1.14 DATA PROTECTION POLICY inc. MANAGEMENT AND DISCLOSURE OF EMPLOYEE DATA

Issue No. 4 dated 08/06/2009

1. Introduction

Data Protection regulates the way in which companies may use the personal information of individuals (whether customers, staff, suppliers or third party etc.) and protects them from unauthorised use or disclosure of their personal details e.g. name, address, telephone number etc. ("personal data").

Johnston Press plc ("the Group") aims to fulfil its obligations under the Data Protection Act 1998 ("the 1998 Act") in order to strike a balance between the Group's legitimate need to run its business and an individual's legitimate right to respect for his or her private life. The purpose of this policy is to provide guidance on management and disclosure of personal data and is not intended to confer any additional rights or contractually bind the Group.

1.1 Governing Legislation

The current law is contained in the 1998 Act, which came into force on 24 October 2001. Whilst it resembles the old 1984 Act in many respects, requirements under the 1998 Act are more stringent: the definition of processing is made wider; the eight Data Protection Principles are more detailed; the investigatory powers of the Information Commissioner (formerly Data Protection Registrar) are widened and the scope of Data Protection law is considerably extended.

1.2 Responsibilities

Compliancy with the 1998 Act is the responsibility shared by all employees of the Group. Employees are expected to familiarise themselves with, and observe at all times the Group's rules and procedures relating to Data Protection, the policy statement and any additional instructions.

The person having overall responsibility for Data Protection within the Group will be the Group Data Protection Manager whose contact details can be viewed within section 12 of this policy or can be obtained from the Divisional HR Director.

The Group Data Protection Manager should be the first point of contact on all legal and policy matters relating to Data Protection and privacy. Should legal advice be required this will be arranged through the Group Data Protection Manager (see policy 4.1 Legal Advice) and should not be taken locally.

All correspondence and training documentation relating to Data Protection and privacy must be approved by the Group Data Protection Manager prior to circulation.

Each Manager and Supervisor will have responsibility for Data Protection matters in his/her own immediate area of work.

It is the responsibility of all employees to ensure that all personal data provided by them to the Group is accurate and updated where appropriate.

The Group will implement and comply with the 8 Data Protection Principles contained in the 1998 Act. The principles of Data Protection state that personal data must be:

1. Fairly and lawfully processed
2. Processed for specified purposes and not in any other way which would be incompatible with those purposes
3. Adequate, relevant and not excessive
4. Accurate and kept up to date

5. Not kept for longer than is necessary
6. Processed in line with the data subject's rights
7. Kept secure
8. Not transferred to a country which does not have adequate Data Protection laws

1.3 Non-compliance

Failure by any Group company to comply with any of the requirements of Data Protection legislation could result in serious consequences for that company and the Group, including being prevented from using the personal data, possible personal criminal liability for staff, the likelihood of damaging media attention and the possibility of an investigation followed by sanctions being imposed by the Information Commissioner.

2. Policy

It is the policy of the Group to comply with the letter and spirit of Data Protection legislation. In specific terms, this means for each Group company:

- Operating within the confines of its Data Protection notification
- Operating in compliance with the eight Data Protection principles
- Providing appropriate Data Protection training to all staff
- Ensuring any exemptions are applied consistently and accurately in accordance with the law
- Taking note of the guidance and standards issued by the Information Commissioner from time to time
- Taking note of applicable industry codes of practice, for example:

    - the Direct Marketing Association
    - the British Codes of Advertising and Sales Promotion
    - the Press Complaints Commission

  These are codes of practice in the UK. Other codes may apply to other specific areas of the business.

2.1 Standards

All businesses will adopt the Johnston Press Data Protection Policy and establish the adequate compliance arrangements, including adequate business processes and training schedules, to implement that policy.

The Group Data Protection Manager and other relevant internal audit functions will conduct an ongoing review of compliance with the Data Protection Policy.

3. Collection and Retention

The Group collects and uses personal data about living individuals in order to carry on its business and meet its customers' requirements effectively. The Group recognises that the lawful and correct treatment of personal data is very important to successful operations and to maintaining trust between the Group and its customers.

Any personal data which are collected, recorded or used in any way whether held on paper, computer or other media will have the appropriate safeguards applied to it to ensure compliance with the 1998 Act.

3.1 Collection

The Group will only collect personal data that is relevant to the carrying out of the legitimate purposes and functions of the Group in a way that is not prejudicial to the interests of individuals.

The Group will ensure that the data collection is accurate as is possible, given the methods used in collection.

Employee's consent will have been obtained by the Group prior to the commencement of employment as part of the Group's ongoing Data Protection compliance. Employees will be informed what personal data needs to be processed for additional purposes and will be informed of the purpose for which it is intended to be processed and the identity of the Group's nominated representatives.

3.2 Data Retention

The Group will ensure that regular data care procedures are fully and conscientiously followed. All personal data will be kept up to date and when no longer required for the legitimate purposes of the Group will be regularly purged (see policy 4.9 Document Retention).

3.3 Sensitive Personal Data

Sensitive personal data are personal data about an individual's racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental condition, sexual life, details of the commission or alleged commission of any offence and any court proceedings relating to the commission of an offence.

The Group will handle sensitive personal data with particular care. Before collecting or processing sensitive personal data, the Group will ensure that the appropriate notifications to the individuals have been given and any required consents obtained.

