Electronic Communications Policy Development Packet

Given the continuing increase in the use of electronic communications (e.g., texting, email, instant messaging, video chatting, Instagram, Facebook, Twitter), it is not surprising that families and Part C and Part B 619 providers are also using these technologies to communicate and share program information. State data governance policies can minimize the risks introduced by electronic communications by addressing its use. State policies can require implementation statewide, require local programs or agencies to develop and implement consistent policies and procedures, or require a combination of these two options. Please see the DaSy Data Governance and Management Toolkit for more information on Electronic Communications Policies and other data governance policies.

How to Use This Packet

1. Review and Complete the Considerations Worksheet for Electronic Communications Policy

The considerations include questions about general policy implementation and the procedures associated with work covered by this policy. A team knowledgeable about this content and the procedures should convene to discuss these considerations. The team assembled should, include but not necessarily be limited to relevant and knowledgeable Part C or Part B 619 staff. (Others might include, IT, broader data governance committee members, etc.)

Each lettered consideration in this worksheet references a corresponding number in Electronic Communications Policy Template. Consideration-specific notes should be captured on this worksheet and be used to refine the applicable section of the Electronic Communications Policy Template. After reflection and discussion by the team, a Part C or Part B 619 program may opt to exclude consideration content in their final policy.

1. Use Responses to the Considerations to Complete the *Electronic Communications* Policy Template

The Electronic Communications Policy Template is a fully modifiable document so that the resulting policy can be adapted to align with other states policies. Where appropriate, some basic content is included in the template; however, the content can and should be edited, added to, or deleted so the resulting policy accurately reflects the Part C or Part B data governance in this area. It may also be helpful to add links to policies referenced within the template.

The Electronic Communications Policy Template has 12 sections and there are one or more considerations that relate to each section. Sections vary in their depth and complexity, but all are important to fully describe the policy and the data governance and procedures covered by the policy. Each numbered section in this template references a corresponding letter in the Considerations Worksheet for Electronic Communications Policy. Once the policy is completed, there is no need to keep the lettered cross references to the associated considerations.

If you have questions about or would like assistance with this work, please contact: DaSy‑Center@sri.com

Considerations Worksheet for Electronic Communications Policy

| Considerations Worksheet for Electronic Communications Policy  |
| --- |
| *Considerations* | *Template Section* | *Notes/Status* | *Draft Language* |
| 1. Which, if any, federal laws/regulations (IDEA and FERPA) related to electronic communications apply to the Part C or Part B 619 program?
 | 1.1 | *See policy template for draft language.* |  |
| 1. What, if any, additional state agency policies related to electronic communications apply to the Part C or Part B 619 program?
 | 1.2 |  |  |
| 1. What specific Part C or Part B 619 data quality policies or procedures, if any, exist and apply to electronic communications?
 | 1.3 |  |  |
| 1. When did/does this policy take effect?
 | 2 |  |  |
| 1. Which Part C or Part B 619 role should be contacted for more information on this policy?
 | 3 |  |  |
| 1. How frequently will this policy be reviewed and, if needed, updated?
 | 4.1 |  |  |
| 1. What mechanisms will be used to collect user and other stakeholder input for consideration in the review and possible revisions to this policy?
 | 4.2 |  |  |
| 1. Where can the public access this policy?
 | 5.1 |  |  |
| 1. How will interested members of the public be informed of this policy?
 | 5.2 |  |  |
| 1. What parties (including participating agencies) will be required to follow this policy?
 | 6 |  |  |
| 1. What is the purpose of the Electronic Communications Policy?
 | 7 | *See policy template for draft language.* |  |
| 1. What is the definition of electronic communications?
 | 8 | *See policy template for draft language.* |  |
| 1. What data systems and data reported from these systems are covered by this Electronic Communications Policy?
 | 9 |  |  |
| 1. Which role is responsible for establishing and managing policies and procedures related to this policy?
 | 10.1 |  |  |
| 1. Which role is responsible for monitoring adherence to this policy?
 | 10.2 |  |  |
| 1. Which role is responsible for addressing questions regarding this policy?
 | 10.3 |  |  |
| 1. Which role is responsible for securing or providing training and technical assistance on data electronic communications?
 | 10.4 |  |  |
| 1. Which role is responsible for addressing failures to adhere to this policy?
 | 10.5 |  |  |
| 1. Which role is responsible for receiving reports of violations of this policy within the agency?
 | 10.6 |  |  |
| 1. Which role is responsible for establishing the circumstances when using electronic devices to communicate PII?
 | 11.1 |  |  |
| 1. Which role is responsible for establishing the procedures for authenticating the recipient’s identity?
 | 11.2 |  |  |
| 1. Which role is responsible for establishing the requirements for the use of personally owned devices for electronic communication when transferring PII?
 | 11.3 |  |  |
| 1. Which role is responsible for establishing the requirements for the use of personally owned devices for electronic communication for non-PII?
 | 11.4 |  |  |
| 1. Which role is responsible for maintaining current virus protection on applicable hardware?
 | 11.5 |  |  |
| 1. Which role is responsible for establishing encryption policies for circumstances that require electronic communication?
 | 11.6 |  |  |
| 1. Which role is responsible for establishing procedures to follow when a device is lost or damaged?
 | 11.7 |  |  |
| 1. Which role is responsible for trainings to support electronic communications?
 | 12.1 |  |  |
| 1. Which role is responsible for documentation to support electronic communications?
 | 12.2 |  |  |
| 1. Which role is responsible for collecting user input to support electronic communications?
 | 12.3 |  |  |

