CHURCHTOWN INSTITUTE
Beauty & Hair College

Data Protection Policy

February 2018

CHURCHTOWN INSTITUTE
Beauty & Hair College

Contents

CHURCHTOWN INSTITUTE
Beauty & Hair College

1. Introduction

Churchtown Institute takes its responsibilities with regard to the management of the requirements of the Data Protection Act 1988 & 2003, and subsequent amendments, very seriously. This document provides the policy framework through which this effective management can be achieved and audited

Churchtown Institute recognise that in order to carry out our services, we must collect personal data relating to the usage of our systems by our clients and their users

"Personal data" means any information relating to a living individual from which that individual may be identified (including, for example, their name or address)

Churchtown Institute will manage any personal data in accordance with the Data Protection Act 1988 & 2003 and other related legislation, in whichever manner that such data is collected, recorded or used (whether on paper, databases, emails, CCTV or telephone records, or recorded by any other means)

2. Scope

The purpose of this policy is to ensure that Churchtown Institute and its staff comply with the provisions of the Data Protection Act 1988 & 2003 when processing personal and sensitive data Any infringement of the Act will be treated seriously by Churchtown Institute and may be considered under disciplinary procedures

Churchtown Institute follow the eight data protection principles set out in the Data Protection Act 1988 & 2003 and understands its obligations to ensure that personal data is managed fairly, lawfully, accurately and securely These principles require that personal data shall:

- be processed fairly and lawfully;
- be processed for limited purposes:
- be adequate, relevant and not excessive:
- be accurate and up-to-date:
- not be kept for longer than is necessary:
- be processed in line with the rights of data subjects:
- be processed securely;
- not be transferred to a country or territory outside the European Economic Area without adequate safeguards

Our approach to data protection is one of sensible risk management which is driven by our core values as listed below

- **Together we talk listen and lead:** We act with courage and openness to create shared solutions
- **What have we done today to makes us feel proud?** We innovate and improve through our passion for excellence and relationships
- **Trust me to run with it** We have freedom, empowerment and ownership to get a great Job done
- **We grow great people** We achieve success by valuing, supporting and investing in colleagues and customers.
- **Together we complete the puzzle** We reach out across boundaries to support and collaborate
- **Our Community** We are welcoming, creative and vibrant, achieving great things for our customers and beneficiaries

3. Company Responsibilities

Churchtown Institute recognises its corporate responsibility under the Act and is the data controller The Data Protection Officer is responsible for data protection compliance and is required to draw up guidance and promote compliance with this policy in such a way as to ensure the easy, appropriate and timely retrieval of information

The Data Protection Officer has access to all relevant documents relating to a legal compliance request and in conjunction with the CTO and appropriate members of the Management team, will make decisions regarding what information is released or exempted

All new members of staff should receive an introductory briefing on the Data Protection Act as part of their induction (See Appendix I)

4. Staff Responsibilities

All staff, particularly those engaged in the access or processing of personal information about learners, centre contacts, other staff members or other individuals must comply with the requirements of this Policy

Staff must ensure that

- all personal information entrusted to them in the course of their employment is kept securely:
- no personal information is disclosed either verbally or in writing, accidentally or otherwise to any unauthorised third party:
- where they are unsure about authorised third parties to whom they can legitimately disclose personal/sensitive data they seek advice from their line manager or the Data Protection Officer

Any deliberate infringement of the Act will be treated seriously by Churchtown Institute and may be considered under disciplinary proceedings

5. Contractor/Casual Staff Responsibilities

Churchtown Institute is responsible for the use made of personal data by anyone working on its behalf Managers who engage contractors or employ casual staff must ensure that

- any personal data collected or processed during work undertaken for Churchtown Institute is kept securely and confidentially This applies equally to where the data is an integral part of the work, or where it is contained on media, etc. which is accessed and applies whether or not Churchtown Institute has made specific mention of the data in the contract for work/services:
- all personal data is returned to the Churchtown Institute on completion of the work, including any copies that may have been made Alternatively that the data is securely destroyed, and Churchtown Institute receives notification in this regard from the contractor or casual member of staff;
- Churchtown Institute receives details of any disclosure of personal data to any other organisation or any person who is not a direct employee of the contractor:
- any personal data made available by Churchtown Institute or collected in the course of the work, is neither stored nor processed outside the UK without formal written consent from Churchtown Institute:
- all practical and reasonable steps are taken to ensure that contractors, short term or other casual staff do not have access to any personal data beyond what is essential for the work to be carried out properly

