data to review or defend the decision made if called upon to do so by any appeals process.

This list of criteria should not be seen as an attempt to sweep the problems of sensitivity of data 'under the carpet'. Rather they are an attempt to be more rigorous about what circumstances might actually lead to environmental damage. Applying the criteria will not be easy; in many cases a judgement will be required. Nevertheless, the decisions reached should be more objective than would otherwise be the case.

Figure 2.
Criterion for the assessment of data sensitivity

Criterion	Reasoning
Are only certain parts of the biodiversity data likely to lead to harm?	It may be possible to disassociate these from the other biodiversity data to give a partial response, or to aggregate biodiversity data so that they are not sufficiently explicit to lead to harm.
Does the subject of the biodiversity data (species, habitat, geological feature) have attributes that make it vulnerable to human activity?	This relates to more than just rarity *per se*. It might reflect the balance between population size of a species on a particular site and its vulnerability to disturbance (e.g. low reproductive rate). Alternatively, it could refer to the fragility of a habitat or geological feature.
Are the biodiversity data already in the public domain?	Many biodiversity data are. It is nonsensical to be secretive for the sake of it. The location of species at 'honeypot' sites is an example; ospreys are well known to nest at Loch Garten, and the site is very carefully wardened.
Does the precision of the locations within the biodiversity data offer someone a significant advantage in finding the subject of the biodiversity data?	It is often the case that while biodiversity data may not be fully in the public domain (i.e. available to anyone), they are known to those who have expertise in the subject. The question then becomes not whether the biodiversity data in question will enable someone to find the species, but how much of an advantage possession of those biodiversity data will confer. This might also apply to one type of biodiversity data giving a significant clue to other biodiversity data (for example if there is a strong habitat association for a particular species that is known to occur within a more general area).
What is the state of protection of the locations cited in the biodiversity data?	There may be little risk of harm to species and habitats in well protected locations, however vulnerable they are at other locations.

Criterion	Reasoning
Would disclosure of otherwise sensitive biodiversity data help protect the environment?	Sometimes it is better to have biodiversity data in the public domain so that more eyes are watching out for potential harm. The example that comes to mind is urban badger setts. In addition, the lifecycle of an organism (e.g. some of the invertebrates that live in dead wood) may be such that the most effective conservation action would be to inform those who own or manage land that the animal or plant in question has been found.
Would disclosure increase the likelihood of an illegal (e.g. under the Wildlife and Countryside Act) activity?	The Wildlife and Countryside Act (as amended by the CROW Act) makes it illegal to kill or take individuals of selected species. While in many cases the taking of an individual would not cause substantial harm to the population, it is nevertheless illegal. The test should be: would disclosure make the illegal taking of species more likely than at present?
Would disclosure actively increase protection of the environment?	Under the Wildlife and Countryside Act (as amended by the CROW Act), an offence is committed only if a landowner *intentionally* causes damage to an animal or plant on the schedule. It is therefore important that owners and occupiers are informed about the presence of species of conservation importance on their land, as this nullifies a defence of inadvertent damage.
Is there established evidence that substantial harm is, or has been, caused to the subject of the biodiversity data?	Examples here might include badger baiting, collecting rare invertebrates, or the digging up of particular species of wild plants.
Would disclosure substantially damage the ability of a conservation organisation to achieve a specific conservation objective?	Sometimes it is necessary to take very pragmatic decisions to achieve conservation aims and objectives. On rare occasions, it may be necessary to refuse to release biodiversity data, because it would compromise a scientific study, or would significantly damage relationships with others (e.g. landowners), without whose support it would not be possible to achieve the desired end.
Is release of the personal data registered under the Data Protection Act?	When registering as a holder of personal data, it is a requirement to list those from whom data will be obtained, and those to whom it may be disclosed. It is an offence under the Act to release personal data where those data have not been registered for disclosure, or beyond the terms of the registration.
Do the biodiversity data contain elements that might be considered commercial-in-confidence?	This in part relates to contract law and the common requirement of contracts that information which might give a competitor an unfair advantage should be confidential (for example the *cost* of tenders for undertaking survey work).

Annex 2 The Legal Framework

Introduction

This annex provides summary information about the legal framework in relation to the exchange of wildlife information in the UK. The information provided does not constitute legal advice, rather it represents the National Biodiversity Network Trust's best interpretation of the legal implications of wildlife data exchange.