Electronic Communications Policy Template for
NAME OF PART C/PART B 619 PROGRAM

1. Requirements
	1. NAME OF STATE is federally required to protect personally identifiable PART C OR PART B 19 data during electronic communication. The following federal requirements (statutes/regulations/rules/policies) apply to electronic communication: (a)

34 CFR Part 300 – Part B Regulation

34 CFR 300.505

34 CFR Part 99 – FERPA Regulations

34 CFR 99.3

34 CFR 99.31(c)

* 1. The state requirements (statutes/regulations/rules/policies) that apply to electronic communications are: (b)

*(insert relevant state requirement)*

*(insert relevant state requirement)*

* 1. The PART C OR PART B 619 policies or procedures that apply to electronic communications are: (c)

*(insert relevant Part C or Part B 619 policy/procedure)*

*(insert relevant Part C or Part B 619 policy/procedure)*

1. Effective Policy Date

*(insert date)* (d)

1. Point of Contact

*(insert Part C or Part B 619 role or other contact as applicable)* (e)

1. Revisions

4.1 The Electronic Communications Policy will be reviewed and updated as needed/or *(insert frequency).* (f)

4.2 PART C OR PART B 619 will collect users and other stakeholders’ input through the following mechanisms to review and revise electronic communications policies and procedures. *(insert mechanisms)* (g)

4.3 Below is a listing of all policy revisions completed to date: *(insert version number, date, and associated notes)*

1. Access

5.1 The Electronic Communications Policy will be available to the public at *(insert URL).* (h)

5.2 Interested members of the public will be informed by *(insert mechanisms).* (i)

1. Relevant Parties

This policy applies to NAME OF PARTICIPATING AGENCY(IES) under TYPE OF MECHANISMS (e.g., contracts, subgrants, or interagency agreements). This includes staff from NAME OF LOCAL PROGRAMS/AGENCIES. All local programs, agencies, contractors, and staff identified in this policy must adhere to this policy. (j)

1. Purpose

The purpose of this policy regarding electronic communications is to establish authority and a process for ensuring protection of PART C OR PART B 619 personally identifiable information (PII) and other important data when sharing these data/this information from the PARTC/PART B 619 PROGRAM NAME through electronic communications (e.g., texting, email, instant messaging, video chatting, Instagram, Facebook, Twitter). (k)

1. Definition

*Electronic communication* methods covered by this policy include texting, email, messaging, video chat or sharing of videos, Facebook, Instagram, Twitter and any other applications facilitating content sharing through technology.

