BORDERS COLLEGE

Working Together

Data Protection Policy

August 2018

History of Changes

Version	Description of Change	Authored by	Date
1.1	Information provided on where further guidance on data protection issues can be found. Direct marketing and CCTV surveillance added to the scope.	D Killean	16 May 2016
2.0	Fully updated to comply with GDPR and the new DPA. Covers the principles of the law and the rights of data subjects and what this means for the College. Some parts of the policy (e.g. marketing) have been removed and a separate procedure will be developed focusing on DPA and marketing. This is also the case for CCTV. Final version ready for approval	A Wilson	28 August 2018

1. Introduction

1.1 Borders College recognises that information, both electronic and manual, their associated processing tools, systems and services now pervade teaching, learning and administration and are of vital importance to the efficient functioning of the organisation.

1.2 The College will abide by the requirements of data protection legislation. This includes the Data Protection Act 2018, the General Data Protection Regulation (GDPR) and associated guidance and, where applicable, codes of practice and conduct. For ease of reference **Annex A** at the end of this policy details the terminology of data protection law.

1.3 The College is committed to ensuring that the processing of personal data is only undertaken in the legitimate operation of the College's business and has a clear legal basis. The College will ensure that the principles of the Data Protection Act 2018 and GDPR are made known to and observed by all staff members.

1.4 This policy sets out the legal framework and risks which govern the College's use of personal data, its commitment to protecting personal data and the obligations of users to protect all data (with particular reference to personal and special (previously called sensitive) categories of personal data).

1.5 This policy applies to:

- All data created or received in the course of college business, in all formats, of any age. "Data" shall include personal and special category data; and also confidential and commercially sensitive data.
- Data held or transmitted in physical (including paper) and electronic formats.
- Data transmitted in verbal format (e.g. in conversation, in a meeting, or over the telephone).

1.6 The policy must be followed by:

- All College staff (including contractors, temporary staff and anyone else who can access or use data, including personal and special categories of data, in their work for the college).

- Non-staff data subjects (these include, but are not confined to: prospective applicants; applicants to programmes and posts; current and former students; alumni; former employees; family members where emergency or next of kin contacts are held; members of the Board of Management and committees; volunteers, potential and actual donors, customers, people making requests for information or enquiries, complainants, professional contacts and representatives of funders, partners and contractors).
- Further details regarding responsibilities of staff and students are found at Section 5 of this policy.

1.7 Where the policy applies:
- To all locations from which college data is accessed, including home use and overseas.

1.8 Any concerns about the protection of personal data at Borders College, or non-compliance with this policy, must be reported to gdpr@borderscollege.ac.uk

2. Objectives

This policy sets out the framework of governance and accountability for data protection compliance across the college, with particular reference to personal and sensitive personal data (now called special category personal data) and the college's responsibilities for this under data protection legislation.

This policy forms part of the college's framework for Information Governance more broadly and should be read in conjunction with associated policies which include the Electronic Systems Policy and Procedure and the Information Security Policy. These policies set the principles by which the college maintains:

- **Confidentiality**: protecting information from unauthorised access and disclosure
- **Integrity**: safeguarding the accuracy and completeness of information and preventing its unauthorised amendment or deletion;
- **Availability**: ensuring that information and associated services are available to authorised users whenever and wherever required;
- **Resilience**: the ability to restore the availability and access to information, processing systems and services in a timely manner in the event of a physical or technical incident.

2.1 Data Security and Classification

Formal guidance on the classification of different types of data processed by the college and the appropriate specific security arrangements for each class of data will be developed based on the Records of Processing Activities, developed during GDPR implementation. However there are general principles which will apply at all times to all data managed by the college, whether the data is personal and/or special category data; confidential business data; or commercially sensitive data:

- All college users of data must ensure that all data, and specifically personal and special category data, they hold is kept securely;
- Users must ensure data is not disclosed to any unauthorised third party in any form either accidentally or otherwise (including verbal disclosure);
- Desks should be left clear at the end of each working day; paperwork shall be locked away when not in use;
- Portable devices (laptops, memory sticks, and external hard drives) must not be left unattended.

Further information on the College's duty and policy on protecting personal and special category data is outlined within this policy and associated procedures.

3. Legal Governance

The safe and secure management of information is integral to compliance with information law. It is also a key enabler of effective business practice.

Borders College must comply with data protection law ensuring that the college is specifically protecting the privacy rights of individuals where their personal and special category data are concerned. These laws require the college to protect personal information and control how it is used in accordance with the legal rights of data subjects – the individuals whose personal data is held. For further information on the range of privacy law to which the College is subject please refer to the guidance on the intranet and the privacy notice on the website.

