



## **SECTION II: COMMUNITY RELATIONS POLICY 2110**

### IDENTITY THEFT PREVENTION

This Policy is adopted to ensure compliance with the Fair and Accurate Credit Transaction Act, 15 USC. § 1601 et seq. and the Federal Trade Commission’s rules regarding Identity Theft (the “Red Flag Rules”). The District is subject to the Red Flag rules if it is a “Creditor.” The District is a Creditor if it provides any goods or services for a fee *and* as a matter of course extends credit to its customers by offering them the ability to pay for those goods and services *after* they are provided as opposed to requiring prepayment or contemporaneous payment. The District is a creditor with respect to limited areas involving a low risk of identity theft. Areas in which the District allows a debtor to defer payment owed the District include but are not limited to facility use charges and similar accounts. The District will review all of its “Accounts” to determine whether any of those accounts are “Covered Accounts.” As to “Covered Accounts,” it will develop an Identity Theft Program (herein referred to as the “Program”) designed to detect, prevent, and mitigate identity theft in connection with a Covered Account.

#### Definitions

For purposes of this Policy, the following definitions apply:

1. “Account” means a continuing relationship established by a person with the District to obtain a product or service for personal, family, household, or business purposes. Note that the requirements of the federal rules apply not only to existing accounts but also to new account openings, when a relationship has not yet been established.
2. “District” means the Broken Arrow Public School District.
3. “Covered Account” pertains to accounts which involve prepayment or contemporaneous payment as well as payment in arrears and means
  - a. An account that the District offers or maintains, primarily for personal, family or household purposes, that involves or is designed to permit multiple payments or transactions, such as a child care account, tuition account, or facility rental account and similar accounts;
  - b. any other account that the District offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the District from identity theft, including financial, operational, compliance, reputation, or litigation risks. This category of Accounts includes the District’s small business accounts, sole proprietorship accounts, and accounts for which the risk of identity theft is reasonably foreseeable because of how they are opened and accessed (i.e., they accounts can be accessed without face-to-face contact, such as through the Internet or by telephone).
4. “Credit” means the right granted by the District to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefore.



## **SECTION II: COMMUNITY RELATIONS POLICY 2110**

### IDENTITY THEFT PREVENTION

5. “Creditor” means a business or organization that regularly defers payment for goods or services or provides goods or services and bills customers later (as opposed to requiring prepayment or contemporaneous payment).
6. “Customer” means a person that has a covered account with the District.
7. “Identity Theft” means fraud committed or attempted using identifying information of another person without authority.
8. “Person” means a natural person, a corporation, government or governmental subdivision or agency, trust, estate, partnership, cooperative, or association.
9. “Personal Identifying Information” means a person’s credit card account information, debit card information, bank, bank account information, and driver’s license information and for a natural person includes their social security number, mother’s birth name, and date of birth.
10. “Red Flag” means a pattern, practice, or specific activity that indicates the possible existence of identity theft.
11. “Service Provider” means a person that provides a service directly to the District.

The District shall create an Identity Theft Program to protect Covered Accounts. At a minimum, the District’s Program will:

1. Identify and list the Covered Accounts.
2. Identify and list the red flags indicating that someone might be attempting to obtain services, products or information surreptitiously by claiming to be someone they are not.
3. Explain how the District will detect red flags that have been identified.
4. Explain how the District will respond if a red flag is detected.
5. Designate a senior administrative employee to administer the program.
6. Describe the District staff that needs to be trained on how to detect and respond to identity theft and the training they should receive.
7. To ensure the protection of the District’s clients from identity theft via the District’s contracted service providers, identify the categories of service providers that should be required via contract to assist the District in detecting red flags and must therefore either have their own red flags program or ensure compliance with the District’s red flags program.



## **SECTION II: COMMUNITY RELATIONS POLICY 2110**

### IDENTITY THEFT PREVENTION

8. Identify how the District will periodically reassess its operations to ensure that its red flag program reflects the current risks of identity theft to its clients (including, but not limited to, the types of records/accounts that are subject to the Red Flag Rules as Covered Accounts and the activities or occurrences that should be designated as a red flag for identity theft).
9. Be submitted to the District's board for approval.
10. Be annually re-evaluated to determine whether material changes have occurred warranting changes to the District's identity theft policy and program.

#### Updating the Program

Upon the recommendation of the superintendent, the board of education shall annually review and, as deemed necessary by the board, update the district's identity theft prevention program along with any relevant red flags in order to reflect changes in risks to customers or to the safety and soundness of the District and its covered accounts from identity theft. In so doing, the board of education shall consider the following factors and exercise its discretion in amending the program:

1. The District's experiences with identity theft.
2. Updates and methods of identity theft.
3. Updates and customary methods used to detect, prevent, and mitigate identity theft.
4. Updates on the types of accounts that the District offers or maintains.
5. Updates in service provider arrangements.

Source: *Broken Arrow Board of Education policy adoption, November 9, 2009.*  
*Broken Arrow Board of Education policy revised, July 10, 2017.*