University of Bristol

New Information Security Policy

The University has a new Information Security Policy. This leaflet outlines the key information you need to know.

bristol.ac.uk/infosec/policies

University of BRISTOL

Why do we have a new Information Security Policy?

Information is a vitally important University asset and we all have a responsibility to make sure that this information is kept safe and used appropriately.

Without due care, personal, research or business information can be misplaced or leaked, which is a big enough problem in itself without the added difficulty of having to protect it against increasingly proactive and sophisticated attempts at theft.

Therefore, the University has adopted a new Information Security Policy that both complies with stringent legal requirements, as well as providing the necessary assurance that information held and processed by the University is treated with the highest appropriate standards to keep it safe.

The aim is to raise your awareness to avoid inadvertently causing others inconvenience through disclosure of information, avoid breaking the law and avoid causing the University financial and potential reputational damage.

The majority of organisations are aware of the dangers of information security breaches and some have suffered intellectual property theft or loss of personal data, resulting in serious reputational damage and in some cases fines for negligent management of information. We all have a requirement to work within the guidelines of the new policy and by doing this you can help ensure the safety of your own information and that of others.

In simple terms, the most common causes of information loss or leakage can be avoided by:

- Making sure that only those who need access to information have that access.
- Not storing information where it can be accidentally exposed or lost, e.g. unencrypted USB drives and laptops.
- Making sure that if confidential information has to be transported it is done so securely using encrypted devices or channels.

What do I need to know?

We don't expect you to read the policy in its entirety, but all members of the University should read the Acceptable Use Policy (ISP-09). We do, however, expect you to be familiar with the key principles of the policy and associated sub-policies and this pamphlet acts as an introduction to those principles and points you toward further information.

Key principles
bristol.ac.uk/infosec/policies/key.html

Acceptable Use Policy
bristol.ac.uk/infosec/policies/docs/isp-09.pdf

Test your knowledge now!
There is a mandatory training module for all staff and research postgraduates. If you've not done this, test your knowledge now at bristol.ac.uk/infosec/training/

What are the key principles of the new Information Security Policy?

The underpinning principles of the new Information Security Policy are best presented as a set of do's and don'ts.

Do…

☑ Seek advice if you are unclear about any aspect of information security.

☑ Report any loss or suspected loss of information.

☑ Change your password if you have any suspicion that it may have been compromised.

☑ Ensure that personally owned equipment which has been used to store or process University information is disposed of securely.

☑ Encrypt your mobile devices and make sure that restricted information is always encrypted before it's sent to others.

☑ Password protect your personally owned devices.

☑ Keep all of the software on your personally owned devices up to date.

☑ Comply with the law and University policies.

☑ Be mindful of the risks of using open (unsecured) wifi hotspots or computers in internet cafes, public libraries etc.

☑ Assume that Information Security is relevant to you.

Don't…

☒ Disclose your password to anyone.

☒ Use a personal email account for conducting University business.

☒ Undermine or seek to undermine the security of computer systems.

☒ Make copies of restricted University information without permission.

☒ Provide access to University information or systems to those who are not entitled to access.

☒ Use your University password as the password for any other service.

☒ Connect personally owned storage or mobile devices to University owned equipment.

☒ Send unauthorised bulk email (spam).

☒ Leave your computers unlocked when left unattended.

☒ Leave hard copies of confidential information unattended or unsecured.

For further information on the above do's and don'ts, see bristol.ac.uk/infosec/policies/checklist.html

You can be assured that the University will:

— Look after its information properly and be respectful of your privacy.

— Give you access to information and systems for which you have a legitimate need.

— Allow you to make reasonable personal use of University systems.

— Investigate suspected breaches of the Information Security Policy and take appropriate action.

Why is the Information Security Policy relevant to me?

Support staff
You need to be aware because you are likely to work with confidential University information, for example: financial records; exam information; student lists; staff records.

Academics
You need to be aware because you have access to confidential and research information - strict safeguards are required to protect yourself and others, such as research subjects, from loss, accidental exposure or theft of research information.

Students
You need to be aware because you must know what constitutes acceptable use of University IT systems and know how to protect yourself from potential harm when using social networks.

Managers
You need to be aware because you must ensure that both you and those you manage are working appropriately with the University's information assets.

By considering your use of and access to information you will help to protect your, your colleagues' and the University's information assets.

University of
BRISTOL