



HOLMES UNIVERSITY FLORIDA

Licensed by the Florida Commission for Independent Education (CIE)

PD16 – Privacy and Data Protection Policy

Policy Code	PD16
Policy Title	Privacy and Data Protection Policy
Domain	B – Data Protection
Internal Ref	B.16
Jurisdiction	Florida, United States – Holmes University Florida (HUF)
Version	1.1
Policy Owner	Director of Risk and Compliance, Holmes University Florida
Approved By	Holmes University Florida Board of Directors

1. Related Policies

- PD17 – Privacy Notice (Florida)
- PD51 – Data Breach Policy (Florida)
- PD54 – Records Access Request Policy (Florida)
- PD44 – Records Management (Florida)

2. Introduction

- 2.1** Holmes University Florida (HUF) is committed to protecting the privacy and security of personal information belonging to its staff, students and other stakeholders. This policy sets out HUF's policy statement on the protection of personal information; the roles and responsibilities of HUF and its officers regarding the collection, processing, security of and access to personal information; and the framework for investigating and preventing data breaches, together with governance and training arrangements. It is read in conjunction with HUF's Privacy Notice (PD17).

3. Policy Statement

- 3.1** This policy aims to set out how personal information is received, managed and processed at HUF; to support HUF's compliance with applicable privacy and data-protection law; and to minimize the risk of breaches. HUF is committed to full compliance with the Family Educational Rights and Privacy Act (FERPA, 20 U.S.C. §1232g; 34 C.F.R. Part 99), the Florida Information Protection Act (FIPA, §501.171, Fla. Stat.) and, where applicable, the Gramm-Leach-Bliley Act (GLBA). To achieve these aims, HUF undertakes to:

- Make privacy and data protection a core part of operational activities;
- Provide staff training on this policy and the management of personal information;
- Collect and use personal information only for specific and legitimate purposes;

- Process personal information lawfully and transparently, and disclose to individuals how their information will be used (through a privacy notice at the point of collection);
- Maintain personal information that is accurate and up to date, and correct information that is inaccurate;
- Retain personal information only as long as necessary, in accordance with the records-retention schedule (PD44) and applicable law;
- Keep personal information confidential and secure;
- Not share personal information with third parties unless adequate standards of protection are assured and, where required, the individual is informed; and
- Incorporate data-protection measures into HUF's governance through reporting to the Board of Directors on adherence to this policy and the law.

4. Scope

- 4.1** This policy applies to all HUF activities and processes in which personal information is used, whether digital or hard copy, and to HUF staff and students and to others acting for or on behalf of HUF who are granted access to its information infrastructure.

5. Key Definitions

- **HUF (as the responsible institution):** HUF determines the purposes and means of processing personal information and is responsible for ensuring that any service provider it engages can protect that information and comply with applicable law before it is provided to them.
- **Service Provider:** a person or body that processes personal information on behalf of HUF, such as an agent or contractor.
- **Privacy Officer:** the person responsible for informing on and monitoring HUF's compliance with its privacy obligations. At HUF, the Privacy Officer is the Director of Risk and Compliance.
- **Individual:** the identified or identifiable person to whom personal information relates, including employees, students, applicants, business contacts, visitors, suppliers and contractors.
- **Personal Information:** information relating to a person who can be identified directly or indirectly, such as by name, identification number, location data or online identifier.
- **Sensitive Personal Information:** information given additional protection under law, including Social Security number, driver-license or identification-card number, financial account numbers, health and health-insurance information, and information revealing racial or ethnic origin, religious beliefs, health, or sex life or sexual orientation.
- **Data Breach:** a security incident affecting the confidentiality, integrity or availability of personal information - where it is lost, destroyed, corrupted, disclosed, accessed or passed on without authorization, or made unavailable with significant negative effect on individuals.
- **Processing:** almost anything done with personal information, including collection, recording, storage, alteration, retrieval, use, disclosure, restriction, erasure or destruction.