*Personally identifiable information* (PII) as defined by FERPA regulations at 34 CFR 99.3 includes information that can be used to distinguish or trace an individual’s identity either [directly](https://studentprivacy.ed.gov/glossary#glossary-node-210) or [indirectly](https://studentprivacy.ed.gov/glossary#glossary-node-227) through linkages with other information (e.g., name, address, student ID, birthdate, social security number).

*Record* as defined by FERPA regulations at 34 CFR 99.3 is, “any information recorded in any way, including, but not limited to, handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche.” (l)

1. Policy Application

The following PART C/PART B 619 PROGRAM NAME data systems are covered by this Electronic Communications Policy. (m)

| Data System | Description |
| --- | --- |
| *(data system name)* | *(description)* |
| *(data system name)* | *(description)* |
| *(data system name)* | *(description)* |
| *(insert data systems as needed)* | *(description)* |

1. Responsibilities

The table below outlines the specific responsibilities and roles related to electronic communications.

| Responsibilities | Data System | Role Responsible (by data system) |
| --- | --- | --- |
| 10.1 Establish and manage procedures related to this policy. (n) | *(data system name)**(data system name)* | *(role responsible)**(role responsible)* |
| 10.2 Monitor adherence to this policy. (o) | *(data system name)**(data system name)* | *(role responsible)**(role responsible)* |
| 10.3 Address questions regarding this policy. (p) | *(data system name)**(data system name)* | *(role responsible)**(role responsible)* |
| 10.4 Secure or provide training and technical assistance on data requests. (q) | *(data system name)**(data system name)* | *(role responsible)**(role responsible)* |
| 10.5 Address failures to adhere to this policy. (r) | *(data system name)**(data system name)* | *(role responsible)**(role responsible)* |
| 10.6 Receive reports of violations of this policy within the agency. (s) | *(data system name)**(data system name)* | *(role responsible)**(role responsible)* |
| *(insert other responsibilities as needed)* | *(data system name)**(data system name)* | *(role responsible)**(role responsible)* |

1. Procedures

The table below includes the procedures used to support this Electronic Communications Policy.

| Procedures | Role Responsible |
| --- | --- |
| 11.1 Communicate PII using electronic devices only under the following circumstances: *(insert circumstances)*. (t) | *(role responsible)* |
| 11.2 Authenticate the recipient’s identity by: *(insert procedures)*. (u) | *(role responsible)* |
| 11.3 Establish the requirements for the use of personally owned devices (e.g., mobile, computers) for electronic communication when transferring PII. *(insert requirements)*. (v) | *(role responsible)* |
| 11.4 Establish the requirements for the use of personally owned devices (e.g., mobile, computers) for electronic communication for non-PII. *(insert requirements*. (w) | *(role responsible)* |
| 11.5 Maintain current virus protection on applicable hardware. *(insert policies)*. (x) | *(role responsible)* |
| 11.6 Establish encryption policies for circumstances that require electronic communication. *(insert circumstances)*. (y) | *(role responsible)* |
| 11.7 Establish procedures to follow when a device is lost or damaged. *(insert procedures)*. (z)(See *Data Breach Response Policy* for loss or theft of equipment.) | *(role responsible)* |
| *(insert additional responsibilities as needed)* | *(role responsible)**(role responsible)* |

1. Responsibilities for Supporting Electronic Communications Policy

The table below includes the roles responsible for the tools and supports for this Electronic Communications Policy.

| Tool/Support  | Role Responsible  | Location  |
| --- | --- | --- |
| 12.1 Training(s) that support this policy. (aa) *(Training 1 name and description)* *(Training 2 name and description)* *(Include all trainings)*  | *(role responsible)* *(role responsible)*  | *(insert URL training location)*  |
| 12.2 Documentation that supports this policy. (bb) *(Document 1 name and description)* *(Document 2 name and description)* *(Include all documents, including any applicable forms or reports)*  | *(role responsible)* *(role responsible)*  | *(insert URL or document location)*  |
| 12.3 User input that is collected and used to support this policy. (cc) *(User input 1 description of input)* *(User input 2 description of input)* *(Include all user inputs)*  | *(role responsible)* *(role responsible)*  | *(insert URL or location with applicable content)*  |
| *(insert additional tools/supports as needed)* | *(role responsible)* | *(insert URL or location with applicable content)*  |