Data Protection Policy

Context and Overview

Key details

- Policy prepared by: Aaron J. Simon, Vice President
- Approved by: Ronnie L. Williams, President/CEO
- Last policy review date: March 18, 2015

Introduction

Camelot College needs to gather and use certain information about individuals during the employment, enrollment, educational and financial aid processing periods.

This can include personal and identifiable information from students, parents/guardians, employees, vendors and/or other people that Camelot College has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards and to comply with the law.

Why this policy exists

This data protection policy ensures Camelot College:

- Complies with data security regulations and follows good practice
- Protects the rights of staff, students and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Information Security

Information Security regulations require that Institutions, including Camelot College, safeguard data when collecting, handling and storing personal information.

This applies regardless of whether data is stored electronically, on paper or on other materials.

To comply with regulations, personal information must be collected and used fairly, stored safely and not disclosed unlawfully. To ensure compliance, Camelot College has adopted the following principles regarding Information Security and data received. All personal data must:

1. Be processed and handled 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 institution without the adequate permission and level of protection.

People, Risks and Responsibilities

Policy Scope

This policy applies to:

- The Executive office of Camelot College
- All branches of Camelot College
- All staff, students and volunteers of Camelot College
- All contractors, suppliers, vendors, third-party servicers and other people working on behalf of Camelot College

It applies to all data that the company holds relating to identifiable information which may include but is not limited to:

- Names of individuals/references

- Social Security Cards/Numbers
- Drivers License Information
- Postal Addresses
- Email Addresses
- Telephone Numbers
- Any other information relating to individuals

Data Protection Risks

This policy helps to protect Camelot College from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for of with Camelot College has some responsibility for ensuring data is collected, stored and handled appropriately.

Each department that handles personal data must ensure that it is handled and processed in line with this policy and protection principles.

However, these people have key areas of responsibility:

- The **President/CEO** is ultimately responsible for ensuring that Camelot College meets its legal obligations.
- The **Data Protection Officer, Aaron Simon,** is responsible for:
    - Keeping the President/CEO updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies.
    - Arranging data protection training and guidance for the people affected by this policy.
    - Handling data protection questions from staff and anyone else affected by this policy.

    - Dealing with requests from individuals to see the data Camelot College holds about them.
    - Checking and reviewing any contracts or agreements with third parties that may handle the company's sensitive date.
- The **IT Manager, Aaron Simon,** is responsible for:
    - 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 that stores data on behalf of Camelot College.
- The **Marketing Manager, Pastor Ronnie L. Williams,** is responsible for:
    - Approving any data protection statements attached to communications such as emails and letters
    - Addressing any data protection queries from journalists or media outlets like newspapers.
    - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

General Staff Guidelines

- The only people able to access data covered by this policy should be those who **need it for their work.**
- Data **should not be shared informally.** When access to confidential information is required, employees must be gain approval from departmental managers.
- **Camelot College will provide training** to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below:
    - In particular, **strong passwords must be used** and they should never be shared with anyone other than the President/CEO and Data Protection Officer.
    - Personal data **should not be disclosed** to unauthorized people, either within the company or externally.
    - Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be depleted and disposed of.
    - Employees **should request help** from their President/CEO or Data Protection Officer if they are unsure about any aspect of data protection.

Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the President/CEO or Data Protection Officer.

When data is **stored on paper,** it should be kept in a secure place where unauthorized people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet.**
- Employees should make sure paper and printouts are **not left where unauthorized people could see them,** like on a printer or face up on their desk.
- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically,** it must be protected from unauthorized access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers,** and should only be uploaded to an **approved cloud backup service,** approved by the President/CEO.
- Data should be **backed up frequently.** Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should **never be saved directly** to non-company laptops or other mobile devices like tablets or smart phones.
- Company laptops should **never be removed from the premises** without prior approval from the President/CEO.
- All servers and computers containing data should be protected by **approved security software and a firewall.**

Data Use

Personal data is only used by Camelot College to conduct the business of the college. However, It is when personal data is accessed and used inappropriately that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally.** In particular, it should never be sent by unsecure, unencrypted email.
- Data must be **encrypted before being transferred electronically.** The IT manager can explain how to send data to authorized external contacts.
- Personal data should **never be transferred outside of the institution** without prior permission from the President/CEO and with the adequate level of protection.
- Employees **should never save copies of personal data to their own computers and or removable drives.**

Data Accuracy

We at Camelot College place a high level of emphasis on ensuring that personal data is accurate and correct.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary.** Staff should not create any unnecessary additional data sets.
- Staff should **take every opportunity to ensure data is updated.** For instance, by confirming a student's details when they call.
- Data should be **updated as inaccuracies are discovered.** For instance, if a customer can no longer be reached on their stored telephone number, it should be removed or updated in the database.

Subject Access Requests

All individuals who are the subject of personal data held by Camelot College are entitled to:

- Ask **what information** the company holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date.**
- Be informed how the company is **meeting its data protection obligations.**

If an individual contacts Camelot College requesting this information, this is called a Data Access Request.

Data Access Requests from individuals should be made in writing to Camelot College, 2618 Wooddale Blvd, Ste A, Baton Rouge, LA 70805 or via email at datarequest@camelotcollege.com. The data controller can supply a standard request form, although individuals do not have to use this. Data Access Requests are reviewed by the President/CEO and Data Protection Officer to ensure timely and appropriate delivery of requests. Contact information must be provided on all requests to ensure proper verification of the identity of anyone making a Data Access Request.

Disclosing Data for Other Reasons

In certain circumstances, this policy will allow personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Camelot College will disclose requested data. However, the President/CEO and/or Data Protection Officer will ensure the request is legitimate, seeking assistance from the company's legal advisers where necessary.

This policy is also viewable via our website at the following address:
http://www.camelotcollege.com/downloads/dataprotectionpolicy.pdf

Employee Disclosure

I _____understand and agree to comply with the Data Protection Policy. I also understand if I knowingly participate in the unauthorized illegal use of personal data that I will be terminated from Camelot College immediately and subject to any state and/or federal prosecution as a result of my actions.

_____ _____

Employee Signature **Date**

_____

Employee Name (Please Print)