Under law the College is responsible for and must be able to demonstrate compliance with, the following data protection principles as set down in the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA), and outlined in the section below.

3.1 Data Protection Principles:

There are 6 Data Protection Principles. They are as follows:

1. Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ('**lawfulness, fairness and transparency**').

2. Personal data shall be collected only for specified explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes ('**purpose limitation**').

3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('**data minimisation**').

4. Personal data processed shall be accurate and, where necessary, kept up to date ('**accuracy**').

5. Personal data shall be kept in a form which permits identification of data subjects for no longer that is necessary for the purposes for which the personal data are processed ('**storage limitation**').

6. Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('**integrity and confidentiality**').

Borders College must also meet the '**Accountability principle**' which means the College is responsible for and must be able to demonstrate compliance with the six principles above. This principle compels the College to adopt policies and implement appropriate measures to ensure and demonstrate that the processing of personal data complies with privacy law. The College is required to maintain necessary documentation of all processing activities; implement appropriate security measures (technical and organisational); perform Data Protection Impact Assessments (DPIAs); comply with the requirement of prior consultation with the regulator (where there are significant risks identified by a DPIA); and designate a Data Protection Officer (DPO).

Individuals (data subjects) have rights under data protection law; these rights are detailed in Section 3.2 in this policy. The College has appropriate procedures in place to ensure these rights can be actioned if an individual makes a request.

3.1.1 Principle 1 Personal data shall be processed fairly, lawfully and transparently

This means that Borders College will:

- Only collect and use personal data in accordance with the lawful conditions set down in the DPA;
- Treat people fairly by using their personal data for specific purposes and in a way that they would reasonably expect;
- Inform people how we use their personal data and what their rights are (known as a privacy notice). This includes being clear, open and honest about how the College uses their data to meet the transparency requirements of the right to be informed (for further detail please see Section 3.2 about individuals' rights);
- Rely on an individual's consent, as the legal basis for processing their personal data, only where:
    - o We've obtained the data subject's specific, informed and freely given consent, and:
    - o The individual has given consent, by a statement or a clear affirmative action (that we document);
    - o The individual has the right to withdraw their consent at any time without detriment to their interests; and
    - o It is as easy to withdraw consent as it is to provide it.

3.1.2 Principle 2 Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; ('**purpose limitation**').

This means that Borders College will:

- Ensure that if we collect someone's personal data for one purpose (e.g. to provide advice on study skills), we will not reuse their data for a different purpose that the individual did not agree to or expect (e.g. to promote goods and services for an external supplier);
- Be clear in the privacy notice as to the specific purposes of processing and ensure that the data subjects are fully informed (for further information regarding the right to be informed see Section 3.2);

- Ensure that if the data is to be used for another purpose it will be compatible with the original purpose, or we will get the individual's specific consent for the new purpose.

3.1.3 Principle 3 Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('**data minimisation**').

This means that Borders College will:
- Only collect personal data that is sufficient for the stated purpose;
- Ensure that the data collected is relevant for that purpose (i.e. we will not collect personal data that is not necessary for the stated purpose);
- Only collect the minimum data required, (i.e. we will not collect more personal data than is necessary for the purpose);
- Reduce risks of disclosure by pseudonymising personal data where possible;
- Anonymise personal data wherever necessary and appropriate, (e.g. when using it for statistical purposes), so that individuals can no longer be identified;
- Review the data we hold and where appropriate delete what we do not need.

3.1.4 Principle 4 Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('**accuracy**').

This means that Borders College will:
- Take all reasonable steps to ensure personal data is not incorrect and have a process in place to ensure that incorrect or misleading data is corrected or erased as soon as possible;
- Update personal data where appropriate, (e.g. when informed of a change of address, our records will be updated accordingly);
- Ensure the accuracy of the personal data we create and record the source of that data (e.g. from data subject or from partner organisation);
- Have processes in place to address an individual's right to rectification: how it is considered, actioned and recorded.