There is very little case law (examples of actual legal action) to advise wildlife data recorders, managers and users. There remain legal grey areas where the implications of the law and/or the risk of legal action are not always clear.

The legal information provided is expected to develop, expand and mature over time as development of the Network continues and legal understanding grows.

The Relevant Acts

1. The Environmental Information Regulations 1992
2. Copyright Law
3. The Data Protection Act
4. Freedom Of Information Act

1. The Environmental Information Regulations 1992

Scope

The Environmental Information Regulations (EIR) are a statutory instrument intended to make public bodies more open about the ways in which decisions are made and about the information upon which decisions are based. They apply to *public bodies*, but there is no definitive list of organisations covered. Given this, it is likely that the regulations will apply to some Local Records Centres (LRCs) but not to others. However, the EIR provide a useful framework for anyone considering what information should be released without any qualms, and what should be considered more sensitive.

The regulations impose a duty to provide information to anyone who asks for it. A full and substantive response must be given to a data request within two months. Whilst the request can be refused on a number of grounds, and a charge can be levied, there is a clear presumption in favour of release. Those making a request do not have to prove an interest. However, if sensitive data are requested it is not unreasonable for the body or individual holding the data to clarify the request to ensure that they do not contravene any of the restrictions on the release of data. In this case, a decision making process to determine what level of detail of information to release to whom, and for what purpose, can be applied.

What do the regulations cover?

The EIR apply to "information relating to the environment" in whatever form it is held (including written, visual, oral and electronic media). Information relates to the environment if it concerns:

- the state of water, air, soil, fauna, flora, land and natural sites;
- activities or measures that are likely to either adversely affect, or protect, the environment.

The regulations are therefore extremely wide ranging.

Restrictions

There is a presumption that information will be made available to those who request it. However, there are general and specific reasons that could lead to refusal of requests. Environmental information held for judicial or legislative purposes is excluded from the scope of the regulations (Regulation 2(1)(b)), and bodies may refuse a request that is manifestly unreasonable or formulated in too general a manner (Regulation 3(3)).

The specific grounds for refusal to supply information are split into two sections; where information *may* be considered confidential (Regulation 4(2)), and where it *must* be considered confidential (Regulation 4(3)).

Biological records are likely to be caught by Regulation 4(3)(c), on the basis that they have been volunteered. The reason why this is in the *must be* rather than *may be confidential* category is to protect whistle-blowers, e.g. the sources of the former Pollution Inspectorate. It is important therefore to have clearly documented agreement from recorders that their records can be used, or both copyright law and the EIR could be inadvertently broken.

Regulation 4(3)(d) is particularly worth noting, as it is this which is most likely to be used as a justification for refusing to release wildlife information, on the grounds of potential sensitivity. Note that it requires a judgement to be made, and if necessary defended if there is an appeal.

The exceptions to the right to information, which are laid out in Regulation 4, were amended in 1998. The listing below incorporates the amendments made.

Exceptions to the right to information

4. 1. Nothing in these Regulations shall:

a. require the disclosure of any information which is capable of being treated as confidential; or

b. authorise or require the disclosure of any information which must be so treated.

2. For the purposes of these Regulations, information is to be capable of being treated as confidential if, and only if, it is information the disclosure of which -

a. would affect international relations, national defence or public security;

b. would affect matters which are, or have been, an issue in any legal proceedings or in any enquiry (including any disciplinary enquiry), or are the subject matter of any investigation undertaken with a view to any such proceedings or enquiry;

c. Would affect the confidentiality of the deliberations of any relevant person;

d. Would involve the supply of a document or other record which is still in the course of completion, or of any internal communication of a relevant person;

e. Would affect the confidentiality of matters to which any commercial or industrial confidentiality attaches, including intellectual property.

3. For the purposes of these Regulations information must be treated as confidential if, and only if, in the case of any request made to a relevant person under regulation 3 above -

a. it is capable of being so treated and its disclosure in response to that request would (apart from regulation 3(7) above) contravene any statutory provision or rule of law or would involve a breach of any agreement;

b. the information is personal information contained in records held in relation to an individual who has not given his consent to its disclosure;

c. the information is held by the relevant person in consequence of having been supplied by a person who:

i. was not under, and could not have been put under, any legal obligation to supply it to the relevant person;

ii. did not supply it in circumstances such that the relevant person is entitled apart from these Regulations to disclose it; and

iii. has not consented to its disclosure;

or

d. the disclosure of the information in response to that request would, in the circumstances, increase the likelihood of damage to the environment affecting anything to which the information relates.

