DATA PRIVACY AGREEMENT

NEW HAMPSHIRE

NH-NDPA, Standard Version 1.0

MANCHESTER SCHOOL DISTRICT

and

BENEFITFOCUS.COM, INC.

This Data Privacy Agreement ("**DPA**") is entered into on the date of full execution (the "**Effective Date**") and is entered into by and between: Manchester School District, located at 20 Hecker St, Manchester, NH 03102 (the "**Local Education Agency**" or "**LEA**") and Benefitfocus.com, Inc., located at 100 Benefitfocus Way, Charleston, SC 29492 USA (the "**Provider**").

WHEREAS, the Provider is providing certain benefit administrative services to LEA pursuant to the Client Services Agreement ("Services Agreement").

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable employee information, protected health employee information, and other regulated employee data exchanged between them as required by applicable laws and regulations, including, but not limited to, applicable state privacy laws and regulations ("Data").

WHEREAS, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations and

WHEREAS, Provider is providing Services to LEA in its capacity as an Employer. The Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. Section 1232g; 34 CFR Part 99) is a federal privacy law that is designed to protect the privacy of student education records. FERPA provides rights to parents (child is 18 and under) and students (+18) with certain privacy rights regarding the education record. FERPA applies to any school that receives federal funds from the U.S. Department of Education; and

WHEREAS, FERPA does not apply to the services provided to LEA since Provider will not be receiving, viewing or processing education record(s) in any capacity while providing services to LEA.

NOW THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.

2. **Special Provisions.** *Check if Required*

   ☑ If checked, the Supplemental State Terms and attached hereto as **Exhibit "G"** are hereby incorporated by reference into this DPA in their entirety.

   ☑ If Checked, the Provider, has signed **Exhibit "E"** to the Standard Clauses, otherwise known as General Offer of Privacy Terms

3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.

4. This DPA, and Exhibit E, shall stay in effect for the duration of the Services Agreement.

5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in Exhibit A, or subsequent Order Form(s) signed by the Parties and incorporated by reference as a part of the Services Agreement (the "Services").

6. **Notices**. All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the Provider for this DPA is:

Name: Michelle Kraynak Title: Chief Privacy Officer

Address: _____

Phone: _____

Email: michelle.kraynak@voya.com

The designated representative for the LEA for this DPA is:

Stephen P. Cross, CIO
20 Hecker St., Manchester NH 03064
603-624-6300 x162
scross@mansd.org

IN WITNESS WHEREOF, LEA and Provider execute this DPA as of the Effective Date.

MANCHESTER SCHOOL DISTRICT

By: _*STEPHEN CROSS*_____
      STEPHEN CROSS (Jun 21, 2024 13:12 EDT)

Date: 06/21/24 _____

Printed Name: Stephen Cross _____

Title/Position: Executive Director of Information Technology _____

BENEFITFOCUS.COM, INC.

By: _Suzan LoCascio_____
      Suzan LoCascio (Jun 20, 2024 17:11 EDT)

Date: 06/20/24 _____

Printed Name: Suzan LoCascio _____

Title/Position: Asst. VP - Business Unit Controller _____

3

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA**. The purpose of this DPA is to describe the duties and responsibilities to protect LEA Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.

2. **DPA Definitions**. The definition of terms used in this DPA is found in **Exhibit "C".** In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, applicable terms of service, privacy policies etc.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Data Property of LEA**. All Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA.

2. Intentionally Omitted.

3. Intentionally Omitted.

4. **Law Enforcement Requests**. Should law enforcement or other government entities ("Requesting Party(ies)") contact Provider with a request for LEA Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.

5. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect LEA Data in a manner no less stringent than the applicable terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws**. LEA shall provide Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.

4

2. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Data.

3. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Data privacy and security, all as may be amended from time to time.

2. **Authorized Use**. The Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than to perform the Services outlined in Exhibit A, or subsequent Order Form(s) signed by the Parties, or stated in the Service Agreement and/or otherwise authorized under the applicable statutes referred to herein this DPA.

3. **Provider Employee Obligation**. Provider shall require all of Provider's employees and agents who have access to Data to comply with all applicable provisions of this DPA with respect to the Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Data pursuant to the Service Agreement.

4. **No Disclosure**. Provider acknowledges and agrees that it shall not make any re-disclosure of any Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Data other than as directed or permitted by the LEA in this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Data to any third party.

5. **De-Identified Data**: Provider agrees not to attempt to re-identify de-identified LEA Data. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy LEA Data. Except for Subprocessors, Provider agrees not to transfer de-identified LEA Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which de-identified data is presented. Nothing herein prohibits the Provider from publishing summary aggregate de-identified LEA data without LEA approval.