3.1.5 Principle 5 Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; ('**storage limitation**');

This means that Borders College will:

- Only keep personal data for as long as necessary for the purpose it was collected for;
- Apply the College's records management policy and retention and disposal schedule in relation to all records and will regularly review the retention period for any records containing personal data;
- Hold electronic information and records about students centrally by the MIS Department for a period to comply with legal, funding and awarding body requirements and for general enquiries from past students about their education history.
- Keep information about staff for longer periods of time for employment purposes. This will include information necessary in respect of recruitment, pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references.
- In certain circumstances, for example to comply with European funding requirements, keep data for longer periods than noted above.
- Have appropriate processes in place to comply with individuals' requests for erasure under the 'right to be forgotten';
- Destroy records securely in a manner appropriate to their format or anonymise the personal data when we no longer require it;
- Identify personal data that needs to be kept for public interest archiving, scientific or historical research or statistical purposes

3.1.6 Principle 6 Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('**integrity and confidentiality**').

This means that Borders College will:

- Have appropriate organisational security measures in place to protect personal data, including the Electronic Systems Policy and Procedure and the Information Security Policy;

- Have appropriate technical security measures in place to protect personal data;
- Have appropriate physical and personnel security measures in place, (e.g. secure rooms where personal data is held);
- Control access to personal data so that staff, contractors and other people working in the College can only see the personal data that is necessary for them to fulfil their duties;
- Require all College staff, contractors, students and others who have access to personal data in the course of their work to complete data protection training, supplemented as appropriate by procedures and guidance relevant to their specific roles;
- Set and monitor compliance with security standards for the management of personal data as part of the College's framework of information governance policies and procedures;
- Provide appropriate tools for staff, contractors, students and others to use and communicate personal data securely when working away from the College;
- Where transferring personal data to another country outside the European Union (EU) put in place appropriate agreements and auditable security controls to maintain privacy rights;
- Have a robust detection, investigation and internal reporting procedures in place for security incident management and, where applicable, report to the Information Commissioner's Office (ICO) and data subjects affected;
- Where a data breach is likely to result in a risk to the rights and freedoms of data subjects, the Data Protection Officer (DPO) shall liaise with the Information Commissioner's Office (ICO) and report the breach, in line with regulatory requirements, within 72 hours of discovery. The DPO shall also recommend, where necessary, actions to inform data subjects and reduce risks to their privacy arising from the breach.

3.1.7 Accountability Principle

The accountability principle requires the College to take responsibility for what it does with personal data and how it complies with the data protection principles. The College must have the following required documentation and records in place in order to demonstrate compliance.

This includes the following:

- Records of Processing Activities. This will contain all the business functions of the College which collect personal data; the types of personal data collected; the source of the data; who (if any) it is shared with; the security measures in place to protect it; the retention and disposal of the data and the legal basis that it is collected for and the conditions for processing. This must be maintained and reviewed on a regular basis;
- Adopting and implementing data protection policies and procedures that demonstrate appropriate technical and organisational security measures are in place;
- Appointing a Data Protection Officer (DPO), the College has an appointed DPO who can be contacted via the data protection mailbox gdpr@borderscollege.ac.uk;
- Implementing a 'data protection by design and default' approach. This means that whenever a policy, process or system involves personal data that the College considers and builds in the appropriate safeguards to protect the personal data from the start;
- Use proportionate privacy and information risk assessment, and where appropriate data protection impact assessment, to identify and mitigate privacy risks at each stage of every project or initiative involving processing personal data; and in managing upgrades or enhancements to systems and processes used to process personal data;
- Ensuring appropriate contracts are in place with any third party organisations who process personal data on the College's behalf and where the College shares personal data with other organisations that this is properly documented in a data sharing agreement (DSA);
- Recording and where appropriate reporting personal data breaches to the regulator (UK Information Commissioner's Office (ICO)) and if necessary the data subjects;
- The College will adhere to relevant codes of conduct and, where applicable, sign up to certification schemes.

The accountability principle is an ongoing obligation and the college shall regularly review (and where necessary update) documentation and risk assessments. Through meeting the accountability requirements the College shall provide the assurances to individuals that their personal information is secure.

3.2 Rights of Data Subjects (Individuals)

Data subjects have a number of rights under data protection law. These are:

1. The right to be informed;
2. The right of access;
3. The right to rectification;
4. The right to erasure;
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.

These rights are explained in further detail below. It's important to note that some rights have certain conditions that must be met for the rights to apply. When an individual makes any request to exercise their rights then the request must be sent to the data protection mailbox gdpr@borderscollege.ac.uk and it will be allocated and processed accordingly.

There are time limits which apply to data subject requests. All requests must be responded to in one (calendar) month. In some cases the practical application of these can vary therefore the College will adopt a 2-28 day response period to ensure compliance is always within a calendar month.

Parents or guardians of students aged over 16 do not have the right of access to information and will not be given access to data relating to the student unless the student has given written consent for the release of information.

