RICHARD HOUSE CHILDREN'S HOSPICE

Data Protection Policy

Scope of the policy

This policy applies to Richard House Children's Hospice. It applies to paid staff and volunteers.

Purpose of the policy

The purpose of this policy is to enable Richard House to:

- comply with the law in respect of the data it holds about individuals;
- follow good practice;
- protect Richard House's supporters, staff and other individuals;
- protect the organisation from the consequences of a breach of its responsibilities.

Policy Statement

Richard House will:

- comply with both the law and good practice
- respect individuals' rights
- be open and honest with individuals whose data is held
- provide training and support for staff and volunteers who handle personal data, so that they can act confidently and consistently

Richard House recognises that its first priority under the Data Protection Act is to avoid causing harm to individuals. In the main this means:

- keeping information securely in the right hands, and
- holding good quality information.

Secondly, the Act aims to ensure that the legitimate concerns of individuals about the ways in which their data may be used are taken into account. In addition to being open and transparent, Richard House will seek to give individuals as much choice as is possible and reasonable over what data is held and how it is used.

Mobile devices, such as smartphones and tablet computers, are important tools for the organisation and their use is supported to achieve business goals.

However mobile devices also represent a significant risk to information security and data security as, if the appropriate security applications and procedures are not applied, they can be a conduit for unauthorised access to the organisation's data and infrastructure. This can subsequently lead to data leakage and system infection.

Data Protection Policy

Richard House has a requirement to protect its information assets in order to safeguard its customers, intellectual property and reputation. This policy also outlines a set of practices and requirements for the safe use of mobile devices.

All mobile devices, whether owned by Richard House or owned by employees, that have access to corporate networks, data and systems, not including corporate IT-managed laptops. This includes smartphones and tablet computers. Exemptions: Where there is a business need to be exempted from this policy (too costly, too complex, adversely impacting other business requirements) a risk assessment must be conducted being authorised by a member of the Senior Management Team.

Technical requirements

- Devices must use the following Operating Systems: Android 2.2 or later, IOS 4.x or later and Windows mobile.
- Devices must store all user-saved passwords in an encrypted password store.
- Devices must be configured with a secure password that complies with Richard House's network password policy. This password must not be the same as any other credentials used within the organisation.
- With exception of those devices managed by IT, devices are not allowed to be connected directly to the internal corporate network.

User requirements

- Users must only load data essential to their role onto their mobile device(s).
- Users must report all lost or stolen devices to Finance and IT Officer or Director of Finance & Operations immediately.
- If a user suspects that unauthorised access to company data has taken place via a mobile device they must report the incident in accordance with Richard House's incident handling process.
- Devices must not be "jailbroken"* or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.
- Users must not load pirated software or illegal content onto their devices.
- Applications must only be installed from official platform-owned approved sources. Installation of codes from un-trusted sources is forbidden. If you are unsure if an application is from an approved

source contact Finance and IT Officer or Director of Finance & Operations.

- Devices must be kept up to date with manufacturer or network provided patches. As a minimum patches should be checked for weekly and applied at least once a month.
- Devices must not be connected to a PC which does not have up-to-date and enabled anti-malware protection and which does not comply with corporate policy.
- Devices must be encrypted in line with Richard House's compliance standards.
- Users must be cautious about the merging of personal and work email accounts on their devices. They must take particular care to ensure that company data is only sent through the corporate email system. If a user suspects that company data has been sent from a personal email account, either in body text or as an attachment, they must notify the Finance & IT Officer immediately.
- Users must not use corporate workstations to backup or synchronise device content such as media files unless such content is required for legitimate business purposes and has been authorised.

* To jailbreak a mobile device is to remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorised software.

Brief introduction to the Data Protection Act 1998

The Data Protection Act 1998 regulates the collection, storage, use and disclosure of information about individuals by organisations. Any organisation that keeps information about individuals must comply with the act.

The Act applies to *personal data* - information about identifiable living individuals that is:

- Held on computer or any other automated system
- Held in a *relevant filing system* (a paper system such as client records system, or a set of files on service users that is organised alphabetically by the name of the person or some other identifier such as case number)
- Intended to go onto computer or into a relevant filing system

Sensitive personal data is data which relates to an individual's political opinions, racial or ethnic origins, mental or physical health, sexual life, religious persuasion, trade union affiliation, or criminal record. The obligations

imposed on data controllers and data processors are more onerous for sensitive personal data than other personal data.

