

NATIONAL GRID PLC
GROUP POLICY STATEMENT
INFORMATION & RECORDS MANAGEMENT

1. Objective

1.1 This policy provides the criteria for all users of information to:

- Ensure that information and records are complete and accurate
- Classify information appropriately and handle information in accordance with its classification
- Keep records safe from loss or damage & secure them from unauthorised access
- Make stored information available to all authorised users
- As promptly as practicable, discard records that are no longer required to be retained to meet business needs or legal requirements.

1.2 Efficient information and records management will allow National Grid to :

- Comply with the requirements placed upon us by legislation such as the Companies Act, the US Securities Laws, and the Federal Power Act, external agencies such as Ofgem, the SEC, the FERC, and the Inland Revenue
- Contribute to the efficient operation of our businesses ; and
- Control the costs of information management and retention.

1.3 Failure to classify information appropriately increases the risks of unauthorised access and disclosure. Failure to provide an efficient and effective system of document retention and retrieval hinders the efficiency of our day to day business activities, can prejudice the position of National Grid in litigation, tax and regulatory matters, and result in potential damages and loss of reputation.

1.4 The key sources of best practice for this policy are:

- ISO15489 Code of Best Practice for Information Records Management
- ISO17799 Code of Best Practice for Information Security Management
- BIP0008 Code of Practice for Legal Admissibility & Evidential Weight
- The Sarbanes Oxley Act and other laws and regulations relating to spoliation of evidence.

2. Scope

2.1 This policy applies to all businesses within National Grid. For Associate Companies and Joint Ventures National Grid will seek to promote the adoption of procedures consistent with the principles set out in this document.

2.2 Information owners, must classify information appropriately, and create and maintain records that meet the legal, regulatory, fiscal and operational needs of the Group and its specific companies and businesses.

3. Policy Implementation Framework

3.1 Responsibility

- 3.1.1 It is the responsibility of each business within National Grid to adopt information & records management procedures that comply with all relevant legal requirements, consistent with best practice as applied to their business needs.
- 3.1.2 Each business should create and retain records to provide the rationale underpinning key strategic decisions and significant transactions in order to maintain a Corporate Memory.
- 3.1.3 All National Grid businesses must have as a minimum:
- A procedure for the creation of complete and accurate information & records that deliver appropriate information quality requirements
 - A procedure that assesses the nature of the information, the risk of its disclosure and classifies it accordingly
 - Procedures for the management, retention, storage and destruction of records in all media, for the whole period of their retention
 - An up to date records retention schedule that is published and made available to all internal stakeholders
 - A procedure for identifying and protecting business critical records / records that must be retained by law
 - Records officers or other officers responsible for co-ordination and implementation of the policy in each area of the business
 - Filing structures for records
 - A method of identifying records of archival value
 - A means of sharing information held in libraries

3.2 Information Classification

- 3.2.1 National Grid's position is that information should be freely available, internally and externally, except in circumstances where disclosure is prohibited by law, regulation or contractual obligation or would potentially harm or place an unreasonable burden on its business, or that of any of its operating companies, its employees, or third parties; for example:
- damage or prejudice to National Grid's operational or commercial interests, or that of its partners or third parties, or the security of its assets
 - premature exposure of Price Sensitive or Inside Information
 - breach of a confidentiality clause in a contract with another party
 - release of personnel information
 - breach of the provisions of any legislation / regulation
 - release of Government classified information
- 3.2.2 Owners and creators of information must classify the information appropriately, and for confidential information, must protect it appropriately.

3.2.3 When classified information is received from outside the Group, the recipient must ensure that the classification specified by the originator / sender is understood and respected within the Group.

3.2.4 The following classifications are considered as the minimum to be applied (see Appendix A for definitions of each classification and for further advice):

- Publicly Available
- Internal Use Only
- Confidential
- Privileged and Confidential
- Strictly Confidential
- Price Sensitive Information (also known as Inside Information)

3.3 Control of Information

3.3.1 Information that is vital to the Group's day-to-day operations is increasingly important in maintaining a competitive edge. It is a corporate asset that must be classified appropriately and securely protected to minimise the risks to the business using existing in-house storage facilities where possible.

3.3.2 Each business within National Grid must effectively classify, handle, store, communicate and discard information consistently with applicable legal and regulatory requirements.

3.4 Disclosure of Company Records

3.4.1 In general, all records produced within National Grid are the property of the relevant company or business that produced them. Consideration must be given before disclosing them externally and reference must be made to the confidentiality classification the information contained has been given.

3.4.2 Information Users should seek advice from the relevant information owner and/or policy leads before disclosing information if disclosure has not been specified in the classification or if the user wants to disseminate that information outside the original distribution list. Obligations placed upon us by any relevant access to information legislation must be understood.