3.2.1 Right to be informed

This means that, at the point that we collect individuals' personal data; we will explain to them in a clear, concise and accessible way the following information:

- The name and contact details of our organisation;
- The name and contact details of the college and the Data Protection Officer;

- For what purposes we collect and use their personal data;
- What lawful conditions we rely on to process data for each purpose and how this affects their rights;
- Our obligations to protect their personal data;
- What personal data we collect (if the personal data is not obtained from the individual it relates to);
- The sources from which we obtain their data, where we have received the data from third parties;
- To whom we may disclose their data and why (e.g. sharing with accrediting bodies like the SQA);
- Which other countries we may we may send their data to, why we need to do this and what safeguards apply in each case;
- How long we intend to retain their data, and that it will be destroyed securely when we no longer require it;
- The rights available to individuals in respect of the processing and how to exercise their rights including:
    - The right to access;
    - The right to object;
    - The right to rectification;
    - The right to withdraw consent (when consent has been used);
    - The right to lodge a complaint with the regulator – the UK Information Commissioner's Office (ICO);
- Whether they need to provide data to meet a statutory or contractual requirement and if so, the consequences of not providing the data;
- Whether we use automated decision-making, including profiling, and if so the impact on data subjects and their rights to object.

The College shall publish this information on its website and where appropriate in printed formats. We will review the content of these Privacy Notices regularly and inform our data subjects of any significant changes that may affect them.

Where we process personal data to keep people informed about college activities and events (i.e. marketing) we will provide in each communication a simple way for individuals to withdraw their consent of further marketing communications. For further information on marketing and data protection please contact the marketing team or email the data protection mailbox.

In these ways the college shall provide accountability for our use of personal data and demonstrate that we will manage people's data in accordance with their rights and expectations.

3.2.2 The right of access

This means that individuals have the right to request access to their personal data that the College holds. Any individual may make such a request and receive a copy of their information free of charge and within one month of their request.

3.2.3 Right to rectification

This means that individuals have the right to have inaccurate personal data rectified and incomplete personal data completed. We will provide simple and secure ways for our students, staff and other data subjects to update the information that we hold about them, such as home addresses.

3.2.4 The right to erasure

This is commonly known as the right to be forgotten. It means that individuals can have their personal data erased when it is no longer needed, if the data has been unlawfully processed or if the data subject withdraws their consent, unless there is an overriding legal or public interest in continuing to process the data.

3.2.5 The right to restrict processing

Individuals may restrict the processing of their personal data until a dispute about the data's accuracy (see 4.2.3) or use has been resolved, or when the College no longer needs to keep personal data but the data subject needs the data for a legal claim.

3.2.6 The right to data portability

This means that where a data subject has provided personal data to the College by consent or contract for automated processing they have the right to request a machine readable copy or have it sent to another data controller.

3.2.7 The right to object

All individuals have the right to object and prevent further processing of their data. This right is not absolute and requires certain conditions to be met. These conditions include:

- Where the College is processing personal data for direct marketing purposes an individual can object and the College must stop processing their data for marketing;
- If consent was given by or on behalf of a child for online services such as social media, they have the right to withdraw their consent and stop the College processing their data;
- Where decisions have been taken solely by automated means then an individual can object to, especially where such decisions could have a negative impact on them (see further detail at 3.2.8).
- If the individual objects to processing which is carried out in the course of the College's legitimate interest or public interest unless the College can demonstrate compelling lawful grounds for continuing to process the individual's data.

3.2.8 Rights in relation to automated decision making and profiling

Automated individual decision-making means a decision is made solely by automated means and without any human intervention. Profiling is automating processing of personal data to evaluate certain things about an individual. Profiling can be part of an automated decision making process. This type of decision-making can only be carried out where the decision is necessary for the entry into or performance of a contract; authorised by law or based on the individual's explicit consent.

When the College processes personal data which involves automated decision-making or profiling then it's important that the College does the following:

- Provide the individual with information about the processing;
- Provide a simple way for them to request human intervention or challenge a decision;
- Carry out checks to ensure that the systems are working properly as intended

4. Roles & Responsibilities

4.1 Designated Data Controller and Data Protection Officer

The College as a body corporate and a legal entity is the data controller under the legislation. The Regional Board is responsible for agreeing the Policy. Although the Regional Board is therefore ultimately responsible, the College has designated that the Vice Principal – Finance and Corporate Services is responsible for the implementation of this Policy and will act as the single point of contact in the College.