The Data Protection Act applies mainly to the Data Controller - the "person" who decides why and how personal data is processed. This "person" doesn't have to be an individual and in most cases will be an organisation. Individual members of staff or volunteers will merely be agents of the data controller.
Richard House is a data controller, the accountable person being the Director of Finance & Administration. Richard House has notified the Data Protection Commissioner that it processes personal data. The notifications cover:

- the purposes for which data is processed
- the data subjects
- the data classes
- the sources and disclosures, and
- the fact that data is not transferred outside the EEC

The full notification is available on a public register www.ico.gov.uk, but an extract is available on request from the Director of Finance & Administration, Richard House Children's Hospice, Richard House Drive, E16 3RG.

"Processing" is so widely defined that it may be assumed to cover everything you do with it – obtaining, recording, organising, using, disclosing or just simply holding it.

A "data processor" is someone, other than an employee of the data controller, who processes data on behalf of and at the direction of the data controller – examples would be a payroll bureau or a fulfillment house.

Data Protection Principles

The Act has eight Data Protection Principles:

1. Data processing must be 'fair' and legal
Richard House will always take reasonable steps to ensure that the data subject knows who the data controller is and the purpose(s) for which the data is to be used, giving the individual the opportunity to opt-out (a specific opt-in is required for sensitive personal data). Only where it is necessary for the legitimate interests of Richard House will it process information without the actual or implied consent of the individual. This might be where:

- it involves a criminal matter
- it is necessary to comply with a legal or contractual obligation
- it is demonstrably in the vital interests of the individual.

It is the responsibility of all Richard House staff that process personal data to ensure they do so fairly and lawfully.

2. You must obtain data only for specified purpose(s) and use it only in ways that are compatible with its purposes

It is the responsibility of all Richard House staff that process personal data to satisfy themselves their processing is for a notified purpose.

3. Data must be adequate, relevant and not excessive
It is the responsibility of all Richard House staff that process personal data to ensure the adequacy and relevancy of the data, and that it is not excessive.

4. Data must be accurate and up to date
It is the responsibility of all Richard House staff that process personal data to ensure that information is properly documented initially, and that it is kept up to date.

5. Data must not be held for longer than necessary
If the purpose for which the data was obtained no longer exists, the data must be erased. If staff want to keep it, then the individual must be asked for consent. The only exception to this is where the data is retained for research or statistical purposes only.

6. Data Subject's rights must be respected
Access must never be refused without the express written authority of the Chief Executive. A request for data to be rectified or erased must similarly never be refused without the express written authority of the Chief Executive.

7. You must have appropriate security
In terms of electronic data systems, this responsibility will be carried out by the Director of Finance & Administration All staff that control local electronic databases have a responsibility to ensure data is not unlawfully processed, disclosed or lost. Similarly all staff have an essential role in, and responsibility for, ensuring the physical security of paper files containing personal data. Personal data is not to be passed to an external body for processing, for example a fulfillment house or researcher, without the knowledge of the Director of Finance & Administration. It is the Director of Finance & Administration's responsibility to ensure that there is a written contract between Richard House and the data processor covering:

- the nature of the data,
- the purposes for which it is transferred and
- the measures to be taken by the processor to protect that data from unauthorized or unlawful disclosure or loss.

8. Special rules apply to the transfers abroad
As a matter of policy Richard House will not generally transfer personal data outside the UK. Any staff member who wishes to do so must seek prior written approval from the Chief Executive.

Rights of Data Subjects

Individuals on whom personal data is held have a number of rights. These include:

- a right of access to it ("subject access")
- a right to prevent processing where it is likely to cause substantial harm to the individual
- a right to prevent processing for direct marketing purposes
- a right to compensation if damage results from the data controller's contravention of the Act
- a right to have certain data rectified, blocked or erased

There are statutory exemptions relating to most of these rights. It is Richard House policy however to seek always to work within the spirit of the law, rather than mere legal compliance, and it will not exercise its right to exemption unnecessarily or inappropriately.

