IT Security Policy

Contents

OVERVIEW AND PURPOSE

1. This IT Security Policy forms a key part of the University's overall Information Security arrangements. The IT Security Policy focuses on the technical and usage issues in relation to the University's IT systems whereas the Information Security Policy governs the broader issues of ensuring information is only read, heard, changed, broadcast and otherwise used by people who have the right to do so.

2. In using Information Technology (IT), users at Kingston University have the ability to create, store and/or access a wide range of electronic information. The aim of the policy outlined in this document is to ensure that;

    - confidentiality is maintained. Access is limited to those authorised to do so.
    - integrity is maintained. Information is not changed or deleted without reason.
    - availability is maintained. Information should be readily available to authorised individuals when needed.
    - data access and use conforms to regulations in regard to the data protection legislation. This policy is intended to enable the appropriate use of IT within KU and is reinforced by recommendations from JISC & UKERNA in line with the international security standard ISO27001. The UCISA Information Security Toolkit, designed to encourage best practice, has also been used as a foundation for this document.

3. The University needs to be aware of IT security as there is a range of undesirable consequences associated with breaches of IT security which include but are not limited to;
    - services being unavailable.
    - reputational impact.
    - fraud.
    - data breach.
    - personal investigation.
    - prosecution.
    - Fines or other penalties.

SCOPE

4. This and all other IT security related policies apply to all IT related hardware or software and users of IT services at the University, including all staff, students and any other individuals visiting or connecting to the University network either wired or wirelessly, from either University owned and managed or personally owned devices.

POLICY

Definitions & Abbreviations

5. The term “IT” refers to any communication device or application, encompassing: radio, television, smart phones, computer and network hardware and software, satellite systems and so on, as well as the various services and applications associated with them, such as videoconferencing and distance learning.

6. The term “user” refers to any person who accesses an IT system, service or equipment owned, managed or supplied by KU or one of its partners.

7. The term “ affiliate” refers to any person who accesses an IT system, service or equipment owned, managed or supplied by KU or one of its partners, but is not a KU student or KU member of staff.

8. The term “Production Systems Environment” refers to the physical areas where production systems reside such as Comms Rooms

9. The term “network” refers to any data communications links, whether wired or wireless, that reside on KU sites or one of its partners or any connections between these sites or its partners.

10. “Shared Account” refers to a KU IT account that is used by multiple persons.

11. The term “System Support Staff” refers to all Service Desk and other support staff.

12. “Filing systems” refers to areas where electronic data is stored.

13. The term “Production Systems” refers to IT systems that are used on a daily basis by users at KU. These systems are supported by IT Services.

14. “Prevent” refers to the UK government’s anti-radicalisation initiative and the duty of the University to ensure the safeguarding of its staff and students.

Governance & Review

15. The policy owner will review the policy content annually at least.

16. The policy owner will review the policy immediately in circumstance where any detail within the policy has significantly changed.

17. All University policy documents must be signed and submitted to the University Secretary’s office for record.

YOUR RESPONSIBILITIES

18. In order for this policy to be employed effectively it is essential that those in a managerial position at Kingston University are fully aware of it and apply it in their own use of IT.

19. Managers are responsible for;

    - ensuring that staff, affiliates and students only use IT facilities when they have agreed to abide by the terms of this policy. This includes staff working in Collaborative Partner institutions who have access to University systems.
    - handling any disciplinary issues that arise and proactively investigating any suspected breaches.

20. Incoming students will be notified of the policy when they enrol.

21. Newly appointed staff will be notified of the policy when they sign their contract of employment.

22. The policy and any changes will be made available through StaffSpace and MyKingston.

POLICY

23. This policy exists within the University's overall Information Security framework and consists of a subset of related policies.

24. Access to the University network of IT Services is conditional on staff, affiliates and students agreeing to abide by the terms of this and associated IT acceptable use policies. Some of these are listed here in the RELATED LEGISLATION, REGULATIONS AND POLICIES section.

25. Users of University IT facilities must abide by any relevant laws in place at the time of use. Only individuals with a valid University IT user account, whether staff, affiliate or student, are authorised to use the University's network of IT services. Individuals must always use their own credentials when accessing IT services, and must never share their username or password with others.

26. All IT policies are available via the IT Services pages on both StaffSpace and MyKingston.

27. In order to meet our commitment to ensure the confidentiality, integrity and availability of information all changes to operational services must be made only by qualified and authorised individuals using established change control procedures.

28. It is possible that individual faculties or directorates may adopt externally hosted IT services for their local requirements. It is important that such requirements are coordinated through IT Services to ensure that any associated security considerations are taken into account. Requests to use any such services should, in the first instance, be directed through the Service Desk.

29. When disposing of old or unwanted IT equipment please contact IT Services beforehand to ensure that any security related considerations are taken into account. Such equipment can be disposed of using the University's WEEE procedure.

30. Good practice and behaviours will be actively promoted by IT Services through periodic awareness raising initiatives, targeted communications, workshops and printed informational booklets. IT security is the responsibility of everybody authorised to access the University IT network. It is everybody's responsibility to report incidents of security breach to the Cyber Security Manager through the Service Desk.

31. The University reserves the right to monitor and view information stored or processed within its information services as owner of that information.

32. Individuals found to be in breach of this or any other IT policy may be subject to established University disciplinary procedures.

Security Breaches

33. Any suspicion of breach of the policy must be reported to the Service Desk or a line manager immediately. Failure to do so constitutes a breach of this policy. The line manager should then report the issue to the Service Desk or direct to the Cyber Security Manager.

34. Within the current KU guidelines, the Cyber Security Manager has the power to authorise IT support staff to suspend access to all accounts affected by the breach. The Cyber Security Manager has the authority to suspend these accounts as well. Suspensions will be lifted in three working days unless further suspension is authorised by the Vice Chancellor.

Compliance with National Security and Investment Act (NSIA)

35. The University is committed to full compliance with the National Security and Investment Act, and will report to the relevant government authorities any IT infrastructure, technological assets, or research activities that may trigger review or intervention under the NSIA's provisions. This includes but is not limited to transactions, collaborations, and acquisitions that could affect national security.

36. Any member of the University who is involved in or becomes aware of a proposed acquisition, research partnership, or technology transfer that might fall under the NSIA's remit must immediately report this to the university Cyber Security Manager or Legal Compliance Officer. The University will then review and potentially notify the UK government's Investment Security Unit (ISU) in accordance with the NSIA.

37. The University may conduct due diligence on any external partners, including international collaborators, contractors, and suppliers, to ensure compliance with the NSIA. Partnerships involving sensitive research or technology must be subject to enhanced scrutiny and review.

38. If the University becomes aware of a breach or unauthorised access to systems that are flagged as sensitive under NSIA, an immediate investigation will be initiated, and the incident will be reported to national authorities where appropriate. Remedial measures must be taken to mitigate any potential risks.

RELATED LEGISLATION, REGULATIONS AND POLICIES

39. Acceptable Use Policy – IT Facilities
40. Acceptable Use Policy – Mobile & BYO Devices
41. Acceptable Use Policy – Email