4. Nothing is this regulation shall authorise a refusal to make available any information contained in the same record as, or otherwise held with, other information which is withheld by virtue of this regulation unless it is incapable of being separated from the other information for the purpose of making it available.

2. Copyright Law

What is Copyright?

Copyright is a legal mechanism that exists to safeguard the intellectual property rights of individuals and organisations. The law is set out in the Copyright, Designs and Patents Act 1988, the Copyright (Computer Programs) Regulations 1992, the EC Directive on European harmonisation of copyright protection (93/C 27/09), and the Copyright and Rights in Databases Regulations 1997.

Copyright is one of a number of intellectual property rights (others include moral rights, patent rights, database right, and plant breeders' rights). This is a *very* complex area of law; there is a good summary in Appendix 4 to the CCBR[2] report.

Copyright applies once information has been written down; the material does not have to be published, and does not have to have a copyright statement attached to it.

What Does Copyright Enable?

Copyright enables:

- authors to control and regulate use by others of their original works,
- authors and publishers to seek financial returns for distribution of their works,
- owners to determine how others use their work,
- a legal remedy for unlawful copying that infringes these rights.

Copyright in a published work in the UK

A published literary work, for example a book, journal, magazine, or newspaper cutting, is likely to contain two separate categories of rights protected by copyright.

The copyright in the literary work - lasting for the life of the author, plus a period of 70 years after the end of the year of his death.

The copyright in the typographical arrangement of every published edition of a literary, dramatic or musical work. This copyright belongs to the publisher of the edition and lasts for 25 years from the end of the year in which the edition was first published.

Collecting and holding biodiversity data

For the purposes of the National Biodiversity Network, copyright for data can be summarised within the following framework:

- Biological records are covered by copyright as literary works (there is no requirement for 'literary merit').
- A person making an observation for their own purposes has the copyright to the observation (provided they write it down).
- If a person is paid (through employment or a specific contract) to make an observation, the copyright will belong to their employing organisation or client - unless there is a written agreement to the contrary.
- A person or body collating observations from many sources owns the copyright to the collation. They need to document their agreements with their sources over the purposes of the collation, the right to use the observations, and the way in which use of the information will be managed.

2 Department of the Environment. (1995). Biological Recording in the United Kingdom : Present Practice and Future Development. Main Report. London, HMSO. 145pp + appendices.

- Interpretations, summaries or recommendations are the copyright of the people or organisations making them.

Note that the copyright of a record belongs to its author; i.e. the person who wrote it down. This means that landowners do not own the copyright of data collected on their land. However, in collecting data, it is *essential* that permission to collect information has been gained from landowners, as quite apart from the good practice that this entails, information which has been collected illegally cannot legally be used - for example in a Public Inquiry.

To help to manage biodiversity data without infringing copyright in the future, it is important to set up more formal procedures for keeping track of permissions to use biodiversity data. It is likely that biodiversity data will be collected by many people for very different reasons. It is neither possible nor desirable to give a 'one size fits all' approach to solving these issues, but the thoughts below are intended to be a pragmatic start to thinking about how to alleviate the problems currently faced.

Dealing with copyright in a commercial contract

If another organisation is collecting information as part of a legal contract, then the conditions in that contract should cover the issue of who owns the copyright of the products developed as under the contract. In most cases this will be the organisation that commissioned the work.

Dealing with copyright where there is no contract

Biodiversity data are collected in a number of ways not covered by a commercial contract. For example, biodiversity data might be collected by:

- individual volunteers;
- a voluntary organisation;
- an academic institution through its students.

In these cases those involved should be asked to sign copies of a letter formally donating the information. These will give the recipients either full or limited rights of use over the biodiversity data. Those asked to sign should include not just those people who are collecting biodiversity data in the field, but also anyone drawing up charts, graphs, plans or diagrams which form part of the biodiversity dataset as a whole. It is unlikely that biodiversity data suppliers who have collected a significant amount of information will be willing to fully sign-away their copyright in the biodiversity data that they have collected. However, this need not be an insurmountable problem – all that is actually required is a licence for the data to be used for the wide range of purposes that the National Biodiversity Network enables.