Subject Access Procedure

Individuals have a right to:

- a description of the data being processed
- a description of the purposes for which it is processed
- a description of any potential recipients
- any information held as to the source of the data

Data Controllers must provide this information within 40 days of a written request from an individual on whom data is held.

In certain circumstances individuals may be denied access rights for example where disclosure would necessitate the disclosure of another's personal data. The Chief Executive is to be informed of all applications from an individual for data access. The Data Controller may then respond positively to the request, but must not refuse access without the express authority of the Chief Executive. This policy rule ensures that accountability for potential non-compliance lies with the Data Controller, not the individual staff member.

Before responding positively to a request, the staff member must satisfy him/herself as to the identity of the data subject, and be specific about the database or paper file that has been searched to provide the disclosure.

You are allowed to charge for the access but Richard House will not charge unless significant administrative effort and/or a lot of photocopying is needed. It must not exceed £10.

Responsibility of Staff

All staff have a responsibility for:

- reviewing the contents of all files (paper and electronic) to ensure any personal data held complies with the eight principles
- reviewing application forms, employment contracts and referral documents to ensure that all information systems comply with the standards of fair practice and good procedure contained in the data protection principles
- informing data subjects of the identity of the Data Controller, the nature of the data held, the purpose for which it is held and the likely recipients of the data
- having regard to all relevant legislation in particular around any improper disclosure of intensely sensitive personal information. The Police Act 1997, the Protection of Vulnerable Children Act 1999, the Care Standards Act 2000 and the disclosure procedure operated by the Criminal Records Bureau and Codes of Practice place a heavy emphasis on the principles underlying the Data Protection Act and the Human Rights Act with regard to disclosures of criminal offences. Separate policies exist in this regard, but it is emphasised that any improper disclosure of such intensely sensitive personal information would be treated as a very serious disciplinary matter.

Offences

All staff should be aware that unlawfully obtaining personal data for a purpose not covered by the Notification is a criminal offence, and will be treated as a serious disciplinary offence.

The selling of unlawfully obtained personal data is a criminal offence, and is likely internally to be treated as gross misconduct, meriting summary dismissal.

Monitoring of Staff

The monitoring of the movements or actions of staff by CCTV or random checking of e-mails, websites used or telephones is covered by the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000.

Issues arising from e-mail and website monitoring are covered in Richard House policy on Information Systems Acceptable Use, which is made available to all staff as part of their induction. This policy document states that it is the charity's policy to randomly check e-mails and website use, and in some areas to undertake CCTV surveillance (restricted to overt surveillance of access to buildings) in order to protect itself against unlawful use or access.

Data from Third Parties

Where personal data is obtained from someone other than the data subject, that data subject must be informed that Richard House holds that information and the purpose for which it holds it. The only exception is where informing the data subject would involve a "disproportionate effort" on the part of the data controller.

All staff who maintain manual or electronic records containing such data must review it regularly, and ensure not only that explicit consent has been obtained to retain it, but that it really is necessary to keep it. If it is, then a process must be put in place to ensure that, from time to time, its accuracy is confirmed.

Provision of Employment References

Personal data covers opinions as well as facts and disclosure of both to a third party is a processing of personal data. The individual will therefore normally have a right of access to employment references received by, and given by, Richard House, and any giving of a reference has to be effected in accordance with the first data protection principle – that of 'fair' and legal processing.

References should therefore only be given where an employee has given prior consent. This will be done by the giving of an expressed consent as part of the Exit Interview procedure.

With regards to access to references, an employee is not legally entitled to demand access to a reference ***given*** by Richard House but s/he can demand it from the recipient of that reference, provided the identity of the author of the reference is removed.
Richard House policy in these circumstances is that as a "best practice" standard Richard House will allow access to confidential references it writes, unless to do so would result in harm to the author of the reference or some third party. In such a case the consent of that author/third party to the release should be sought.

Historical, Research or Statistical Purposes

There is a general exemption if data is processed for these purposes, provided the data was originally obtained fairly, for a lawful purpose.

In this case, further processing for research is not incompatible with the data protection principles, even though it is kept indefinitely. If the data identifies the individual, then that person can of course require access to it.

Communication & Training

All staff and volunteers will be made aware of this policy.