Data security and protection

Toolkit for Universities

[October 2019]

Are you geared up for the Data Security and Protection Toolkit?

The Data Security and Protection Toolkit is an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards.

> All organisations that process health and care data should complete a Data Security and Protection Toolkit
>
> **NHS Digital – (28 March 2019)**

The University of Greenwich was fined £120,000 by the Information Commissioner.

The fine was for a security breach in which the personal data of 19,500 students was placed online.

The data included names, addresses, dates of birth, phone numbers, signatures and – in some cases – physical and mental health problems.

Source: BBC News May 2018

Any University that works directly with the NHS or handles NHS Patient data for example as part of research work or the medical school is required to complete the toolkit self assessment (supplied by NHS Digital) submit their results and to have their submission independently reviewed and verified.

NHS partner organisations will request that Universities confirm their compliance with the DSPT Toolkit before agreeing to any share data. Non completion of the toolkit will mean the NHS Trust will not be able to share their data.

32% of organisations have experienced a major cyber attack in the last two years

26% of Technology Leaders feel very well prepared for a cyber attack.

Source: Harvey Nash/KPMG CIO Data Survey 2019

What do you have to do?

We have set out below a summary of the steps that Higher Education providers are required to take to implement the 10 data security standards.

These requirements are across the three leadership obligations under which the standards are grouped (People, Process and Technology).

People

- You should have a named senior executive to be responsible for data and cyber security.
- You should ensure all staff understand their responsibilities under the National Data Guardian's Data Security Standards.
- You should ensure all your staff are aware of their responsibilities and have received appropriate training.

Processes

You should ensure that :

- Personal confidential data is only accessible to staff who need it for their current role.
- Processes are reviewed at least annually to address any known areas which have previously caused breaches or near misses.
- Cyber-attacks against services are appropriately guarded against.
- A continuity plan is in place to respond to data security incidents including significant data breaches or near misses.

Technology

You should ensure that :

- No unsupported operating systems, software or internet
- browsers are used within the IT estate
- A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials
- IT suppliers are held accountable via contracts for protecting the personal confidential data they process on behalf of the University

How can we help?

Will we be able to confirm positive action against the 10 standards?

Are we going to be the next victim of a cyber-attack?

Are we at series risk of a data breach?

Do our staff know what to do to respond to an incident?

At KPMG we have been helping our Health related clients accurately represent their data security compliance for over 10 years. Having provided over 100 assessments in this time we are well placed to support our Higher Education clients to provide the independent view you need and in doing so help to develop a mature framework of data security practice.