3.4.3 Requests for information made in judicial or administrative processes must be referred to company legal counsel for review unless there is an established procedure in place that has been approved by the Group Company Secretary and General Counsel.

4. Related Group Policies/Procedures and Other Documents

- Business Continuity Procedure
- Information Security Management Procedure
- Physical Security Procedure
- Company Secretariat Roles & Responsibilities Statement
- Protection and Disclosure of Inside Information

5. Key Contacts

Policy Owner Group Company Secretary & General Counsel

Policy Lead UK - Information Assurance Manager (Legal Services)
US - Deputy General Counsel

6. Monitoring & Compliance

- 6.1 The Group Company Secretary and General Counsel will review compliance with this policy statement at least annually. Any material changes needed to ensure its effectiveness will be drawn to the Board's attention.
- 6.2 Each business within National Grid will ensure that it has the necessary arrangements in place to monitor and report compliance against this policy on an annual basis. Each Associate Company will be encouraged to put in place similar arrangements to enable compliance to be reported on an annual basis.

7. Definitions

Owner: All information/data should have an owner. The owner of specific items of information or data is an individual who has been given the responsibility, by the business, for defining who should be given access to the information, the classification level and the retention period.

Information: All forms of written, printed and electronic documents; information given or received orally in meetings, informal discussions or telephone conversations; data stored on magnetic or other electronic media or in the memory of a computer; streams of data being transmitted over communications lines; and information in digital, graphic, text, voice or image format.

Record: Any written document, whether paper or electronic, including records stored on disc, tape, microfiche and other similar media

Associate Company: A company whose equity share capital is 20% or more but not more than 50%, beneficially owned by a National Grid company or companies.

Joint Venture: A commercial undertaking entered into by two or more parties (one being a National Grid company), by setting up a separate company in which all partners have shares.

8. Timing

- Date policy came in to effect **July 2005**
- Date policy was last updated **January 2007**
- Date policy will next be reviewed **November 2007**

CLASSIFICATION DEFINITIONS AND ADVICE

Publicly Available

Information that is routinely received from or made available to the public and information that, if disclosed outside the Group, would not harm or cause embarrassment to the Group or its employees or to the public.

Internal Use Only

Information made available to employees, but to which external access is granted only with authorisation. The disclosure or loss of such information would be inappropriate and could have an adverse effect on the Group.

Confidential

Information that is commercially or operationally sensitive and whose disclosure or loss could have a significant impact on the Group or information that pertains to employees and is protected through local policies and/or laws and regulations relating to the privacy of personal data. The impact could be financial or involve embarrassment or loss of reputation. This classification requires authorisation by the owner of the information and should be disseminated only on a “need to know” basis and, if applicable, in accordance with local policies and laws and regulations.

Access to Confidential Information should be controlled by methods such as utilisation of defined distribution lists or specific shared electronic folders. Information may also be restricted by requiring the explicit approval of the owner before further dissemination via electronic or paper form.

Privileged and Confidential

This refers to certain legal documentation and shall be applied only at the instigation of legal counsel. “Privileged and Confidential” should only be disseminated with the approval of legal counsel.

Strictly Confidential

This refers to information that is commercially or operationally sensitive and whose disclosure or loss would have a very significant impact on the Group. This information should be restricted to named groups or individuals only. If only paper copies of information are distributed controls may be enhanced by numbering each copy and recording receipt.

For example, this level of classification would be used where disclosure or loss could result in damage or prejudice to the security of National Grid’s assets or situations where business development proposals are still under negotiation.

Price-sensitive Information/Inside Information (see “Related Group Policies and Procedures” below)

This is defined as Information not already public knowledge, the disclosure of which may lead to a significant movement, whether up or down, in the price of National Grid shares or other listed securities.

Each business within National Grid may further define its own system of classifications based on the following principles:

- a classification should not be used unless it can be clearly understood by the users of that classification throughout the Group without additional explanation
- information whose disclosure would entail no risk of any adverse effect should not be classified as “confidential, “strictly confidential” or “privileged and confidential”
- confidentiality classifications given to a specific item of information should be the lowest practicable, having regard to the magnitude of the adverse effect or effects expected to arise from disclosure
- the classification level of much information is time dependent. The status of classified information should be regularly revisited with a view to reducing or removing the confidentiality classification of information whose disclosure would no longer involve a risk of an adverse effect or effects
- information which refers to employees, groups or other individuals, regardless of whether disclosure would cause distress or embarrassment to those persons, should only be gathered, stored and used in accordance with local policies and any statutory requirements relating to the privacy of personal data. An appropriate classification should be applied to this category of information.

Each business within National Grid is responsible for classifying the information it creates and receives appropriately, and for handling such information consistently with its classification. Individual documents and emails need not be individually labelled with its classification as long as appropriate measures are taken to classify them and treat them accordingly.