A sensible approach may be to take the line that occasional records received from the general public are treated as donations and can be used freely in output, but that the use of records from more productive recorders should be agreed with those recorders. In cases where local experts have contributed large quantities of information it should be possible to negotiate a written agreement between the user(s) and collector(s).

Copyright of datasets

A dataset is simply shorthand for the different pieces of data put together in a group. When this is done it is important to make sure that all authors of the information to be collated have given their permission for its use.

Passing biodiversity data on

Where information is collected by one source and then passed on to someone else to collate, turn into tables etc, then the second source should have either; a) signed a formal agreement, or; b) signed a donation form.

When they hand over their completed package of work. For complicated information products, it is possible that a chain of rights will exist, with additions for each stage from basic raw biodiversity data to finished report.

Dealing with legacy data

It is likely that most organisations hold a good deal of information that was supplied a long time ago (historic or legacy data). If no positive permission to release data has been given, then all copyright and other intellectual property rights remain with the original supplier of the data. These rights are passed down with an individual's estate on their death.

Data custodians for historic data will need to try to find out whether permission was ever given. It is sensible however to be pragmatic about whether it is necessary to seek retrospective permission for use (as may be true in some cases).

Moral rights

The concept of moral rights comes from the Berne Convention for the protection of literary and artistic works. Copyright essentially deals with the economic rights that someone has in a work, i.e. to stop someone else using it, copying it and getting money from it. Moral rights refer to the right of the true author of a work to; a) be properly identified, and; b) object to any derogatory treatment of the work, i.e. to protect the author's reputation.

Some questions have been raised whether verification (and potentially re-determination of records) could impinge on the moral rights of an author of records if the process leads to a challenge to the identification made by the originator of the biodiversity data. This is unclear, but a pragmatic solution is to ensure that it is clear both what the original record was and that the subsequent determination is an amendment to the record, as this then ensures that an audit trail of changes is available. This would ensure the original author of the record could be identified (their name is not overwritten by the determiner's name), and whether the determination is viewed as derogatory can be assessed by consideration of the expertise of the author and determiner(s). The new version of Recorder implements this approach.

Protecting copyright

It is standard practice for many organisations to include a paragraph asserting copyright when their data are passed to others. The exact details will clearly vary between organisations, but might be similar to the example below:

> © [Name]. All rights reserved. The moral rights of the Author are asserted. The copyright of material provided in response to this request for information is vested in [Name]. This information is provided subject to the condition that it shall not in any way of trade or otherwise, be lent, sold or resold, hired out, or otherwise circulated in any form without the prior written consent of [Name].
>
> The information provided here is believed to be correct. However, no responsibility can be accepted by the [Name] or any of its partners or officers for any consequences of errors or omissions, nor responsibility for loss occasioned to any person acting or refraining from action as a result of this information and no claims for compensation for damage or negligence will be accepted.

Infringement of copyright

An infringement occurs if a work protected by copyright, or any substantial part of such a work, is copied without the permission of the copyright owner. The copyright law does not define the meaning of 'substantial part' but the courts have held that 'substantial' is a qualitative and not merely a quantitative criterion.

The potential for infringement of copyright exists in many parts of everyone's work. For example, it is *not* permissible to answer requests for information by copying press cuttings. Similarly, only limited parts of reports or academic papers should be photocopied. Blithely

copying whole works is illegal, and infringes the principle of fair dealing under which copies of some material can be made.

In the context of the use of information within the National Biodiversity Network, infringement of copyright would mean using or holding data without permission of its owner or their agents. It also means copying a substantial part of a database without permission – this would infringe the database right created by the Copyright and Rights in Databases Regulations 1997 (which implement the EC Directive on the legal protection of databases (96/9/EC)).

Who is liable for infringement of copyright?

The individual who actually carries out the infringing act is liable. In the case of photocopying, however, liability is not limited to the person who actually makes the copies.

A person who causes an infringing act to take place, by giving instructions to an agent or employee acting on his behalf, will be liable for those acts.

