

# 1 Electronic Privacy

2 Effective: November 8, 2012

3 Updated: June 14, 2021

4 Contact: [Information Technology Services \(ITS\)](#)

## 5 Contents

6 **Introduction**

7 **Policy Statement**

8 **1. Privacy and Confidentiality**

9 **2. Exceptions to Privacy of Information**

10 *2.1 State and Federal Law*

11 *2.2 Proxy Access to Accounts Necessary to Conduct Business or Research*

12 *2.3 Investigations*

13 *2.4 Official University Business*

14 *2.5 Internal Administrative Disclosure*

15 *2.6 Maintenance of Iowa State University Network and Systems*

16 *2.7 Legal Disclosure Requests*

17 *2.8 Health and Safety Emergency*

18 *2.9 Authorization*

19 *2.10 Cookie Privacy*

20 **Resources**

## 21 Introduction

22 Iowa State University is required by federal and state laws to keep certain information confidential.  
23 Privacy and confidentiality must be balanced with the need for the university to manage and  
24 maintain networks and systems against improper use and misconduct.

## 25 Policy Statement

### 26 1. Privacy and Confidentiality

27 To the extent permitted by law and university policy, Iowa State University maintains and protects  
28 both the privacy of individuals and the confidentiality of official information stored on its information  
29 technology (IT) systems. While the university permits limited incidental use of its IT resources, users  
30 of those resources do not acquire an expectation of privacy in communications transmitted or stored  
31 on university information technology resources. In order to comply with the law, university officials  
32 may have direct access to stored information as described below.

### 33 2. Exceptions to Privacy of Information

34 Data traversing or stored in university systems are subject to disclosure requests under public  
35 records law, under subpoena, and in the discovery process in litigation. Iowa State University may  
36 preserve, access, monitor, or disclose information containing all classes of data as described in  
37 the **data classification policy** (see *Resources below*) residing on its information networks and  
38 systems in the following situations:

#### 39 2.1 State and Federal Law

40 All information including the personal, academic, or research data and files residing on university  
41 systems is subject to state and federal laws and regulations requiring its disclosure, including laws  
42 on public records, court-ordered disclosure, and discovery in litigation.

43 **2.2 Proxy Access to Accounts Necessary to Conduct Business or Research**

44 Faculty and staff may need access to accounts of other faculty and staff when that individual is not  
45 available but access is needed to conduct university business or further research. Approval to  
46 access the account should be given either by prior proxy access to the individual's account or by  
47 written recommendation and justification by the individual's department chair or director and  
48 approval by a senior vice president, the senior vice president and provost, general counsel or other  
49 designee acting on the basis of university policy and law.

50 **2.3 Investigations**

51 Iowa State University may preserve, access, or monitor accounts and equipment during the course  
52 of an investigation of misconduct, violations of law, or violations of university policy by students or  
53 employees. Access must be approved in writing by the senior vice president for operations and  
54 finance, senior vice president and provost, general counsel or other designee acting on the basis of  
55 university policy and law. In accessing the account or equipment, university officials are expected to  
56 avoid accessing information that is personal and irrelevant to the investigation.

57 **2.4 Official University Business**

58 As part of their assigned responsibilities, Iowa State University faculty and staff may have access to  
59 all classes of data and are restricted to using it only for purposes associated with the requirements of  
60 their position.

61 **2.5 Internal Administrative Disclosure**

62 Disclosure or use of any information containing data with a high or moderate security category for  
63 extraordinary circumstances must be approved in writing by the senior vice president for operations  
64 and finance, senior vice president and provost, general counsel or other designee acting on the  
65 basis of university policy and law.

66 **2.6 Maintenance of Iowa State University Network and Systems**

67 Iowa State University reserves the right to maintain its information systems; to audit networks and  
68 systems on a periodic basis to ensure compliance with security policies; and to locate and resolve  
69 security breaches or other situations that potentially impact the reliability, robustness, or security of  
70 the campus network and systems infrastructure. Individuals performing these functions or others  
71 may have access to information containing all classes of data and are restricted to using it only for  
72 purposes associated with their position.

73 **2.7 Legal Disclosure Requests**

74 Iowa State University may preserve, access, and disclose information contained in its IT systems in  
75 response to a lawfully issued records request, subpoena, court order, or other compulsory legal  
76 process ("disclosure request"). To the extent possible and practical, the account holders for email  
77 and electronic files will be notified in advance of access or disclosure.

78 The public records officer, the research integrity officer or an attorney in the office of general counsel  
79 may order preservation of electronic records to comply with a disclosure request or to preserve  
80 records for purposes that may relate to pending investigations or litigation.

81 Access to email and electronic files must first be approved by the senior vice president for  
82 operations and finance, senior vice president and provost, general counsel or the president. Upon  
83 approval, attorneys in the office of general counsel may request or conduct targeted searches of  
84 electronic files to find material relevant to the disclosure request. In accessing the files, attorneys  
85 shall limit access to material that is relevant to the disclosure request.

86 **2.8 Health and Safety Emergency**

87 In the event of a health or safety emergency, Iowa State University may preserve, access, or  
88 disclose information containing all classes of data necessary and relevant to addressing the  
89 emergency situation.

90 **2.9 Authorization**

91 Iowa State University may preserve, access, or disclose information containing all classes of data  
92 relating to an individual student or employee upon the written authorization of the individual student  
93 or employee.

94 **2.10 Cookie Privacy**

95 Iowa State University complies with the [EU General Data Protection Regulation \(GDPR\)](#) as it relates  
96 to the use of cookies. ISU's **Cookie Privacy Disclosure** (*see Resources below*) provides  
97 information and instructions.

98 **Resources**

99 **Links**

- 100 • [Acceptable Use of Information Technology Resources policy](#)
- 101 • [Information Technology Security policy](#)
- 102 • [GDPR: Compliance with the European Union General Data Protection Regulation](#)
- 103 • [Office of General Counsel](#)
- 104 • [Public Records Officer](#)
- 105 • [Research Integrity Officer Dianah R. Ngonyama](#)
- 106 • [Data Classification policy](#)