**IT SYSTEMS ACCESS form**

Approved by the Vice-Chancellor: 11 November 2020

This form is used for applications for access to University IT systems including, where applicable, the student record system (Paradigm), the learning management system (ARK) and the Library Hub. This form is governed by the University’s [Information Technology Access and Use Policy](https://divinity.edu.au/documents/information-technology-access-and-use-policy/).

|  |
| --- |
| **1. PERSONAL DETAILS**  |
| Full Name |  |
| College |  |
| Email |  |
| **2. SYSTEM ACCESS REQUIRED** *- Tick up to one in column A and / or column B* |
| *Type* | *A* | *Paradigm Access* | *B* | *ARK Access* | *Approval required* |
| Basic |  | ARK and Library Hub |  | ARK Unit administrator (College) | College Registrar |
| Advanced |  | Paradigm Write College records |  | ARK User administrator (College) | Head of College |
| OVC |  | Paradigm Write all records |  | ARK Unit/User administrator (site) | Dean of Academic Programs |
| Admin |  | Paradigm System administrator access |  | ARK Technical administrator (site) | Vice-Chancellor |
| **3. APPLICANT’S DECLARATION** - *to be signed by the applicant* |
| I have read and agree to abide by the Code of Practice for the use of IT assets (overleaf). |
| Signature |  | Date |  |
| **4. APPROVAL** *- to be signed by the officer listed in section 2* |
| Name  |  |
| Signature |  | Date |  |

Please forward the completed application electronically to: forms@divinity.edu.au

**CODE OF PRACTICE**

This Code of Practice for the use of Information Technology Assets supports the University of Divinity’s Information Technology Access and Use Policy and applies to all users, information assets, and information technology assets (IT assets) as defined within the Policy.

The University monitors the access and use of IT assets to ensure compliance with this code of practice; this includes where IT assets are being used for personal use or where personal devices are accessing IT assets. Users are required to report any actual or suspected breaches of this code of practice by other users or themselves (even inadvertent) as per the requirements of the policy. Users found to be in breach of this code of practice are considered to be in breach of the Policy.

Access to IT assets must only be granted to authorised users who are responsible for all activity that originates from the assets themselves and user software accounts therein. This includes access to connectivity points (such as WiFi) through personal devices.

Access and stewardship of IT assets is granted for the primary purpose of advancing the University towards its mission. Limited personal use of IT assets, where it does not relate to University business, is permitted where it does not require a substantial expenditure of time, adversely affect the University or breach the policy or this code of practice.

**Users must:**

a) only use IT assets that have been allocated to them, or to which they have been temporarily granted access, by the University.

b) only access IT assets using their unique usernames and associated passwords.

c) maintain total confidentiality of their unique usernames and associated passwords.

d) ensure that physical IT assets are secure at all times both within University premises and when outside University premises.

e) advise any visitors accessing IT assets of the need to act in accordance with this Code of Practice.

f) report immediately to the Office of the Vice-Chancellor if they suspect that IT assets of the University have been inappropriately accessed by third parties (‘hacked’) or where the confidentiality of usernames or passwords may have been compromised.

**Users must not:**

g) intentionally connect compromised or unapproved devices or communication equipment to the University’s information infrastructure or end-to-end network;

h) intentionally attempt to breach security to access information or parts of the information infrastructure that are outside their authority;

i) allow access to the information infrastructure or end-to-end network to unauthorised users;

j) use another user’s credentials, masquerade as, or represent, another user;

k) use IT, information infrastructure, or the end-to-end network to harass, threaten, defame, libel, or illegally discriminate, as defined in relevant legislation;

l) create, transmit, access, solicit, or knowingly display or store electronic material that is offensive, disrespectful, or discriminatory;

m) contravene any provision of the Copyright Act 1968 including, but not limited to, unauthorised use of copyright material, and downloading or sharing pirated content using the University’s information infrastructure or end-to-end network;

n) modify or remove University information without authority to do so;

o) breach the confidentiality of others, or the University, and the confidential information of others or the University. Information is considered confidential, whether protected by the computing operating system or not, unless the owner intentionally makes that information available; and

p) damage or destroy IT equipment used to access the information assets and end-to-end network.