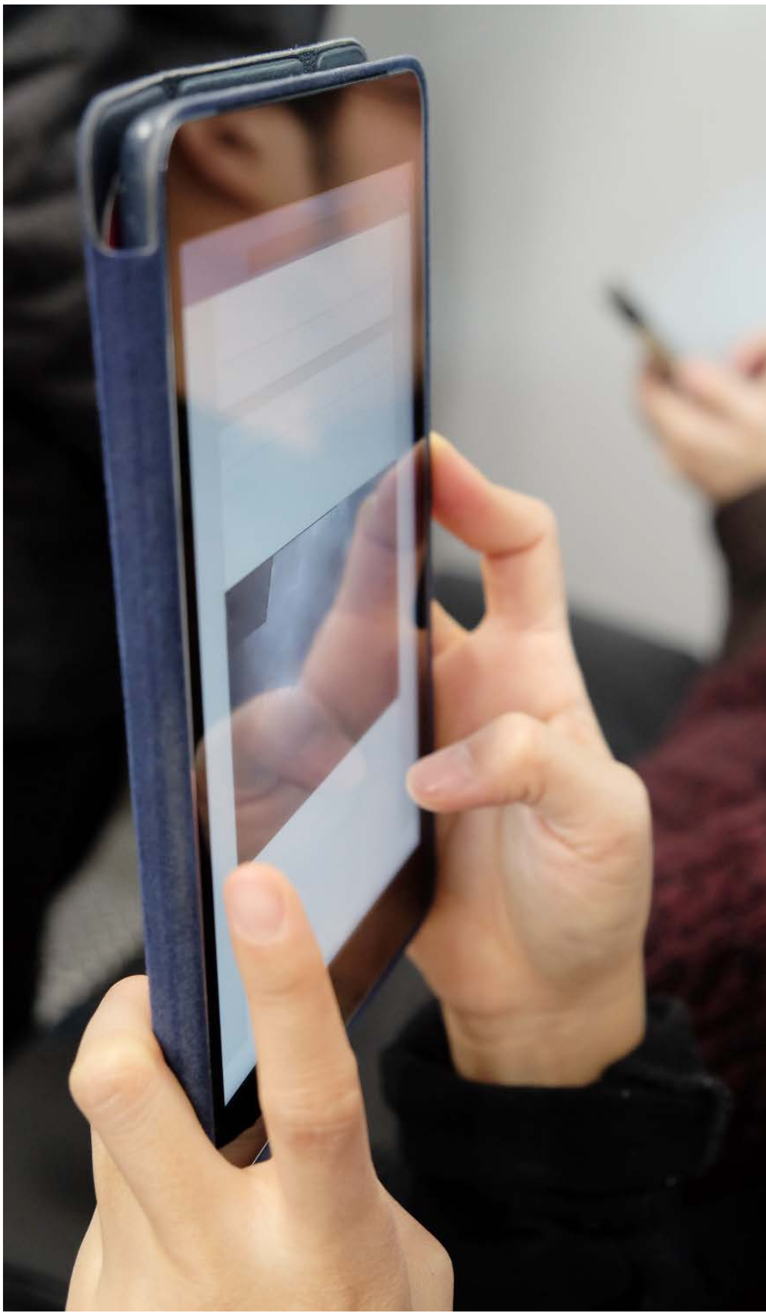
Where necessary we can help you develop your control framework or provide a gap analysis on your controls to help you meet the toolkit assertions based on our experience and knowledge.

Our approach

Our work will help **bridge any gaps** between current security standards in place and the Data Security & Protection Toolkit and provide an independent assessment of the submission, as required by the toolkit.

We can help you to **understand** where your gaps are, and where you should aim to **focus your efforts**, and **help reduce the risk** of disruption to Education services, unwelcome press coverage, sanctions/fines and damage to reputation.

The KPMG Team will work with you to quickly and efficiently diagnose your current level of compliance. We will develop a realistic and practical roadmap to help you to meet the requirements and help you to prioritise your key actions.



Independent

KPMG member firms technical strategies and recommendations are based solely on what is fit and appropriate for your business.

Collaborative

KPMG's I-4 forum brings together over 50 of the world's leading organisations to discuss emerging issues and the solutions which work in an ever-increasing threat landscape.

Trusted

KPMG member firms have a long list of certifications and permits to work on engagements for the world's leading organisations.

Global, local

KPMG is a global network of independent member firms of over 155,000 professionals in 155 countries.

We have over 2,000 security practitioners globally, giving member firms the ability to orchestrate and deliver to consistently high standards worldwide.

Contact your regional KPMG lead:

Andrew North
Technology Risk Director
Mob: +44 (0)7711 713385
Email: andrew.c.north@kpmg.co.uk

Nicolina Demain (London)
Technology Risk Director
Mob: +44 (0)7748 885220
Email: nicolina.demain@kpmg.co.uk

Lee Dobbing (North & Scotland)
Technology Risk Senior Manager
Mob: +44 (0)7919 293691
Email: lee.dobbing@kpmg.co.uk

Raj Cheema (Midlands & South West)
Technology Risk Senior Manager
Mob: +44 (0)7795 354415
Email: rajvir.cheema@kpmg.co.uk

Tim Colclough (London & South East)
Technology Risk Manager
Mob: +44 (0)7887 826733
Email: tim.colclough@kpmg.co.uk

kpmg.com/uk

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

Designed by CREATE | Date | CRT120489A