F

REGIONAL BOARD REPORT

Subject: General Data Protection Regulations (GDPR)	**Purpose:** **For Approval** ☐ **For Discussion** ☐ **For Information** ☒
Prepared by: Janet Robertson Director of Business Performance & Improvement	**Date:** 01 March 2018

Purpose: To update the Board on progress towards GDPR compliance

Linked to Strategic Goal 5: Build Sustainability.

Executive Summary:

An update on progress towards achieving compliance with GDPR by the deadline date of 25 May 2018 is attached.

Progress is being measured against "Preparing for the General Data Protection Regulation (GDPR) -12 steps to take now" document published by the Information Commissioners Office (ICO).

A project management approach has been adopted to address the steps. The steps are not sequential and are being undertaken in parallel, against a continually developing guidance from the ICO as updates are added to its website: www.ico.org.uk.

Recommendation: Board note the GDPR update.

Previous Committee Approvals: n/a

For publication ☒	**For publication with redactions** ☐	**Not for publication** ☐

Borders College - Preparing for the General Data Protection Regulation (GDPR)

Data Protection Principles

1. Processed lawfully, fairly and in a transparent manner
2. Collected for specified, explicit and legitimate purposes and not further processed for incompatible purposes
3. Adequate, relevant and limited to what is necessary
4. Accurate, and where necessary, kept up to date
5. Kept in a form which permits identification of the data subjects only for as long as necessary
6. Processed in an appropriate manner to maintain security

12 Steps to take now – as recommended by the ICO[i]

Steps	Position Summary at 1/3/18
1 Awareness You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.	The new Cylix online GDPR training module was made available to staff via Moodle in advance of Learning week (14 Feb) with an accompanying all staff email emphasising its mandatory nature and strongly encouraging uptake by the GDPR live date of 25 May. Uptake is being monitored via Moodle and CHRIS system reports and will be used to follow up with line managers to ensure staff follow through on the training. The training is also available to Board members via Moodle. GDPR is a standing item on SLT agendas.
2 Information you hold You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.	An information audit has been carried out involving: • Interviews with SLT members and other key members of staff • Creation of a systems spreadsheet • Update of previous Data Protection audit information from 2016 • Meetings on specific GDPR issues to develop approaches This highlighted that updates will/may be required to: • Data Protection Policy and other related policies, such as Disclosure Policy, Electronic Systems Policy & Procedure, Information Security Policy • Relevant Student record documents e.g. Admissions, Enrolment, Financial Assistance, Transport, Additional needs, Learning Support etc. • Simplify the audit documentation, so we can use it to be able to demonstrate our knowledge and compliance with the Data Protection Principles, should the ICO require this. The ICO has published guidance on documentation which will be taken into account.
3 Communicating privacy information You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR	No privacy notice is obviously available on the BC website, although there is a Data Protection Policy. We are developing a privacy notice for the College, using the ICO and others as examples, adapting them to suit our circumstances. These cover the situations in which they

implementation.	collect personal information, how they use it and links to third parties where relevant. This type of approach is a familiar one on many websites and is also recommended by Brodies.[ii]
4 Individual's rights You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.	The GDPR provides the following rights for individuals: 1. The right to be informed 2. The right of access 3. The right to rectification 4. The right to erase 5. The right to restrict processing 6. The right to data portability 7. The right to object 8. Rights in relation to automated decision making and profiling For the most part these require new procedures/processes to support them e.g. the existing Data Protection Policy contains a right to object to data processing, which must be in writing; however, it does not give further indication as to how to go about this. First drafts of procedures and related parts of Privacy Notice have been created.
5 Subject access requests You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.	The Data Protection Policy does cover the principle of Subject Access Requests, although a supporting procedure or process is not apparent. This will require a clear route for data subjects and an underlying procedure to ensure it is handled appropriately and records maintained. A first draft procedure has been developed.
6 Lawful basis for processing personal data You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.	The ICO guidance states that the privacy notice should include the lawful basis for processing as well as the purposes of the processing. There are 6 lawful bases: 1. Consent 2. Contract 3. Legal Obligation 4. Vital Interests 5. Public Task 6. Legitimate Interests Public authorities (the upcoming DP Bill defines these as being covered by FoI; likely also only when performing a task carried out in the public interest or in the exercise of official authority vested in it) cannot use 6. A first draft of relevant parts of a privacy notice is in progress, however further external guidance on this may be required.
7 Consent You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.	Consent must be *freely given*, *specific*, *informed*, and *unambiguous*, and requires *affirmative action*. In general, our current consents don't completely meet the GDPR standard as they tend to be quite general and there are some inconsistencies across them e.g. in terms of opt ins or opt outs, or areas where we use them when a different legal basis may be appropriate going forward.

