Information Security

Who is this information aimed at?
All users who have been authorised by the University to access, download or store University information.

Who can you contact if you require further information?
IT Service Desk on 0141 273 1234 or internal extension 1234 or https://myservice.gcu.ac.uk

Information
Information Security is the responsibility of all staff students and visitors authorised to access University information.

The top level Information Security policy provides the overarching approach to the management of University information. The information security policy is supported by a series of sub policies, processes and procedures that will set out the expectations for information security within the University.

The security of the University's information is paramount if the University is to ensure appropriate legal, regulatory and contractual compliance. Information security is achieved by protecting the information against unauthorised or unintended losses of **confidentiality (C)**, failures of **integrity (I)** or interruptions to the **availability (A)** of that information. This approach uses the **CIA** triad model to develop information security policy.

In lay terms this means that the 3 key principles **(CIA)** should be guaranteed in any secure information system.

1. **Confidentiality**
   This is the protection of information from unauthorised access.
   Confidentiality requires measures to ensure that only authorised users are allowed to access the information. Controlling user access to information systems (being able to login to a system) will help maintain and protect the confidentiality of that systems information.

2. **Integrity**
   This is where information is kept accurate and consistent unless authorised changes are made.
   Information integrity is maintained when the information remains unchanged during storage, transmission and usage not involving modification to the information. Accurate and consistent information is only achieved as a result of proper information protection (security).

3. **Availability**
   This is where information is available when and where required by authorised users. The availability of information is maintained when all the component parts of the information's system are working properly and in tandem; hardware maintenance, software patching and upgrading and network optimisation will ensure information availability.

Information Security Policies: https://www.gcu.ac.uk/staff/it/itregulationspolicies/