The College has appointed a Data Protection Officer (DPO) through HEFESTIS DPO Shared Services, initially for one day per week. The DPO can be contacted by the data protection mailbox: gdpr@borderscollege.ac.uk

4.2 Compliance

Compliance with data protection legislation is the responsibility of all members of the College. Any deliberate breach of the data protection policy may lead to disciplinary action or withdrawal of access to College facilities or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be raised with the Vice Principal – Finance and Corporate Services or the DPO.

4.2.1 Staff Responsibilities

Staff who, as part of their responsibilities, collect data about other people must comply with this policy and any associated policies and procedures.

Staff must ensure that any personal data is held securely and that information is not disclosed, either orally or in writing, accidentally or otherwise, to any third party.

Staff members are responsible for:

- checking that the information they provide to the College in connection with their employment is accurate and up to date; and
- Informing the College of any changes to the information they have provided.

4.2.2 Student Responsibilities

Students using the College's computer facilities may, on occasion, process personal data as part of their studies. If they do so they must notify their tutor to ensure that they are processing in line with this policy and the legal requirements.

Students are responsible for:
- ensuring that all personal data provided to the College is accurate and up to date;
- Notifying the College of any alterations to their address or personal details as provided on the enrolment form.

The College cannot be held responsible for any errors unless the member of staff or student has advised the College accordingly.

5. Related Policies and Further Reference

The relevant policies include (but are not limited to):
- Employee Disciplinary Policy and Procedure
- Information Security Policy
- Electronic Systems Policy and Procedure
- Breach Notification Procedure
- Engage Staff Induction and Compliance Training

The Data Protection Act 2018 is available here:
http://www.legislation.gov.uk/ukpga/2018/12/contents

The UK Information Commissioner's Office (ICO) website has a guide to GDPR https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/ as well as a suite of guidance on the various aspects of information law which the College must comply with.

This includes a guide to the Privacy and Electronic Communications Regulations (PECR) https://ico.org.uk/for-organisations/guide-to-pecr/

6. Review

This policy will be reviewed every 3 years or more regularly where dictated by legislative changes.

Equality Impact Assessment

(Rapid impact assessment tool)

What Impacts may there be from this Proposal on any Group's ability to use the College services?

Policy: Data Protection

Positive Impacts (Groups affected)	**Negative Impacts (Groups affected)**
The policy is in place to protect individuals' data. This applies to all groups of people.	
Actions taken to alleviate any negative Impacts: None	
Recommendations: None	

From the outcome of the rapid equality impact assessment, have negative impacts been identified for any protected characteristic or any other potential disadvantaged group?

Has a full Equality Impact Assessment been recommended?

Yes ☐

No x

Reason for recommendation:

n/a

Definitions in Data Protection

The following provides a definition of the terminology used in this policy in relation to data protection law.

Biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person such as facial images or dactyloscopic data (fingerprint).

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Data concerning health means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

Data controller means the organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data processor means the organisation which processes personal data on behalf of the data controller. If an organisation is a data processor there are specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach.

Filing system means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Genetic data means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample form the natural person in question.

Personal data means any information relating to an identifiable person (data subject); who can be directly or indirectly identified in particular by reference to an identifier. This definition is wide a means that a wide range of personal identifiers constitute personal data. This includes name, identification number (e.g. NI Number), location data, online identifier (IP address) which reflects the changes in technology and the way that organisations collect information about individuals. It also includes information relating to factors specific to the physical, physiological genetic, mental, economic, cultural or social identity of that individual.

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Processing means any operation or set of operations which is performed on personal data or on sets of personal data. Processing occurs whether it is electronic or physical records, it includes: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. So even if data is held in a server but not used this is still processing.

Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be identifiable without the use of additional information, provided. The additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data identifiable unless the additional information (e.g. use of a key code).

Recipient means a natural or legal person, public authority agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

Restriction of processing means the marking of stored personal data with the aim of limiting their processing in the future.

Special category data (formerly known as sensitive personal data) means personal data which identifies an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, sex life or sexual orientation. This data requires extra safeguards to protect it from unauthorised use, disclosure etc. as it is considered that this information can have a higher impact on the rights and freedoms of an individual. Criminal records and convictions information is not under this category of data but should also be handled with extra safeguards due to the sensitivity of the information.

Territorial Scope Data protection law applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU. Third party means a natural or legal person, public authority, agency or boy other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Third party means a natural or legal person, public authority, agency or boy other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Status:	Agreed by JCCP and the Regional Board
Dated:	August 2018
Author:	Data Protection Officer
Review Date:	June 2021
Equality Impact Assessed:	June 2018