Information Security Policy Statement

Introduction

Information is a key resource for the Childhood Cancer Research Group, without which virtually all of our activities would cease. Our information includes: case, control, coding and incidence data; administrative, personnel, financial and funding data; computing network and database systems, methodology; analyses; publications and references. Information may exist in many forms: it may be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected.

The Childhood Cancer Research Group must endeavour to do all it can to protect its information assets in ways that are appropriate and effective. This will help enable the Childhood Cancer Research Group to fulfil its responsibilities and to enable our staff to continue their research and to provide information to other research groups.

Our ability to receive, develop, analyse and publish our information will enable us to maintain and improve our reputation and ensure that we meet our business and professional goals. In addition it will ensure that we do not lose opportunities for funding or our ability to receive data through a poor reputation for security.

Objective

Our security objective is to protect the Childhood Cancer Research Group from security problems that might have an adverse effect on our operations and our professional standing.

Security problems can include confidentiality (people obtaining or disclosing information inappropriately), integrity (information being altered or erroneously validated, whether deliberate or accidental) and availability (information not being available when it is required). A wide definition of security will be used to include all types of incident that pose a threat to the effective use of information. This includes performance, consistency, reliability, accuracy and timeliness.

Principles

Approach

We will:

Use all reasonable, appropriate, practical and effective security measures to protect our important processes and assets in order to achieve our security objective.

Utilise BS7799: Code of Practice for Information Security Management as a framework for guiding our approach to managing security.

Continually review our use of security measures so that we can improve the way in which we protect our business.

Protect and manage our information assets to enable us to meet our contractual, legislative, privacy and ethical responsibilities. As a publicly funded organisation we are aware of the need to provide value for money and be aware of public opinion.

Responsibilities

All staff, past and present, permanent, honorary and temporary, of the Childhood Cancer Research Group have an obligation to protect our information assets, systems and infrastructure. They will, at all times, act in a responsible, professional and security-aware way, maintaining an awareness of and conformance to this Policy.

Everyone will respect the information assets of third parties whether or not such protection is required contractually, legally or ethically.

All members of the Childhood Cancer Research Group are responsible for identifying security shortfalls in our existing security practices and/or improvements that could be made. These should be reported to the Security Steering Group.

All members who have supervisory responsibility are required to actively promote best practice amongst their staff.

The Director of the Childhood Cancer Research Group has ultimate responsibility for ensuring that information within the Childhood Cancer Research Group is adequately protected. The Director will delegate responsibility for approving and reviewing access rights to information to named, responsible individuals.

The Director of the Childhood Cancer Research Group is responsible for ensuring that our security objective is achieved. The Security Steering Group is authorised by the Director to pursue appropriate activities and actions that contribute to achieving our security objective and that are consistent with this Information Security Policy.

The Director of the Childhood Cancer Research Group is responsible for allocating sufficient resources so that the Childhood Cancer Research Group can realistically achieve its security objective. This includes people, time, equipment, software, education and access to external sources of information and knowledge.

Practices

We will identify our security risks and their relative priorities, responding to them promptly and implementing safeguards that are appropriate, effective, culturally acceptable and practical.

All members of Childhood Cancer Research Group will be responsible for their actions with regard to information security.

All information (including third party information) will be protected by security controls and handling procedures appropriate to its confidentiality, sensitivity and criticality.

When needed, information will be made available outside of the Childhood Cancer Research Group to other research groups. Information owners will be responsible for identifying and recording to whom their information may be released.

The Childhood Cancer Research Group will ensure that its activities can continue with minimal disruption, or other adverse impact, should it suffer any form of disruption or security incident.

Actual or suspected security incidents will be reported promptly to the Security Steering Group, who will manage the incident, and arrange for an analysis of the incident and consequent lessons to be learnt.

Documented procedures and standards, along with education and training, will support these Principles and the Practices to which they give rise.

Compliance with the Policy will be monitored on a regular basis by the Security Steering Group which will meet on a regular basis.

The Director of the Childhood Cancer Research Group owns this Information Security Policy and is committed to the implementation of it. He or she will facilitate an annual review of it by the Security Steering Group. It will be reviewed for completeness, effectiveness and usability. Effectiveness will be measured by the Childhood Cancer Research Group’s ability to avoid security incidents and minimise resulting impacts.

The Director of the Childhood Cancer Research Group will sign off all new versions of the Information Security Policy. All members of the Childhood Cancer Research Group are

responsible for identifying ways in which the Information Security Policy might be improved. Suggestions for improvement should be sent to the Security Steering Group. If immediate changes are required a special meeting of the security group will be called, otherwise suggestions will be discussed at the meeting to conduct the annual review of the Policy.

Policy Awareness

A copy of this Policy will be made available to all staff currently employed, or when they join the Childhood Cancer Research Group. Individual sections of the Policy will be updated as required and will be available on the Childhood Cancer Research Group's Intranet site. All members of the Childhood Cancer Research Group are expected to be familiar with, and to comply with, the Information Security Policy at all times. The members of the Security Steering Group will, in the first instance, be responsible for interpretation and clarification of the Information Security Policy. Staff requiring further information on any aspects of this Policy should discuss their needs with a member of the Security Steering Group.

Applicability and Enforcement

This Policy applies to all members of the Childhood Cancer Research Group and those who use its facilities and information. Compliance with the Policy will form part of the contractual agreements.

Failure to comply with the Information Security Policy could harm the ability of the Childhood Cancer Research Group to achieve its aims and security objectives and could damage the professional reputation of the organisation. Failure to comply will, in the ultimate sanction, be treated as a disciplinary matter. The Director of the Childhood Cancer Research Group will be responsible for all decisions regarding the enforcement of this policy, utilising the disciplinary procedures at his or her disposal as appropriate.

The Childhood Cancer Research Group will encourage the adoption and use of this Information Security Policy by third parties cooperating in joint ventures.

Mike Murphy, Director of the Childhood Cancer Research Group