6. Responsibilities

- 6.1** The Board of Directors has overall oversight of this policy and ultimate responsibility for ensuring a current policy is in place and that systems protect privacy and personal information accordingly. The Director of Risk and Compliance (Privacy Officer) advises the Board on HUF's obligations; trains staff; monitors and enhances compliance; processes records-access requests (PD54); investigates data breaches and reports them to the Board and other appropriate parties; and coordinates with external authorities. The Senior Management Group (SMG) ensures compliance

within departments, liaises on training, and ensures agents, contractors and other service providers under its control adhere to this policy. All staff must comply with this policy, complete refresher training at least every two years, keep personal information secure and undisclosed to unauthorized parties, retain it per the retention schedule, refer any records-access request or complaint to the Director of Risk and Compliance within 24 hours, and report suspected breaches to their line manager or the Privacy Officer. Students are made aware of the Privacy Notice and this policy, must keep their data up to date, and must respect the privacy of others.

7. Privacy Notice and Data Protection Impact Assessments

- 7.1** HUF's Privacy Notice (PD17) is read with this policy and published on HUF's website; it explains the types of information HUF collects and how it stores, processes and uses personal information, and is updated from time to time. HUF uses Data Protection Impact Assessments (DPIAs) to identify and reduce privacy risks in its processes and data-sharing arrangements. A DPIA is undertaken by the Director of Risk and Compliance for major projects or significant changes involving personal information; it identifies the need for the assessment, describes the processing (nature, scope, context and purposes), assesses necessity, proportionality and risk, and identifies measures to reduce risk. Completed DPIAs are maintained in a register and may be made available to appropriate authorities on request.

8. Sharing Information with Third Parties

- 8.1** Where required, HUF puts in place a data-sharing agreement with a third party that acts as an independent recipient, covering the parties' roles, the purpose of sharing, what happens to the data at each stage, and ongoing checks. Where a service provider processes information on HUF's behalf, the agreement covers the subject matter, duration, nature and purpose of processing, the type of information and categories of individual, and HUF's obligations and rights. Any third party intending to enter such an agreement should first contact the Director of Risk and Compliance to ensure the appropriate template is used; registers of data-sharing agreements and service-provider contracts are maintained by the Director of Risk and Compliance.

9. Data Breaches

- 9.1** HUF implements appropriate technical measures (such as encryption, access control and password protection) to mitigate the risk of breaches, and trains all staff in data-protection procedures. Should a breach occur, all suspected and actual breaches are reported to the Director of Risk and Compliance as soon as possible (staff via their supervisor, students via a Student Support Officer). The Director of Risk and Compliance contains the breach to recover data and minimize harm; assesses the associated risks; notifies affected individuals and, consistent with FIPA, the Florida Department of Legal Affairs where a breach affects 500 or more individuals, without unreasonable delay and no later than 30 days; takes steps to prevent recurrence; considers whether staff-disciplinary or student-misconduct procedures apply; and maintains records of the breach and HUF's response, the effectiveness of which is reviewed by the Board of Directors. Full procedures are in the Data Breach Policy (PD51).

10. Records Access, Governance and Training

- 10.1** Individuals may request access to the personal information HUF holds about them; such requests are handled under the Records Access Request Policy (PD54), and eligible students exercise

their rights to inspect, review and request amendment of education records under FERPA. If any person (for example, law enforcement or a parent) requests access to another person's information, staff must check with the Director of Risk and Compliance before any disclosure. Governance is evidenced by the appointment of the Director of Risk and Compliance as Privacy Officer, regular reports to the Board of Directors, breach reports retained for at least two years, disclosure of significant breaches to relevant authorities, and a published, current Privacy Notice. HUF ensures staff are trained at onboarding and at least every two years, with a training register maintained by the Director of Risk and Compliance.

Document Control

Prepared by	Director of Risk and Compliance, Holmes University Florida
Risk and Compliance Review Date	14 July 2026
Board of Directors Review Date	21 August 2026
Board of Directors Approval Date	21 August 2026
Policy Implementation Date	21 August 2026
Policy Review Date	21 August 2029