Copyright law stipulates that a person is liable if he 'authorises' another person to carry out an infringing act. Thus, any person who makes a copyright work available to another person and tells that person to make a copy of it, or of a substantial part of it, would, if that copying were not covered by proper permission or by statutory exception, be infringing copyright.

So what can I copy?

Only the copyright holder has exclusive rights in the work, and only they can copy freely. However, in the interests of the dissemination of knowledge, a copy may be made by individuals for purposes of research or private study, criticism or review, or news reporting. Unfortunately, the 1988 Act is not clear about amounts that may be copied, and the law has been subject to varying interpretations.

As a general rule, *restrictions on copying apply to **all** published material and only a single copy of any item can be made*; source details should be acknowledged on any copies. *If it is necessary to make multiple copies for any reason, it is essential to contact the copyright holder to seek permission or to have obtained a licence.* If permission from the copyright owner to copy outside the normal rules has been received, details to this effect should be retained. Photocopies should not be held on files; it is good practice to keep reference details to the article instead. Photocopies also cannot be held in libraries unless permission to copy has been obtained. Where a photocopy is placed on a library's shelves the item must contain a statement of the right to hold a photocopy for such purposes.

Libraries can copy material for you, but are subject to similar regulations and will ask you to sign a copyright declaration form, without which copies cannot be provided. The signature has to be the person retaining the copy and an electronic signature is not yet acceptable in the law.

Map-based information

A number of datasets include maps as an integral part of the information. The copyright on maps is complicated, and restrictions on copying and release of such data do apply, depending on the owners of the maps and of the data superimposed on the base map.

Photographs, slides, videos and other artwork

Equally, photographs and other artwork (including diagrams, slides, videos, and audio recordings) also form parts of a number of datasets, and are covered by copyright law in their own right. Given that the source (and therefore copyright) of some of these may be unknown, it is important to take great care to ensure that copyright is not infringed.

The Internet

Copyright also applies to information that is posted on World Wide Web (www.) pages or otherwise passed around the Internet. This is the case even if there is no obvious copyright statement. Great care should be taken to ensure that appropriate permission is gained before

using any material sourced from the Internet, and to ensure that the information used is correct (it should not be trusted just because it is electronic).

3. Personal Data and the Data Protection Act

What is data protection?

Data protection is a mechanism to regulate the use of personal data about individuals. It has a legal basis in the Data Protection Act 1998, which updates the Data Protection Act 1984 as a result of the EC Directive on Data Protection (95/46/EC). This intended to provide a balance between the Convention on Human Rights and the Treaty of Rome. The Directive took effect on 24 October 1998, but there was a short delay (until 1 March 2000) before the new Act came into force, owing to the need to implement secondary legislation to support it.

Data protection

- Data protection provides a legislative framework for the collection, storage and use of personal information held on manual and computer files.
- Data protection applies to living people, and therefore does not apply to corporate bodies.

Data Protection Act 1998

- Covers *all* users of personal data (whether registered or not, or exempt from the requirement to register).
- Refines the data protection principles.
- Extends them to cover certain categories of manual data (i.e. paper files).
- Requires those using data to make available details of their processing on request.

There is a three-year transition period for data controllers to bring 'processing under way' into compliance with the new law (i.e. by October 2001). Data in manual filing systems may not need to comply with many aspects of the new law until 2007; however, the transition arrangements are complex, so advice on specific circumstances should be sought.

The data protection principles of the 1984 Act have largely been retained (Schedule 1 of the 1998 Act). Principle 1, which deals with obtaining information fairly, is strengthened as it expressly provides that certain conditions must be met. These include informing the data subject of the purposes for which the data are to be processed.

In addition, processing of personal data may only be carried out if at least one of the following conditions is met (Schedule 2):

- the individual has given their consent to the processing;
- the processing is necessary for the performance of a contract with the individual;
- the processing is required under a legal obligation;
- the processing is necessary to protect the vital interests of the individual;
- to carry out public functions, or;
- the processing is necessary to pursue the legitimate interests of a business (unless prejudicial to the interest of the individual).

Stricter conditions apply to the processing of sensitive personal data (which includes racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, sex life and criminal convictions). Not only must the data controller conform to the principles and Schedule 2, but also processing is prohibited unless at least one of the conditions in Schedule 3 is met. This will usually mean that *explicit* consent of the individual concerned to process such data is required. Note that the definition of processing includes obtaining data.

