DATA PROTECTION

Those employees, who have authorised access to personal data, should not use or disclose information in any manner that is incompatible with the purpose for which it is being held. Failure to abide by the above requirements may result in disciplinary action.

Compliance with the Data Protection Act 1998

Because the Association holds and processes information about individuals (employees, people in customer and supplier organisations, etc.) it falls within the scope of the 1998 Data Protection Act, and is registered as a 'Data Controller' under it.

The Act covers not only computerised data, but also manual records held in "relevant filing systems" (systems which are structured, and which allow for ordered retrieval, including card indexes).

This describes the key principles that impact employees in the normal course of their work. Some employees may have additional procedures that cover specialised activities, for example, management of mailing lists.

The 1998 Act distinguishes between what might be called ordinary personal data such as name, address and telephone numbers; and sensitive personal data including information relating to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life and criminal convictions. The processing of the latter type of data is subject to stricter conditions.

Principles of the Data Protection Act

The Act comprises eight principles that are summarised, to highlight aspects which will be most relevant to the Association's employees in the course of their normal activities. As such, this is not a definitive explanation of the Act in all circumstances.

The First Principle says that data shall be processed fairly and lawfully. In practice, this means that the data subject (the individual whose data is being processed) understands what data the Association holds and what the Association is doing with it, either because the subject has given their consent (this may be explicit or implied by not taking up an opportunity to 'opt-out') or because it is a necessary part of a business transaction. So, the Association could use a customer's name and address to process an order, but could not use those details for marketing purposes without consent for this extended use. In the case of sensitive personal data, the consent must be specific.

People contact the Association to request information of various types, such as membership data these requests should be forwarded to the Association Manager for their response. Data that the Association holds about people is not used for marketing purposes or to explicitly request money / donations. People who ask to stop receiving the Association information have their information deleted / destroyed.

The Second Principle says that data shall be obtained only for one or more specified and lawful purposes. Notification to the Information Commissioner (previously the Data Protection Registrar) requires the Association to state the purpose(s) that types of data will be used for.

Even if the Association holds data that would be useful for new purposes, the Association cannot use it in that way without making the data subjects aware and updating the notification that the Association sends to the Information Commissioner.

Data held by the Association is used for four specified purposes which are registered with the Information Commissioner's Office (and renewed annually) in accordance with the Data Protection Act 1998:

- *Staff administration*
- *Administration of membership records/training provision & CPD services*
- *Fundraising*
- *Realising the objectives of a charitable organisation*

The Third Principle requires that personal data shall be adequate, relevant and not excessive. In other words, the Association should not capture and hold information that does not have an identified use today

The information captured by the Association is determined by the nature of the initial enquiry. For example, someone who wishes to do a fundraising parachute jump for CRY may initially only have their postal address stored by the Association; whereas someone who has just suffered a bereavement may have full contact details and family medical history captured. In many cases, enquirers provide further information to the Association after their initial contact and this information will be stored in order to best address any current and future queries that person may have.

The Fourth Principle says that personal data shall be accurate, and *where necessary*, kept up to date. In practice, keeping data up to date will be far more important where employees' records are concerned than, for example, in the case of a marketing mailing list.

Data held by the Association about the Association supporters is kept up to date as and when the Association is informed about changes by data subjects themselves. This is to ensure that the Association supporters are provided with the information most relevant to their circumstances (e.g. with regards to bereavement; screening; fundraising; medical conditions; etc.); and to ensure that information is provided via the correct / preferred medium (e.g. postal address; e-mail address; etc.).

The Fifth Principle requires that personal data processed for any purpose(s) shall not be kept for longer than necessary for that purpose(s) so housekeeping becomes more important.

The Association retains data about its supporters until such time as a supporter requests to no longer be sent the Association information. The purpose of 'providing supporters with free information about the Association services and activities' is considered to have an indefinite length as it is not for the Association to decide when a CRY supporter has had 'enough' information. In the Association's experience, supporters – especially bereaved families – vary greatly in the amount of time they continue to require information and support from the Association. Once a supporter has instructed the Association that they no longer require information or support, data about that supporter will be destroyed (deleted from electronic records and any hardcopies shredded).