	We are currently reviewing consents alongside identifying appropriate alternative legal bases for processing. ICO consultation on consents has ended, however publication of their guidelines is not expected until 11/4/18.
8 Children You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.	Where we deal with children we will need to be extra clear around parental consents and direct communications. An ICO consultation on detailed guidance on children and the GDPR closed 28/2/18 therefore an update to the ICO site is imminent and will inform developments in this area. Initial discussions have taken place with the Students' Association representative, to build in time for testing the readability of documentation such as the privacy notice with children and in relation to equalities.
9 Data breaches You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.	A new mandatory breach reporting requirement has been imposed that has quite stringent time constraints e.g. by the data controller within 72 hours of the data breach occurring, not within 72 hours of the employer being informed. We will need to reinforce the messages in the training module about protecting data, but also have a straightforward method for reporting breaches, including near misses, quickly, and for responding to them, including out of hours. A first draft procedure has been developed however, final guidance on data breach notification has recently been released by the ICO which will have to be taken into account.
10 Data Protection by Design and Data Protection Impact Assessments You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.	Data protection should be designed into everything we do going forward. This means introduction of DPIAs is required rather than optional. We'll have to do it for key changes and new initiatives. Brodies suggest a short Rapid Impact tool to run basic checks to see if a full DPIA exists. This is a similar idea to the E&D approach. The guidance referred to from the ICO isn't fully in place as yet but the optional guidance that already exists from the current regime is suggested as a starting point.
11 Data Protection Officers You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.	As a public authority we are required to appoint a DPO. Pete Smith has been liaising with APUC regarding the appointment of a shared regional DPO with notional weekly time allocation to the College.
12 International If your organisation operates in more than one EU member state	As we work mainly in the UK, the ICO is our lead DP authority. However, we do have international students and our

(i.e. you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.	students may go abroad, which could involve cross border transfer of personal information. Also, some of our Data Processors (e.g. some cloud based services) are based out-with the UK. We will take this into account when planning (see Step 10 above) and in drafting privacy statements (Step 3 above).

GDPR – plan to achieve compliance

Result: Compliance with GDPR requirements by the time they come into force on 25 May 2018.

Measured through each of the 12 steps to data compliance recommended by the ICO having been addressed.

Approach: Develop a current picture based on an initial Data Protection Audit and information gathered by ISLT on systems; these provide a basis on which to develop the Borders College knowledge, documentation and information.

Convene a steering group, chaired by DBI&P, membership comprised of key areas touched on.

Involve others as required to work through the 12 steps.

Involve the Students' Association as appropriate.

Deployment: Meet regularly as a steering group (fortnightly), progressing actions, and reporting to SLT (standing item) and to Board (as required).

Communicate information to staff, seeking views or updating on progress in discussion with SLT & Marketing, to develop understanding and ownership.

Publish updated documentation: forms, policies & procedures, website content.

Monitor progress using a project plan (Gantt chart based on examples).

A&R: Develop drafts based on: reference to ICO guidance, discussion with staff and benchmarking approaches with others in and out-with sector.

Test readability and understanding with staff and students.

Review of approach and achievement post-implementation.

---

[i] Preparing for the General Data Protection Regulation (GDPR): 12 steps to take now V2.0 20170525
[ii] Brodies 2240118.PPPX (CDN HR & OD Steering Group)