When is information 'personal'?

Personal data are defined under the new Act as information from which someone can be identified either directly or by combination with other data in the possession of (or likely to come

into the possession of) the data controller (i.e. the person who controls the purpose and manner of processing the data).

Personal data also includes opinions about the data subject or data which relate to the intentions of the data controller in relation to the data subject.

In the old Act if a name was incidental then the Act didn't apply. Under the new Act naming someone, for example in the preparation of a document, *is* covered.

Registration / Notification

Under the 1984 Act, all individuals and organisations who use 'personal information' (with only very minor exceptions) were required to register with the Data Protection Registrar[3] the *purposes* for which the information is held, the *classes* of data held, its *sources* and the *disclosures* they expect to make.

A revised and simpler process of notification will replace the current system of registration. The details of the notification process and its cost have not yet been decided; until then there is little data users can do to revise their current arrangements. Notification will have to include an outline of the security measures to be taken to ensure compliance with the seventh data protection principle, but obviously this will not have to be in such detail that the security processes would be invalidated.

Registration (currently) costs £75 and lasts for 3 years. It is possible to amend a registration at any time. Unless covered by an exemption, holding or using personal information without being registered is a criminal offence.

Exemptions

A range of exemptions are likely to be included in the secondary legislation implementing the 1998 Act. These are:

- National security.
- Crime and taxation.
- Health, education and social work.
- Regulatory Activity.
- Research Purposes.
- Information required to be made public.
- Domestic Purposes.

The definition of what these cover and the manner in which they can be applied will be strictly defined and applied; they are not a catch-all, and are exemptions from individual rights rather than from the need to notify. In addition to the exemptions listed above, a number of miscellaneous exemptions will apply, and three 'special purposes' are defined (journalism, artistic purposes and literary purposes): these are intended to allow for 'freedom of expression'. Those holding information under an exemption will still be required to comply with the Act, and will be required to respond to a request for information as if they were registered.

It is worth noting that the 'research purposes' exemption may be relevant to biological records in-as-much as it defines that the second and fifth principles will not be breached provided that the processing will not adversely affect individuals referred to within the data. This allows for data to be archived and used indefinitely provided that the personal data is *incidental* to the processing undertaken.

Releasing personal information

3 Office of the Data Protection Registrar, Wycliffe House, Water Lane, Wilmslow. Cheshire. SK9 5AF. Information line : 01625-545745. email : data@wycliffe.demon.co.uk

If the data have not been registered as available for disclosure, then they *must* not be released. *Release of personal information for which an organisation or individual is not registered is a criminal offence.* It is possible for employees to be held *personally responsible* for unauthorised release(s) of personal data.

Data subject request

An individual asking for information held about them must receive a response within 28 days (but note that there are transitional arrangements regarding the release of data from manual files).

If releasing information on an individual would allow the identification of another individual (who may for example be the source of the information to be released) a balancing test (the 'Gaskin' test) must be applied to determine what information to release. This must assess whose right is the most pressing - the right of an individual to have information about themselves, or the right of the third party to have their identification protected. It will be necessary in such a case either to seek the consent of the third party involved or assess if the circumstances are such that it is reasonable to release the information without consent. Guidance on this can be sought from the Data Protection Registrar.

New rights

The new law creates some new rights for individuals. These include:

- prevention of processing likely to cause damage or distress;
- knowledge of the logic behind automated decision making;
- not to have significant decisions based solely on the results of automatic processing;
- prevention of processing for the purpose of direct marketing.

Manual records

The 1984 Act only covered personal data held in a form that could be automatically processed - e.g. on computer. The scope of the 1998 Act has been extended to cover information in a 'relevant filing system' where the records are structured either by reference to individuals or by reference to criteria relating to individuals so that 'specific information relating to a particular individual is readily accessible'. This will include some manual files. Exactly what should or should not be regarded as covered is at present unclear, as the definition could be interpreted in a number of ways (e.g. what do 'readily' and 'specific' mean).

It is likely that structured information such as card indexes, microfilm systems and personnel records will fall within this definition. It would probably be risky to limit interpretation of the scope of the incorporation of manual filing systems to an absolute minimum. It may be worth noting that the Data Protection Registrar is interpreting the provision more widely than Government.

