University Campus St Albans

Cyber Security Policy

2021/22

Effective Date: 1st August 2021 – 31st July 2022

UNIVERSITY CAMPUS ST ALBANS CYBER SECURITY AND DATA PROTECTION POLICY

POLICY STATEMENT

University Campus St Albans (UCSA) recognises and accepts its responsibility to protect and safeguard all confidential data and take actions to that minimise the risks of cyber-attack.

UCSA deploys IT systems operated by both the two shareholders who have the specialist expertise and resources ie Oaklands College and the University of Hertfordshire. All staff are required to comply with the policies of the relevant institutions in order to protect confidentiality and data.

STATEMENT OF ORGANISATION FOR IMPLEMENTING THE CYBER SECURITY POLICY

Oaklands College provide and maintain IT systems that are enabled for staff to communicate in a secure environment. Student enrolment data is also stored securely within the Oaklands College student records systems. Data is only shared with the University of Hertfordshire with the permission of students.

The University of Hertfordshire provide and maintain IT systems to enable secure communication with students. UCSA staff have limited permissions with access to data stored by the University of Hertfordshire with regards to students. This data is owned and managed by the University of Hertfordshire and UCSA staff cannot access personal data stored securely by the University of Hertfordshire.

UCSA has its own website and this is maintained by an external party. They are required to ensure that the website is securely hosted on a managed WordPress dedicated Google Cloud server with real-time security threat detection. They are also required to comply with CyberEssentials best practice to ensure the security of information.

UCSA STAFF

All UCSA staff, whether permanent or temporary and whether seconded to UCSA by Oaklands College or the University of Hertfordshire, are expected to comply with this policy.

All staff are also required to comply with the Oaklands College Data Protection Policy (which governs the work of UCSA) and this can be found at https://oaklandsacuk0.sharepoint.com/:w:/r/sites/Quality/_layouts/15/Doc.aspx?sourcedoc=%7B9BAE678E-C510-466C-9F1A-4DC217EFC747%7D&file=05%20Data%20Protection%20Policy%20and%20Procedure%20(GDPR).docx&action=default&mobileredirect=true

To minimise the risk of cyber threats the UCSA policy has 7 key elements that staff must adhere to:

1. **Storing data**

Personal data can only be stored in secure data systems either operated by the College or University and must not be stored on personal laptops or computers.

2. **Backing up data**

All essential student and staff data will be backed up within the relevant College and University systems and databases that are regulated and managed centrally. Staff must comply with relevant instructions by either institution to ensure the back up of data.

3. **Protection form malware**

Malicious software (also known as 'malware') is software or web content that can harm an organisation. The most well-known form of malware is viruses, which are self-copying programs that infect legitimate software.

Staff must comply with any requirements to protect their computer and use/update the anti-virus software provided.

Staff should only download apps for mobile phones and tablets from manufacturer-approved stores (like Google Play or Apple App Store).

Staff should avoid downloading third party apps from unknown vendors/sources.

Staff should not transfer files by USB stick but utilise other means provided by either shareholder to share data (i.e. encrypted in email, cloud or exchange file).

Staff must ensure the firewall provided is enabled at all times.

4. **Keeping smartphones and laptops safe**

Mobile technology requires even more protection than 'desktop' equipment.

Staff must deploy a suitably complex pin and password and where possible enable fingerprint or eye recognition as additional security measures.

Staff must utilise the mobile device management software to:

- track the location of a device
- remotely lock access to the device (to prevent anyone else using it)
- remotely erase the data stored on the device
- retrieve a backup of data stored on the device

Staff must ensure the operating system is kept up to date and keep all apps up to date.

Staff must not to connect to the Internet using unknown wi-fi hotspots, and instead use mobile 3G or 4G mobile networks, which will have built-in security.

5. Using passwords to protect your data

Laptops, computers, tablets and smartphones will contain a lot of business-critical data as well as personal student information and also details of the online accounts that you access. It is essential that this data is not available to unauthorised users.

Staff must ensure:

- password protection is deployed at all times
- they use two-factor authentication for any accounts where this added protection is provided

6. Avoid Phishing Attacks

In a typical phishing attack, scammers send fake emails to thousands of people, asking for sensitive information (such as bank details), or containing links to bad websites.

Staff should report any unusual requests received by email to the relevant shareholder IT helpdesk.

7. Training

Staff will be required to attend core training provided by Oaklands College to ensure both Cyber Security and GDPR awareness.