BOARD MEETING	
Date of Meeting	13 December 2017
Paper Title	Preparation for Cyber Resilience Strategy for Scotland: Public Sector Action Plan
Agenda Item	17.109
Paper Number	17.109A
Responsible Officer	B Hughes; Vice Principal Curriculum and External Relations
Status	Disclosable
Action	For Noting

1. Report Purpose

This paper provides members with an update on the preparations being undertaken by the college in response to the Scottish Government's publication; A Cyber Resilience Strategy for Scotland: Public Sector Action Plan, 2017/18.

2. Recommendations

Members are asked to **NOTE** this paper.

3. Background

On 8 November 2017, the Scottish Government published A Cyber Resilience Strategy for Scotland and an associated Implementation Toolkit. An extract from the Executive Summary is provided below:

The importance of cyber resilience in Scotland's public bodies has never been greater. Digital technologies bring enormous opportunities for Scottish public services – but they also bring with them new threats and vulnerabilities that we must take decisive action to manage.

This Public Sector Action Plan has been developed in partnership by the Scottish Government and the National Cyber Resilience Leaders' Board (NCRLB). It sets out the key actions that the Scottish Government, public bodies and key partners will take up to the end of 2018 to further enhance cyber resilience in Scotland's public sector. While there are already strong foundations in place, its aim is to ensure that Scotland's public bodies work towards becoming exemplars in respect of cyber resilience, and are well on their way to achieving this by the end of 2018.

The action plan focuses on public bodies. Delivery of the action plan will be coordinated and led by the Scottish Government's Cyber Resilience Unit, working in partnership with the NCRLB and Scottish public bodies. Wherever possible, the

Scottish Government will work with key partners in the wider public sector, including local authorities, and universities and colleges, to promote an aligned approach to work on cyber resilience.

A link to the full Strategy and toolkit is provided below:
http://www.gov.scot/Publications/2017/11/6231

The Implementation Toolkit sets out a number of Key Actions and a timetable for the implementation of these actions. The attached paper provides a summary of these key action points (Paper Number 17.109A).

In relation to Key Action 1, due by end November 2017, the college has identified two key contacts as follows:
Working level contact responsible for day-to-day implementation of the action plan in the college: Scott Renton, Head of ICT.
Board/Senior Management level contact with overall responsibility for implementation of the action plan in the college: Brian Hughes, Vice Principal Curriculum and External Relations.
These contacts have been acknowledged by the Scottish Government's Cyber Resilience Unit.

The college has established a working group to assist in the preparation of the further actions that are required in line with the implementation timeline.

4. Risk Analysis

Implementation of the actions outlined in the strategy and toolkit are required by the Scottish Government and the college will need to demonstrate, at various points in time, its compliance with these requirements. The Board will be kept fully appraised of developments and will require, at specific points, to take decisions on the direction of travel.

5. Legal Implications

There are no specific legal implications relating to this paper.

6. Financial Implications

The strategy outlines that funding of up to £1,000 will be made available to public bodies to undertake a pre-assessment in relation to Cyber Essential or Cyber Essentials Plus accreditation. The output of this pre-assessment should include a report to the Board providing them with an analysis of their current conformity with

the five critical controls under the scheme. Following this pre-assessment Board will be required to decide on whether to pursue the basic or enhanced accreditation. Boards will be expected to fund the costs associated with whichever level of accreditation that they opt to pursue. As a broad guide, indicative costs in the region of £300 - £1500 are being identified for Cyber Essentials and £1,500 to £6,000 for Cyber Essentials Plus. Costs will depend on the readiness and complexity of the organisation.

7. Regional Outcome Agreement Implications

There are no specific ROA implications relating to this paper.

8. Has an Equality Impact Assessment been carried out (Y/N/NA)

N/A