Data Protection Policy

21st October 2017

Introduction

This is a statement of the data protection policy adopted by Crohns & Colitis UK to recognise its duty to protect the personal information of service users, members, supporters, current, past and prospective employees and others with whom we communicate.

In order to operate effectively and efficiently Crohn's and Colitis UK needs to collect and use information about the people with whom we work and receives personal and sensitive[1] data from individuals which may include details such as: name; address; date of birth; occupation; illness and date of diagnosis; ethnicity; donation and volunteering history.

Crohn's & Colitis UK understands that it is the custodian of personal information and the importance of handling personal information securely, appropriately and in compliance with the law. It fully endorses the legal principles relating to Data Protection and In order to meet the consent requirements of the EU General Data Protection Regulations we will undertake work – a transition period – to meet the requirements of the GDPR due to come into force on 25th May 2018.

Crohn's and Colitis UK is registered as a data controller on the register kept by the Information Commissioner.

This data protection policy ensures that Crohn's and Colitis UK:

- Complies with data protection law and follows good practice;
- Protects the rights of service users, members, supporters, current, past and prospective employees;
- Is open about how it stores and processes individuals' data;
- Protects itself from the risks of a data breach.

Data Protection law

The **Data Protection Act 1988** creates eight principles saying that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

[1] Personal data *relates to* a living individual and allows that individual to be *identified* from that information. Sensitive data can include health, ethnicity, criminal, political and other similar information.

The Privacy and Electronic Communications (EC) Regulation 2003 (last updated 2015) introduced direct marketing "opt in" to legislation and the right to privacy in modern communication methods e.g. text, cookies etc.

The EU General Data Protection Regulation 2016 that comes into force 25th May 2018; places a greater emphasis on accountability and transparency when handling personal information. It includes providing individuals with greater control and rights over how organisations handle their personal information; for example: limits on the use of automated processing of data to make decisions; tightens deletion and transfer rules including the right to be forgotten; and requires notification if data is compromised in certain circumstances

Scope

The Policy applies to all employees (permanent or temporary) and volunteers who access or use personal data for which Crohn's & Colitis UK is responsible for as a Data Controller.

Crohn's and Colitis UK has a wholly-owned subsidiary trading company called NACC Merchandise Limited. Personal data received in relation to Crohn's and Colitis UK activities is used for merchandise mailings.

Crohn's and Colitis UK contracts with the following third party suppliers:

1. Commercial mailing houses for distributing Crohn's and Colitis UK newsletters, questionnaires and subscription mailings which are too large to be sent from the Crohn's and Colitis UK office. These do not hold data on a permanent basis but process it for the relevant mailings.
2. An external company to maintain its website and some personal data (name, address, age, etc) may be held in a database on the computer which runs the Crohn's and Colitis Website.
3. The Crohn's and Colitis UK database and Crohn's and Colitis UK computer system can require maintenance support from supplier companies.

Crohn's and Colitis UK does not provide data to any other organisation (except for statutory purposes relating to employment) and does not exchange mailing lists with other charities or companies.

The current and future use of contractors, suppliers or third parties – as outlined above and, for example, the outsourcing of a service or the use of temporary or agency staff – will be managed via our use of contracts with specific data protection clauses that impose confidentiality obligations on them and their staff in relation to Crohn's and Colitis UK data.

Data protection risks

Crohn's and Colitis UK recognises a number of data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, where consent is required, individuals should be free to choose how the company uses data relating to them and are informed what those choices mean.

- **Reputational damage.** For instance, the charity could suffer if hackers successfully gained access to sensitive data.

The Policy will enable the charity to mitigate those risks by demonstrating:

- how important the management of personal information is to the organisation;
- that reasonable steps are being taken to meet legitimate expectations of confidentiality and privacy, and to reduce the risk of substantial distress or financial damage being caused to individuals;
- good governance to reduce the risk of damage to Crohn's & Colitis UK reputation and the goodwill and trust individuals have in the charity;
- how Crohn's & Colitis UK will achieve compliance with the data protection principles – by defining what is authorised and lawful so those who handle personal data when working for Crohn's & Colitis UK will know what is expected of them and where to go for further guidance.

Responsibilities

Everyone who works for or with Crohn's & Colitis UK has some responsibility for ensuring data is collected, stored and handled appropriately. Each team must ensure that personal data is handled and processed in line with this policy and data protection principles.

