Issue No: 2
Dated: Sept 2007

PERSONNEL POLICY AND PROCEDURE NO: 1.10

MANAGEMENT & DISCLOSURE OF EMPLOYEE DATA

1. POLICY

The Company has a comprehensive Data Protection Policy which is number 1.14 of the Group Guidelines. Compliance with the Data Protection Act is a responsibility shared by all employees of the Company. As an employee of the Company you are expected to familiarise yourself with, and observe at all times the Company's rules and procedures relating to Data Protection which includes Group guideline 1.14 and any additional instructions which may be released from time to time.

2. MANAGEMENT & DISCLOSURE OF EMPLOYEE PERSONAL DATA

Employee personal data is confidential material and must be treated as such.

Recruitment & Employment
All recruitment and employment practices should follow the advice given in the Johnston Press Recruitment Tool Kit. Any applicant or employee personal data retained must be stored in a secure environment and accessed by only those authorised.

Sensitive Personal Data: Physical or Mental Health
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.

Details of an individual's medical history are classed as sensitive personal data under the Data Protection Act and must be processed according to the instructions detailed in the Company's Data Protection Policy which is number 1.14 of the Group Guidelines.

Sensitive personal data must be retained by HR only. Copies of documents containing sensitive personal data must not be stored in department. For the avoidance of doubt Illness Certification Forms and Sick Notes are to be treated as containing sensitive personal data and should be retained by the HR only. No copies should be retained by the Manager and/or kept in department.

Relevancy and Retention
Any applicant or employee personal data retained by the Company must be relevant for the purposes for which it was collected and not excessive. If there is any ambiguity as to what employee personal data should be retained in department and what should be stored with HR contact the Divisional HR Director or the Data Protection Compliance Officer. Retention of applicant and employee personal data must follow the advice given in the Johnston Press Recruitment Tool Kit. The Data Protection Act does not override any other statutory requirements to retain applicant and employee personal data for employment purposes.

Disclosure
Employee personal data must not be disclosed to anyone outside the Company unless the individual concerned has consented to such disclosure or the Data Protection Compliance Officer has given a specific instruction to do so. There are cases where the welfare of the employee may be in question and to obtain consent may not be possible. In such cases the Divisional HR Director must also be contacted in order to ensure that any personal data disclosed is done so in the interest of the employee and in accordance with relevant employment law.

Access
Details regarding an employee's right of access to their personal data can be found in the Company's Data Protection Policy which is number 1.14 of the Group Guidelines. Any employee wanting to request access should direct their application to the HR department.

The Company monitors its employees in a number of ways. Examples of this are card swipe access/exit systems, closed-circuit television, email traffic monitoring and Internet usage records. Employee monitoring data is highly confidential. Managers must not expect to be given access to this data purely due to their status. In the case of a disciplinary issue requests for access to monitoring data should be directed to the HR department. In the case of a request to access an employee's email in-box in order to retrieve crucial company related data this should be directed to the Group IT Helpdesk.

Destruction
All personal data must be treated as confidential information and shredded when no longer required. Under no circumstances should personal data be placed in waste bins or paper recycling points without firstly having been shredded. Tearing and/or burning should not be used as methods to destroy confidential information.

3. CONTACT

If you have a Data Protection enquiry please contact the Data Protection Compliance Officer:

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