6. Subject Access Requests

Churchtown Institute is required to permit individuals to access their own personal data held by Churchtown Institute via a Subject Access Request Any individual wishing to exercise this right should do so in writing to the Data Protection Officer and a charge may be made for this request

Churchtown Institute aims to comply with requests for access to personal information as quickly as possible but will ensure that it is provided within the time limits set down by the Data Protection Act

Individuals will not be entitled to access information to which any of the exemptions in the Act applies. However, only those specific pieces of information to which the exemption applies will be withheld, and information covered by an exemption will be subject to review by the Data Protection Officer

7. Personal Data Systems

The ICT Department will maintain a register of all electronic systems which include personal and sensitive data held within Churchtown Institute

8. Charges

Churchtown Institute currently charges €30 to make a subject access request, however, Churchtown Institute reserves the right to review this fee at any time

9. Data Security Breach

Any breach of the Data Protection Act and the requirements of this Policy should be reported to the Data Protection Officer as soon as possible

A report of a suspected breach of the Act will be dealt with in accordance with the Churchtown Institute complaints procedure

10. Complaints

The Data Protection Officer will co-ordinate any complaints received in respect of this policy. The complaint should be addressed to the Data Protection Officer in the first instance. Complaints will be acknowledged immediately and every reasonable effort will be made to offer a comprehensive reply within 21 days

If the applicant is not satisfied with the reply, then they should inform the Data Protection Officer within 21 days The complaint will then be forwarded to the Director of Operations and will be dealt with in accordance with Churchtown Institutes General Complaints Procedure or the Churchtown Institute Grievance Procedure as appropriate

If applicants are dissatisfied with the outcome of the Complaints Procedure they may seek an independent review from the Information Commissioner, Requests for review by the Information Commissioner should be made in writing to

Office of the Information Commissioner, 18 Lower Leeson Street, Dublin 2, D02 HE97.

11. Data Encryption

Churchtown institute has a legal obligation to protect personal information and is aware of its legal obligations under the current Data Protection Legislation. For more information visit the website of the information commissioner's office (http://www.oic.ie/)

To comply with our Data Protection responsibilities and to ensure a common approach to data transfer across the organisation, the following procedure should be adopted to cover the transmission of ALL data from Churchtown Institute to other stakeholders.

11.1 Our Responsibilities

We have an obligation to provide data (in an approved and documented format) to our quality assurance and certification regulators. These reports are produced (normally per qualification) and submitted as needed, for example assessment results, withdrawals, deferrals etc.

11.2 Types of Data

Our data mainly falls into the category of Learner Sensitive Data.

11.2.1 Learner Data

VTCT No.	Forename	Surname	ULN	DOB	Grade	Nationality	Qualification

In the example above – should a data request include one or more of the items highlighted, the data is 'sensitive' and needs to be transmitted in a secure way. It must not be sent via email without encryption.

12. Contacts

General enquiries regarding Churchtown Institutes policy and approach to management and compliance with the Data Protection legislation may, in the first instance, be addressed to the office administrator – info@cibht.ie or by phone to our main switchboard – 014586603

More specific enquires and complaints should be addressed to:

Aiden Kelly
Head of Department
Churchtown Institute
CMG House
Earlscourt Industrial Estate
Beaumont Avenue
Churchtown
D14 XR80

13. Related Documents

This document should be read in conjunction with Churchtown Institutes Policies & Procedures.

14. Appendix 1: Good practice in information handling:

14.1 Data security do's and don'ts

This guide has been written for all Churchtown Institute staff who collect, manage, transfer or use data about learners, staff or other individuals during the course of their work. Its aim is to raise awareness of where potential breaches of security could occur.
Following these guidelines will help you to prevent data from being lost or used in a way which may cause individuals harm or distress and/or prevent the loss of reputation Churchtown Institute might suffer if you lose personal data about individuals.

14.2 Your roles and responsibilities

As an employee/subcontractor of Churchtown Institute you have a shared responsibility to secure any sensitive data you use in your day-today professional duties.