4. Disclosures

The Group will not allow data collected from individuals to be disclosed to third parties except in circumstances which meet the requirement of the 1998 Act. For example:

- The individual has consented to the disclosure; or
- The Group is legally obliged to disclose the data; or
- There is a business requirement to disclose the data which is within the remit of the 1998 Act and is not prejudicial to the interests of the individual.

5. Processing

Data processing will be allowed where there is a clear purpose for the activity which meets the requirement of the 1998 Act. Any non-obvious purposes for processing will be notified to the individual, who in turn, will be given the opportunity to object to this type of processing.

Employee personal data may be processed for the purposes of salary administration, pension administration, health administration, health insurance/benefits, training and appraisal including performance records, disciplinary and grievance records, Group car fleet/leasing administration, any Group benefit administration, marketing of products and services to employees, for the purposes of any potential sale of over 50% of the shares of the Group or other changes of control or any potential transfer of an employee's employment under the Transfer of Undertakings (Protection of Employment) Regulations 1981. Disclosure may include the in the case of sale, change of control or transfer, disclosure to the potential purchaser or investor and their advisors.

Where personal data are passed to a third party for processing, the Group will ensure that a written contract is put in place that requires the data processor to act only on the instructions of the Group, not to disclose personal data without specific authority, to provide appropriate operational and technical security and to allow the Group to audit adherence to the contract.

6. Editorial Exemption

Under the 1998 Act journalism is defined as a 'special purpose' to which an exemption applies. In order to claim the exemption the processing of personal data must be undertaken with a view to publication and the publication must be in the public interest. The exemption states that any processing satisfying these two criteria does not have to comply with the principles of the 1998 Act other than the seventh which relates to keeping personal data physically and technically secure. The exemption also removes the individual's right to access a copy of their personal data and to have their personal data deleted, blocked and/or corrected.

It should be noted that the exemption does **not** include the offences under the 1998 Act, for example it is an offence to buy illegally obtained personal data. Journalists should be aware of this and ensure that any personal data purchased is procured from a legal source. For further guidance on Data Protection journalists should refer to the Press Complaints Commission published note, 'Data Protection Act, Journalism and the Press Complaints Commission Code' and the Johnston Press Editorial Data Protection Briefing.

7. Transfers or Joint Venture Arrangements

It is essential that any transfers of personal data outside the Group are subject to safeguards to ensure compliance. Such transfers must comply with established internal guidelines to ensure that appropriate notifications have been given, a comprehensive data processor contract must be put in place if required and any required consents should be obtained or rights to object provided. In particular, the Group will require third parties to agree to comply with appropriate privacy and information security standards designed to ensure an adequate level of protection.

8. Transfers to Third Countries

Transfers of personal data to countries within the European Economic Area (EEA) do not create any Data Protection issues. A comprehensive data processor contract should be put in place if transferring to a third party, but no additional measures need to be taken to ensure Data Protection compliance.

However, personal data must **not** be transferred to a country or territory outside the EEA unless the country or territory ensures an adequate level of data protection. Therefore the Group Data Protection Manager will assess whether the country provides this level of protection and put in place an appropriate contract with the third party to ensure adequacy.

9. Subject Access

Employees are entitled to access their personal data and may do so by completing an Employee Subject Access Request form (SAR01) which can be found on the Johnston Press Intranet or by contacting their local HR Administrator. The local centre will respond to the request with a confirmation of receipt. Within 40 days of receipt the local centre will supply all relevant information to which the individual is entitled under the 1998 Act. The information will be provided in a format agreed with the individual.

Employees should inform their local HR Department immediately when they believe that any personal data held on them is not accurate or untrue.

In the event of a disagreement between an employee and the Group regarding personal data, the matter should be taken up under the Group's grievance procedure.

10. Marketing

The Group will act on any request from an individual to cease processing his or her personal data for the purpose of direct marketing.

The Group will adhere to all other relevant legislation governing marketing by telegraphic and electronic communication methods.

11. Security

The appropriate logical, technical, physical and operational security will be put in place to ensure the security of personal data against the unauthorised or unlawful processing of the personal data and against the accidental loss or destruction of, or damage to, personal data.

Employees who are required as part of their job description to process personal data about employees or customers will receive training and guidance on the security of personal data to ensure that all data is processed fairly and lawfully. However, the Group expects all of its employees to be aware of the basic principles as set out in this policy. In particular, employees should be aware of the following:

- The Group Data Protection Manager must be the first point of contact on all legal and policy matters relating to Data Protection;
- All personal data held by the Group must be treated as strictly confidential;
- Personal data must not be disclosed to anyone outside the Group unless the individual concerned has consented to such disclosure or the Group Data Protection Manager has given specific instructions to do so;
- The personal data must be kept secure at all times. It must not be left unattended unless it has been placed in a secure location. Group companies will be advised by the Group Data Protection Manager of the physical security or arrangements to be adopted appropriate to the level of confidentiality of the personal data concerned;
- Personal data must not be removed or transferred from the Group's premises without documented authorisation from the Group Data Protection Manager,
- It is the responsibility of all employees to report all security breaches or suspected security breaches or disclosure of personal data to the Group Data Protection Manager.

Breach of these guidelines may lead to disciplinary action and depending on the seriousness of the breach may lead to summary dismissal.

12. Contact

If you have an enquiry or concern about our Data Protection policy, please contact the Group Data Protection Manager:

Name: Frank Bingley
Based: Yorkshire Post Newspapers, Wellington Street, Leeds, LS1 1RF,
DX 25151, LEEDS 4
Telephone: 0113 238 8131
Email: frank.bingley@ypn.co.uk