However, the following roles have key areas of responsibility:

- The **Board of Trustees/Directors** is ultimately responsible for ensuring that Crohn's & Colitis UK meets its legal obligations.
- The **Chief Executive,** is responsible for:
    - Ensuring organisational compliance with the law and this policy;
    - Ensuring that supporting procedures and management policies are in place;
    - Taking any proposed changes to this policy to the Board for approval via the Governance Sub Committee;
    - Reporting to the Board at least annually on the effectiveness of this policy via the Governance Sub Committee;
    - Immediately informing the Board of any serious compromises of data.
- Crohn's and Colitis UK will nominate a **Data Protection Compliance Lead. This will be the Director of Finance and Corporate Services. They are** responsible for:
    - Keeping the Chief Executive updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advice for employees and volunteers.
    - Handling data protection questions from staff and volunteers.
    - Managing the process for handling requests from individuals to see the data Crohn's & Colitis UK holds about them (also called 'subject access requests').
    - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Performing regular checks and scans to ensure security hardware and software is functioning properly.

    - Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services or direct marketing agencies.
    - Managing the process that ensures personal information is retained only for as long as necessary for the purposes of Crohn's and Colitis.

- The **Director of Income Generation,** is responsible for:
    - Ensuring that any approaches made to supporters or potential supporters are only made to those who have consented to be approached for that purpose;
    - Ensuring consistent practices and procedures across the organisation on handling personal data held on databases managing supporters or potential supporters.
    - Approving any data protection statements attached to supporter communications such as emails and letters.
    - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles and privacy regulations.

- The **Director of Marketing, Communications and Membership,** is responsible for:
    - In consultation with the Data Protection Compliance Lead, addressing any data protection queries from journalists or media outlets like newspapers.

- The **Senior Leadership Team** is responsible for:
    - everyone managing and handling personal information understanding that they are responsible for following good data protection practice
    - this policy being available to each member of staff
    - everyone managing and handling personal information being appropriately trained and supervised
    - ensuring queries about handling personal information are promptly and courteously dealt with and clear information is available to all staff
    - ensuring that the requirements of this Policy are incorporated into the Crohn's & Colitis UK operational procedures and contractual arrangements
    - advising the Governance Officer of approvals of all procedures, processes and supporting policies and proposed changes to the overall policy

- **All staff, and Volunteers who are members of organising teams** are responsible for managing and handling personal information in accordance with this Policy and the associated policies and procedures. They are responsible for following good data protection practice and they must:
    - be aware of the requirements of the Act and how the rules apply to them particularly in leadership roles;
    - complete data protection induction and annual training to suit their roles;
    - take responsibility for ensuring that they respect confidential information in their possession and maintain information security. Disclosure of confidential information gained as part of their role to a third party, or assisting others in disclosure, may be viewed by Crohn's and Colitis UK as a fundamental breach of trust.

Review and reporting

Crohn's & Colitis UK undertake to review the Policy and the latest best practice:

- at least every 12 months
- during planning for organisational change
- in the event of legislative change
- in the event of case law and/or updated regulatory guidance.

The review will be undertaken by the Data Protection Compliance Lead (DPCL) and agreed by SLT. Requests for amendments, clarifications or additions should be made to the DPCL for consideration.

The review and any agreed recommendations will be reported to the Governance Sub-Committee of the Board of Trustees who will decide whether any further action is needed at Board level. The review will include a report on any Data Protection incidents since the previous review including action taken and learning utilised.

In the event of a major Data Protection breach – for example, where the DPCL considers it likely that the breach will need reporting to the ICO and/or the individual's affected - the DPCL will imediately:

- inform the CEO and Chairman
- take steps to mitigate risks
- start an investigation.

In the absence of the DPCL (due to leave etc.) the CEO will carry out this function or appoint an appropriate temporary substitute.

_____

Sue Cherrie, Chairman - 21st October 2017

Associated policies and procedures to be maintained by the Senior Leadership Team:

Management Commitment Statement
Schedule of additional material and support documents
Acceptable Use Policy
Access Control Policy
Information Retention and Disposal Policy
Offsite Working and Removable Media Policy
Password Policy
Privacy Impact Assessments
Backup and Business Continuity Procedures
Clear desk, clear screen and secure waste Policy
Sharing Personal Information including Subject Access Requests Policy
Physical Security Policy
Information Security Incident procedure
Training programmes and attendance records