6. **Disposition of Data**. Upon written request from the LEA, Provider will return LEA data in its possession, custody or control, or certify the deletion or destruction of LEA data; provided, however, that the Provider may retain a copy of any LEA data to the extent (i) required by applicable law or (ii) it would be unreasonably burdensome to destroy (such as archived computer records). In the event that return or destruction of LEA data is unduly burdensome, or not feasible, Provider shall extend the protections of this DPA to the retained LEA data, and which protections and provisions shall survive the termination of

this DPA. The Provider agrees not to retain LEA data for any time longer than required by applicable law.

7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Data to (a) inform, influence, or enable Targeted Advertising, or (b) develop a profile of teachers for any purpose other than providing the Service to LEA.

ARTICLE V: DATA PROVISIONS

1. **Data Storage**. Where required by applicable law, Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Data is stored.

2. **Audits.** Upon written request by LEA, no more than once annually, Provider will provide LEA with Provider's most recent AICPA Service Organizational Control Type 2 (or the equivalent successor thereto) ("SOC") Reports, HiTrust Certification, or industry equivalent, which may be redacted as applicable, but shall include at a minimum the controls that Provider may audit from time to time in the ordinary course of its business.

3. **Regulatory Audits**. To the extent permitted, LEA shall notify Provider if a United States federal or state regulatory agency ("Regulator") requests a review audit or other examination of the Services or records maintained by Provider ("Regulatory Audit"). To the extent permitted by law, Provider shall provide LEA immediate written notice if a Regulator contacts Provider to conduct a Regulatory Audit of the Services or records maintained by Provider pertaining to the Agreement. Provider shall fully cooperate with LEA and the Regulator(s) in the event of a Regulatory Audit.

4. **Data Security**. The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect LEA Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security.

5. **Data Breach**. In the event of an unauthorized release, disclosure or acquisition of Data that compromises the security, confidentiality or integrity of the Data maintained by the Provider, the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:

    (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:

        i.   The name and contact information of the reporting LEA subject to this section.
        ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
        iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.

6

iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and

v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach .

(3) Provider further acknowledges and agrees to have a written incident response plan that reflects industry standard practices and is consistent with applicable federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of LEA Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.

(4) LEA shall provide notice and facts surrounding the breach to the affected employees.

(5) In the event of a breach originating from LEA's use of the Service, Provider shall reasonably cooperate with LEA to the extent necessary to expeditiously secure LEA Data.

ARTICLE VI: GENERAL OFFER OF TERMS

Provider may, by signing the attached form of "General Offer of Privacy Terms" (General Offer, attached hereto as **Exhibit "E"**), be bound by the terms of **Exhibit "E"** to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **Termination**. In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any service agreement or contract if the other party materially breaches any terms of this DPA, which breach continues for thirty (30) days after a written notice to cure such breach, or if cure is not possible within said thirty (30) day period, the breaching Party has not commenced reasonable steps to cure such breach.

2. **Effect of Termination Survival**. If the Service Agreement is terminated, the Provider shall dispose of all of LEA's data in accordance with Section IV.6 of this DPA.

3. **Priority of Agreements**. This DPA shall govern the treatment of Data in order to comply with the applicable privacy protections, including all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between the SDPC Standard Clauses and the Supplemental State Terms, if applicable, the Supplemental State Terms will control. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

7

4. **Entire Agreement**. This DPA and the Service Agreement constitute the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

5. **Severability**. Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

6. **Governing Law; Venue and Jurisdiction**. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF NEW HAMPSHIRE, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES.

7. **Successors Bound**: This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA . The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.

8. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of LEA Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Data and/or any portion thereof.

9. **Waiver**. No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

EXHIBIT "A"

DESCRIPTION OF SERVICES

The applicable description of services are defined in the Order Form(s) executed between LEA and Benefitfocus and contractually incorporated by reference into the Services Agreement.

EXHIBIT "B"
Intentionally Omitted

EXHIBIT "C"
DEFINITIONS

De-Identified Data and De-Identification: Records and information are considered to be de-identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific indivifdual.

Educational Records: Educational Records are not intended to be in scope under the Services Agreement.

Metadata: means information that provides meaning and context to other data being collected; including, but not limited to: date and time records and purpose of creation Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

Operator: means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is primarily used for benefit administrative services. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an "operator" for the purposes of this section.

Originating LEA: An LEA who originally executes the DPA in its entirety with the Provider.

Provider: For purposes of the DPA, the term "Provider" means provider benefit administrative services. Within the DPA the term "Provider" includes the term "Third Party" as used in applicable state statutes.

Student Generated Content: Student Generated Content is not intended to be in scope under the Services Agreement.

Service Agreement: Refers to the Client Services Agreement.

Student Data: Student Data is not intended to be in scope under the Services Agreement.

Subprocessor: For the purposes of this DPA, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its service, and who has access to LEA Data.

Subscribing LEA: An LEA that was not party to the original Service Agreement and who accepts the Provider's General Offer of Privacy Terms.

