H

REGIONAL BOARD REPORT

Subject: General Data Protection Regulation (GDPR)	**Purpose:** **For Approval** ☐ **For Discussion** ☒ **For Information** ☐
Prepared by: Peter D Smith, Vice Principal – Finance and Resources	**Date:** 18 October 2017
Purpose: To consider the impact of the GDPR on the College.	
Linked to Strategic Goal 5: Build Sustainability.	

Executive Summary:

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU. The GDPR aims primarily to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. It will replace the data protection directive (Directive 95/46/EC) of 1995. The regulation becomes enforceable from 25 May 2018 and has the potential to have significant impact on College operations.

The overall scope of the GDPR is far greater than that of Directive 95/46, as are the penalties for breach or non-compliance. In short: -

- As a public authority, we must appoint a data protection officer (DPO), who must not have a conflict of interest in terms of the use of the data within the College (effectively, a mini-regulator).
- The consent of individuals for the capture, use and retention of their personal data must be more explicit, as is the individual right "to be forgotten".
- Data Protection Impact Assessments have to be conducted when specific risks occur to the rights and freedoms of data subjects.
- Enhanced accountability, with a move to "why we hold data" rather than just "what data we hold".
- Data protection must be designed into our data systems.
- Fines for breach are now up to Eur 20M, or 4% of turnover, whichever is the greater.

The attached guidance provided by UCSS gives more detail on the actions we must undertake to ensure compliance. The College has already undertaken some initial work but, clearly, there is significant work to be done to ensure initial and ongoing compliance.

In terms of awareness, a number of key staff have already attended training sessions and we intend to implement an e-learning module for completion by all staff prior to 25 May 2018.

Of most significance, however, is the role of DPO and we are currently scoping whether a shared service proposal from UCSS would be the most appropriate solution.
Recommendation: Board to discuss the implications on Borders College of the GDPR.
Previous Committee Approvals: n/a

For publication ☒	**For publication with redactions** ☐	**Not for publication** ☐

Appendix I- Getting Ready for GDPR

The below is the latest ICO guidance regarding preparing for GDPR. While a DPO Shared Service as provisionally envisaged would look to support the institution when this work had taken place, it may be helpful to bear this anticipated preparatory work that the ICO believes should already be underway.

1. Getting Ready for GDPR

Awareness

Decision makers and key people in your business are aware that the law is changing to the GDPR and appreciate the impact this is likely to have. Your business has identified areas that could cause compliance problems under the GDPR and has recorded these on the organisation's risk register. Your business is raising awareness, across the organisation of the changes that are coming.

Accountability

Your business has set out the management support and direction for data protection compliance in a framework of policies and procedures. Your business monitors compliance with data protection policies and regularly reviews the effectiveness of data handling / processing activities and security controls. Your business has developed and implemented a needs based data protection training programme for all staff.

Information you hold

Your business has documented what personal data you hold, where that data came from and who it is shared with. Your business has planned to conduct an information audit across the organisation to map data flows.

Data Protection by Design and Data Protection Impact Assessments

Your business has implemented appropriate technical and organisational measures to show you have considered and integrated data protection into your processing activities. Your business understands when you must conduct a DPIA and has processes in place to action this. Your business has a DPIA framework which links to your existing risk management and project management processes.

Data Protection Officers

Your business has designated responsibility for data protection compliance to a suitable individual within the organisation. Your business has appointed a Data Protection Officer (DPO) if you are a public authority

or you carry out large scale monitoring of individuals or you carry out large scale processing of special categories of data or data relating to criminal convictions and offences. Your business supports the data protection lead through provision of appropriate training and reporting mechanisms to senior management.

2. Key Areas to Consider

Lawful basis for processing personal data

Your business has reviewed the various types of processing you carry out. You have identified your lawful basis for your processing activities and documented this. You[r] business has explained your lawful basis for processing personal data in your privacy notice(s).

Consent

Your business has reviewed how you seek, record and manage consent. Your business has reviewed the systems currently used to record consent and implemented appropriate mechanisms in order to ensure an effective audit trail.

Children

If your business offers services directly to children, you communicate privacy information in a clear plain way that a child will understand. If your business offers 'information society services' directly to children, your business has systems in place to verify individuals' ages and to obtain parental or guardian consent where required.

3. Individuals' Rights

Communicating privacy information

Your business has reviewed your current privacy notices and has a plan in place to make any necessary changes in time for GDPR implementation.

Individuals' rights

Your business has checked your procedures to ensure that you can deliver the rights of individuals under the GDPR.

Subject Access

Your business has reviewed your procedures and has plans in place for how you will handle requests from individuals for access to their personal data within the new timescales outlined in the GDPR. Your business

has reviewed your procedures and has plans in place for how you will provide any additional information to requestors as required under the GDPR.

4. Breach Notification

Your business has implemented appropriate procedures to ensure personal data breaches are detected, reported and investigated effectively. Your business has mechanisms in place to assess and then report relevant breaches to the ICO where the individual is likely to suffer some form of damage eg through identity theft or confidentiality breach. Your business has mechanisms in place to notify affected individuals where the breach is likely to result in a high risk to their rights and freedoms.

5. Transfer of Data

International

If your business operates in more than one EU member state, you have determined your business's lead supervisory authority and documented this.