Access to employees Data

Revised March 2013

Contents page

Access to Employee Data

The Wellbeing Residential Group aims to fulfil its obligations under the Data Protection Act 1998 to the fullest extent.

Procedure

1. Employees are allowed to have access to all personal data about them held under the Data Protection Act 1998 This Act requires the Wellbeing Residential Group to respond to requests for access to personal data within 40 days.
2. The Wellbeing Residential Group will send a copy of such personal data to each employee on 1st January of each year if requested to do so.
3. Employees are required to read this information carefully and inform Bob Dhaliwal at the earliest opportunity if they believe that any of their personal data are inaccurate or untrue, or if they are dissatisfied with the information in any way.
4. The Data Protection Act 1998 gives data subjects the right to have access to their personal data at reasonable intervals. The Wellbeing Residential Group believes that a copy of this information given annually will satisfy this requirement. Should employees request access to their personal data at any other time, the request must be addressed to Bob Dhaliwal at the head office address which is, **Wellbeing Care Group, 37 Wyndley Close, Four Oaks, Sutton Coldfield. B74 4JD**. The request will be judged in the light of the nature of the personal data and the frequency with which they are updated. The employee will then be informed whether or not the request is to be granted. If it is, the information will be provided within 40 days of the date of the request.
5. In the event of a disagreement between an employee and the Wellbeing Residential Group regarding personal data, the matter should be taken up under the Wellbeing Residential Group's formal grievance procedure.

Additional Clause(s)

1. Where employees make additional requests for access to their personal data which are granted, a fee of £10 will be charged which must be paid to Wellbeing Residential before a copy of the personal data will be given.
2. In the interests of openness and fairness, the Wellbeing Residential Group will provide copies of personal records held manually to employees on 1st January of each year. The procedure which applies to computerised data will apply to such manual files.

Computer Security

The Wellbeing Residential Group regards the integrity of its computer system as central to the success of the organisation. Its policy is to take any measures it considers necessary to ensure that all aspects of the system are fully protected.

Procedure

1. Overall computer security is the responsibility of the data security officer reporting to either Bob Dhaliwal or Keith Pang. Line managers are responsible for security within their own departments.
2. Job applicants will be questioned on their computer experience. The implications of their software knowledge will be discussed with the data security officer before a job offer is made. All references will be checked.
3. The credentials of all temporary, freelance and consultancy staff should be checked in as much detail as possible before they are allowed access to the computer system. Managers are responsible for ensuring that all such workers receive the information.
4. Computer training at every level will emphasise the importance of security. Staff will receive a detailed statement on the implications of the Data Protection Act 1998 and the Computer Misuse Act 1990.
5. Supervisors are responsible for ensuring that basic procedures are followed. Procedures may be bypassed only with the combined consent of the line manager and data security officer, and a written record must be kept.
6. Employees of all grades are permitted access only to those parts of the computer system which they need to enter in order to carry out their normal duties. Levels of access will be decided by line managers in conjunction with the data security officer who will ensure that levels of access are consistent throughout the organisation.
7. Employees may access the Internet but access to certain sites will be blocked.
8. All incoming emails will be monitored and scanned for viruses before being released to the recipient.
9. Employees with access to personal data are in a particularly sensitive position and must bear in mind at all times the provisions of the Data Protection Act.
10. Passwords must be used at all times and changed regularly. Employees should not select obvious passwords. All passwords must be kept confidential. Employees must not give their passwords to other members of staff or to any person outside the organisation.
11. When an employee leaves the organisation or moves to a different department all passwords in that department will be changed. When an employee is given a temporary password to a higher level of access than he or she normally uses, that password must be cancelled after the individual ceases to need it.
12. Supervisors are responsible for stipulating requirement for back-up operations in their own departments. Regular back-up must be carried out in accordance with departmental instructions.
13. All the Wellbeing Residential Groupôs software must be formally authorised by the data security officer. Regular checks will be made for viruses by the IT department.
14. No external software may be used without authorisation by both the data security officer and the employeeôs line manager.
15. No private work or computer game playing is permitted.
16. The safekeeping of CDs, DVDs and USBôs sent from external sources is the responsibility of the person to whom it was sent. All such CDs and DVDs must be checked for viruses by the IT department before use. CDs and DVDs generated internally must be kept in a secure place.
17. Misuse of computers is a serious disciplinary offence. The following are examples of misuse:
    1. fraud and theft
    2. system sabotage
    3. introduction of viruses, etc
    4. using unauthorised software
    5. obtaining unauthorised access
    6. using the system for private work or game playing
    7. breaches of the Data Protection Act
    8. sending abusive, rude or defamatory messages or statements about people or organisations, or posting such messages or statements on any websites or via e-mail
    9. attempting to access prohibited sites on the internet
    10. hacking
    11. breach of the organisationôs security procedures.

This list is not exhaustive. Depending on the circumstances of each case, misuse of the computer system may be considered gross misconduct. Please refer to the disciplinary rules and procedures. Misuse amounting to criminal conduct may be reported to the police.

18. Management, in consultation with specialist auditors, may institute confidential control techniques and safeguards. Financial systems are subject to special reconciliation processes.
19. A committee of senior managers will meet regularly to review computer security.
20. All breaches of computer security must be referred to Bob Dhaliwal or Keith Pang . Where a criminal offence may have been committed the board will decide whether to involve the police.
21. Any member of staff who suspects that a fellow employee (of whatever seniority) is abusing the computer system may speak in confidence to the HR manager.