Data protection principles

The Act has a number of principles of data management (i.e. how the data are to be collected, stored and used) that data users (those registered with the Data Protection Registrar) must abide by. These Principles are provided below.

The Principles of the Data Protection Act

1 **Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless -**

a) at least one of the conditions in Schedule 2 is met, and

b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2 **Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with those purposes.**

3 **Personal data shall be adequate, relevant, and not excessive in relation to the purpose or purposes for which they are processed.**

4 **Personal data shall be accurate and, where necessary, kept up to date.**

5 **Personal data processed 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.**

There is a lot more detail about how the principles should be applied, for example with respect to fair obtaining (Principle 1), in a set of guidelines to the Data Protection Act. These (and a number of other documents) are available from the Data Protection Registrar's office.

Libel, Slander and Defamation

Under English law there is a differentiation between what is spoken and written (i.e. slander and libel). In Scotland one law fits all (the crime is defamation) and it is the message not the medium that matters. All of these may be broadly defined as casting doubt on someone's performance or opinion, whether they are acting in an amateur or professional capacity.

There are exceptions. For example, if you can prove what you are saying is true, or the somewhat shady area of '*fair comment*' e.g. The Scotland team is [insert adjective of your choice!].

4. Freedom of Information Act

This Section is Under Development

Annex 3 Acknowledgements

This is the edited trial version draft of the National Biodiversity Networks Data Exchange Principles (v3.1). This latest revision is a working document and will continue to develop and evolve, this time in practical trials. This current version has been reached through the work of many individuals in addition to those that contributed to the *Consultation Draft*.

The development work for previous drafts included workshops both within the statutory conservation agencies and organised by the National Biodiversity Network Trust (NBNT), Biological Recording in Scotland (BRISC) and the National Federation for Biological Recording (NFBR). A number of individuals provided particular assistance to the *Consultation Draft* authors, Lawrence Way and James Williams (both of the Biodiversity Information Service, Joint Nature Conservation Committee (JNCC)), including comments on earlier drafts, copyediting and formatting. The consultation draft was released in April 2000.

Responses and feedback to the *Consultation Draft* were summarised and assessed by an NBNT, JNCC, and English Nature (EN) group. The conclusions of this group fed into a redraft of the principles. Oliver Grafton (the Access & Accreditation Projects Officer of the NBNT) led this work with support from Lawrence Way and James Williams (JNCC).

A number of individuals provided particular assistance, including comments on earlier drafts, copyediting and formatting. Without wishing to minimise the inputs from discussions and workshops that included a wide range of individuals interested in the NBN, we particularly wish to acknowledge contributions to all versions from Bill Butcher, Patrick Cloughley, David Connor, Nicky Court, Paul Green, Jeremy Greenwood, Paul Harding, Sara Hawkswell, Keith Hiscock, Trevor James, Stefa Kasnowska, Ed Mackey, Jo Marsh, Jim Munford, Keith Porter, Mike Burke, Deborah Russell, Anne-Marie Smout, Paul Rose and all members of the Access and Accreditation Steering Committee.

The authors (James Williams and Lawrence Way of the Biodiversity Information Service, Joint Nature Conservation Committee, and Oliver Grafton of the National Biodiversity Network Trust) gratefully acknowledge these inputs.

Useful links

In considering the framework presented in this paper, readers may also like to see how other networks and projects are approaching the issues raised by providing access to biodiversity data. The following web links are considered to be particularly useful. If you know of other links that are useful then please let us know.

http://www.biodiversity.org/pfis.html

http://www.hmso.gov.uk/acts.htm

http://www.open.gov.uk/dpr/dprhome.htm

http://www.homeoffice.gov.uk/foi/index.htm

http://www.scotland.gov.uk/pubappt/foi.asp

http://www.hrwallingford.co.uk/projects/envaldat

Copyright

Disclaimer

This is a complex and grey area of legislation and any opinions or interpretations expressed here cannot be taken as a statement of the law. The information provided here is believed to be correct. However, no responsibility can be accepted by the JNCC or NBNT or any of its partners or officers for any consequences of errors or omissions, nor responsibility for loss occasioned to any person acting or refraining from action as a result of this information, and no claims for compensation for damage or negligence will be accepted.