14.3 Why protect information?

Churchtown Institute holds personal data on learners, staff and other people in the course of its daily business activities. Some of this data could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of personal data could result in adverse media coverage, and potentially damage the reputation of Churchtown Institute. This can make it more difficult for Churchtown Institute to use new technology to benefit learners.

14.4 What information do you need to protect?

You should secure any personal data you hold about individuals and any data that is deemed sensitive or valuable to Churchtown Institute – see page 4 of this document. As with any organisation, Churchtown Institute has a Data Protection Officer. This falls within the remit of the Office Administrator who has responsibility for working out exactly what information needs to be secured, how information is securely handled, how the information changes over time, who else is able to use it and why.

14.5 Steps you can take to help prevent security problems.

There are plenty of things that you should do (or not do) that will greatly reduce the risks of sensitive information going missing or being obtained illegally. Many of these guidelines will apply to how you handle your own personal information. Using these practices will help you to protect your own privacy.

14.5.1 When working online

Do:

- Make sure you follow Churchtown Institutes policies on keeping your PC9s) up to dt with the lates security updates and make sure that you keep any computers you own up to date. Get advice from ICT if you need help.
- Only visit websites that are allowed by Churchtown Institute. Remember Churchtown Institute reserves the right to monitor websites which staff are visiting.
- Turn on relevant security warnings in your web browser (for example, the automatic phishing filter available in Internet Explorer)
- Make sure that you only install software that ICT Support has checked and approved and only download files or programs from sources that you trust. If in doubt, talk to ICT Support

14.5.2 Email and messaging

Do:

- Report any phising emails to the organisation they are supposedly from.
- Ensure you use the Churchtown Institute contact address book contained within the CRM. This helps to prevent the email being sent to the wrong address

Don't:

- Click on links in unsolicited emails. Be especially wary of emails requesting or asking you to confirm any personal information, such as password, bank details and so on.
- Turn off any email security measures that ICT support has put in place or recommended.
- Email sensitive information unless you know its encrypted. Talk to ICT Support for advice.
- Try to bypass Churchtown Institutes security measures to access your email off-site (for example forwarding email to a personal account)
- Reply to chain emails

14.5.3 Passwords

Do:

- Use a strong password (strong passwords are usually eight characters or more and contain upper and lower case letters as well as numbers and symbols)
- Make your password easy to remember but hard to guess.
- Change your passwords if you think someone may have found out what they are, in any event, change them at lease every three months.

Don't:

- Share your passwords with anyone else
- Write your passwords down
- Use your work passwords for your own personal online accounts
- Save passwords in web browsers if offered to do so.

14.5.4 Laptops/PCs

Do:

- Shut down your PC/Laptop using the 'Shut Down' or 'Turn Off' option
- Try to prevent people from watching you enter passwords or view sensitive information
- Turn off and store your laptop securely (if travelling use your hotels safe)
- Lock your desktop/laptop when leaving it unattended.
- Make sure your PC/Laptop is protected with encryption software.

Don't:

- Use public wireless hotspots – they are not secure.
- Leave your laptop in your car. If this is unavoidable, temporarily lock it out of sight in the boot.
- Let unauthorised people use your laptop
- Use hibernate or standby.

14.5.5 Sending and Sharing

Do:

- Be aware of who you are allowed to share information with. Check with the Office Administrator if not sure.
- Ask third parties how they will protect sensitive information once it has been passed on to them.
- Encrypt all removable media (e.g. USB sticks, CDs, portable drives) taken outside of premises

14.5.6 Churchtown Institute or sent by post/courier.

Do:

- Lock sensitive information away when left unattended.

Don't:

- Send sensitive information (even if encrypted) on removable media if secure remote access is available.
- Send sensitive information by email unless it is encrypted.
- Assume that third-party organisations know how your information should be protected.

14.5.7 When working off-site.

Do:

- Wherever possible access data remotely instead of taking it off-site.
- Make sure you sign out completely from any services you have used.
- Try to reduce the risk of people looking at what you are working with.
- If taking your laptop abroad on business, check if the country you are visiting has restrictions on encryption technologies.

Don't:

- Take information off-site that you are not authorised to.
- Leave your laptop, portable devices etc unattended.
- Attempt to access Churchtown Institute network/portals on equipment not owned/virus checked by Churchtown Institute.