Virtual Learning Environment Users Agreement

1. Introduction

1.1. Design School Asia and the Virtual Learning Environment (VLE) team seek to maintain a safe and healthy working environment to support its students in their activities. Users who receive abusive or threatening emails or who believe for whatever reason, that the VLE facility is being used inappropriately, should consult their Course Leader.

1.2. Any user to be found in breach of this computer user agreement will be barred from using the VLE, and further action may be taken in accordance with the offence and statutory legal requirements.

2. Unacceptable use

2.1. The VLE must not be used for any of the following:

a) the creation, transmission or retrieval of any illegal, offensive, obscene or indecent images, data or other material; any data capable of being resolved into illegal, obscene or indecent images or material; or any web sites that give reference to them;

b) the creation, transmission or retrieval of any terrorist or extremism-related literature, data or material;

c) the creation or transmission or retrieval of material which is designed or likely to cause annoyance, inconvenience or needless anxiety;

d) the creation or transmission or retrieval of defamatory material;

e) the transmission of material that is confidential to the School and/or the creation or transmission of material intended to undermine School policy;

f) the transmission of material such that this infringes the copyright of another person;

g) the transmission of unsolicited commercial or advertising material either to other user organisations or to organisations connected to other networks;

h) deliberate unauthorised access to facilities or services accessible via the VLE;

i) deliberate activities with any of the following characteristics:

- Corrupting or destroying other users' data;
- violating the privacy of other users;
- disrupting the work of other users service to other users (for example, deliberate or reckless overloading of access links or of switching equipment).

- other misuse of the network or networked resources, such as the introduction of “viruses”.

2.2. All information transmitted and retrieved via the internet is monitored and logged for security/safety purposes. Attempts to access certain sites (including sites which may contain extremism-related content) may trigger a warning to the user and are logged and reported for review. Information regarding individual user’s use of the VLE, and information transmitted or retrieved via the internet may be used as part of safeguarding or disciplinary procedures and may also be provided to external authorities.

2.3. Any access to inappropriate sites (as classified by FortiGuard URL Database Categories, which are based upon the Web content viewing suitability of three major groups of customers: enterprises, schools, and home/families) will be highlighted to the user, and any onward access will be logged.

2.4. Information regarding individual’s use of the VLE, and information transmitted or retrieved via the internet may be used as part of safeguarding or disciplinary procedures, and may also be provided to external authorities.

2.5. You are responsible for any use of the VLE conducted through your VLE account. You must **NEVER** let other people use your username or reveal your password to anyone.

Document version control

Purpose/Change	Author	Date
Original document approved.	IO	01/10/2020