The Sixth Principle says that personal data shall be processed in accordance with the rights of the data subject under the Act. Data subjects are entitled to ask any Data Controller who may hold information about them for a copy of that information. In addition, they have rights which include:

- The right to prevent processing likely to cause damage or distress
- The right to prevent processing for the purposes of direct marketing
- The right to take action to rectify, block, erase or destroy inaccurate data

Data held by the Association is processed only for the four purposes outlined under the Second Principle (above). The Association supporters may at any time request copies of the data held about them; request further details of how their data are used; and request for any / all of their data to be amended, corrected or destroyed.

The Seventh Principle says that appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against its accidental loss or destruction. Compliance with our "Rules and Guidelines for Computer Users" is important in this respect.

The Association staff are aware that data held by the Association should not be copied or taken off site without the express permission of the Association Manager – and even then, only where doing so might be reasonably considered necessary in order to fulfil one of the four purposes for which the Association holds data. Under this principle, the Association staff who work away from the office may have remote access to data held by the Association – e.g. via a virtual personal network – on the understanding that data is not copied or stored off site. The Association staff are aware that deviating from this principle may constitute a serious case of Gross Misconduct, resulting in disciplinary measures up to and including dismissal. With regards to non-Association staff copying data from PCs in the office, the Association has a number of general office security measures (e.g. electronic entry system on the front door; PCs not easy to access without being noticed) which minimise the risks of opportunistic data theft.

The Eighth Principle prohibits the transfer of personal data to a country outside the European Economic Area unless that country has equivalent safeguards for the protection for the rights and freedom of data subjects and their personal data. This does not apply if the individual gives consent or where data protection conditions are embodied in a contract with the overseas organisation.

The Association's paperwork held by the Information Commissioner's Office stipulates that data held by the Association is never transferred outside the European Economic Area.

Compliance

All students must comply with the requirements of the Data Protection Act 1998. If an employee is uncertain how the Act affects them they should discuss it further with the Association Manager.

Data Processing

The Data Protection Act 1998 regulates the way in which certain information about the Association employees is held and used and the Association is registered in accordance with the Act.

Personal File Records

Students should be aware that relevant details, letters, notes, etc., appertaining to their enrolment with the Association, and other related matters, are retained in a confidential

personal file. The contents of the student's file will only be used for necessary business purposes and will not be disclosed to third parties (save for those to whom the Association have a statutory duty to disclose) without the student's express approval.

The student must inform the Association of any changes to their personal circumstances - e.g. name, address, next of kin etc.

Information Security

Information is a vital business asset. It forms the basis of day-to-day operations. It is the basis for informed decision making. Some information is sufficiently confidential that its disclosure to competitors, suppliers or customers could damage the business. Information relating to people may be sensitive and cause damage or distress if wrongly disclosed or lost.

The Association has a duty to safeguard:

Confidentiality - ensuring that information is accessible only to those authorised to have access
Integrity - safeguarding the accuracy and completeness of information and processing methods
Availability - ensuring that authorised users have access to when required

Responsibility

The Association Manager is responsible for the formulation and review of this policy and for providing resources for its effective implementation.

All members of staff are responsible for complying with this policy and any supporting procedures. Failure to do so may lead to disciplinary action that could include dismissal. Gaining unauthorised access to any computer system, whether owned by the Association or third parties, may constitute an offence under the Computer Misuse Act 1990, which is enacted in criminal law.

Principles

The Association will fully comply with all legal and contractual obligations, including, but not limited to, compliance with the Data Protection Act 1998; using only correctly licensed computer software and operating it in accordance with the terms of the license; complying with any non-disclosure agreements and respecting copyright and intellectual property rights.

Access to computer systems will be protected by a system of passwords or other authentication methods appropriate to the importance of the information held. Passwords are issued and must not be disclosed, shared (unless specifically authorised) or written down in a form in which they could be identified and used.

Computer files will be backed up regularly and the back-ups will be stored in a secure location.

Procedures and systems, including software, will be maintained to ensure that the risk of infection by computer viruses is minimised and that all possible steps have been taken, within the limits of reasonable cost, to prevent disclosure, loss or damage as a result of any hacking attack. Breaches, or suspected breaches, of this policy should be reported to the Association Manager who, in consultation with other members of CRY, will conduct an investigation and instigate appropriate remedial action.

Registration with the ICO Commission

As a ‘not for profit’ organisation, BVNA is exempt from being registered.

The British Veterinary Nursing Association
79 Greenway Business Centre, Harlow, Essex CM19 5QE Tel: 01279 408644 E-Mail: bvna@bvna.co.uk

Revised Nov2016