Targeted Advertising: means presenting an advertisement to an employee where the selection of the advertisement is based on Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such employee or the retention of such employee's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted advertising" does not include any advertising to an employee on an Internet web site based on the content of the web page or in response to a employee's response or request for information or feedback.

Third Party: Provider may subcontract third parties to perform services under the Service Agreement. Provider shall remain responsible and liable for subcontractor's performance of the services.

11

EXHIBIT "D"
Intentionally Omitted

EXHIBIT "F"
Intentionally Omitted

EXHIBIT "G"
New Hampshire

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in New Hampshire. Specifically, those laws are RSA 189:1-e and 189:65-68-a; RSA 186; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for New Hampshire;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. All references in the DPA to "LEA Data" shall include "Teacher Data."   **"Teacher Data"** is defined as at least the following:

Social security number.
Date of birth.
Personal street address.
Personal email address.
Personal telephone number
Performance evaluations.

Other information that, alone or in combination, is linked or linkable to a specific teacher, paraprofessional, principal, or administrator that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify any with reasonable certainty.

Information requested by a person who the department reasonably believes or knows the identity of the teacher, paraprofessional, principal, or administrator to whom the education record relates.

"Teacher" means teachers, paraprofessionals, principals, school employees, contractors, and other administrators.

2. In order to perform the Services described in the DPA, the LEA shall provide the categories of Teacher Data described in the Schedule of Data, attached hereto as **Exhibit "I".**
3. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
4. In Article IV, Section 7 amend each reference to "students," to state: "teachers,…"
5. Provider is prohibited from leasing, renting, or trading LEA Data to (a) market or advertise teachers; (b) inform, influence, or enable marketing, advertising or other commercial efforts by a Provider; (c) develop a profile of a teacher, for any commercial purpose other than providing the Service to LEA; or (d) use LEA Data for the development of commercial products or services, other than as necessary to provide the Service to the LEA.
 1. The Provider agrees to the following privacy and security standards. Specifically, the Provider agrees to:

15

(1) Limit system access to the types of transactions and functions that authorized users, such as students, parents, and LEA are permitted to execute;

(2) Limit unsuccessful logon attempts;

(3) Employ cryptographic mechanisms to protect the confidentiality of remote access sessions;

(4) Authorize wireless access prior to allowing such connections;

(5) Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity;

(6) Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions;

(7) Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles;

(8) Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services;

(9) Enforce a minimum password complexity and change of characters when new passwords are created;

(10) Perform maintenance on organizational systems;

(11) Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance;

(12) Ensure equipment removed for off-site maintenance is sanitized of any Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1;

(13) Protect (i.e., physically control and securely store) system media containing Student Data or Teacher Data, both paper and digital;

(14) Sanitize or destroy system media containing Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1 before disposal or release for reuse;

(15) Control access to media containing Student Data or Teacher Data and maintain accountability for media during transport outside of controlled areas;

(16) Periodically assess the security controls in organizational systems to determine if the controls are effective in their application and develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems;

(17) Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems;

16

(18)Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception);

(19)Protect the confidentiality of Student Data and Teacher Data at rest;

(20)Identify, report, and correct system flaws in a timely manner;

(21)Provide protection from malicious code (i.e. Antivirus and Antimalware) at designated locations within organizational systems;

(22)Monitor system security alerts and advisories and take action in response; and

(23)Update malicious code protection mechanisms when new releases are available.

Alternatively, the Provider agrees to comply with one of the following standards: (1) NIST SP 800-171 rev 2, Basic and Derived Requirements; (2) NIST SP 800-53 rev 4 or newer, Low Impact Baseline or higher; (3) FedRAMP (Federal Risk and Authorization Management Program); (4) ISO/IEC 27001:2013; (5) Center for Internet Security (CIS) Controls, v. 7.1, Implementation Group 1 or higher; (6) AICPA System and Organization Controls (SOC) 2, Type 2; and (7) Payment Card Industry Data Security Standard (PCI DSS), v3.2.1. The Provider will provide to the LEA on an annual basis and upon written request demonstration of successful certification of these alternative standards in the form of a national or international Certification document; an Authorization to Operate (ATO) issued by a state or federal agency, or by a recognized security standards body; or a Preliminary Authorization to Operate (PATO) issued by the FedRAMP Joint Authorization Board (JAB).

2. In the case of a data breach, as a part of the security breach notification outlined in Article V, Section 4(1), the Provider agrees to provide the following additional information:

     i. The estimated number of teachers affected by the breach, if any.

Category of Data	Elements	Check if used by your system
EXHIBIT "I" – TEACHER DATA		
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	X
	Other application technology meta data-Please specify:	X
Application Use Statistics	Meta data on user interaction with application	X
Communications	Online communications that are captured (emails, blog entries)	X
Demographics	Date of Birth	X
	Place of Birth	X
	Social Security Number	X
	Ethnicity or race	
	Other demographic information-Please specify:	
Personal Contact Information	Personal Address	x
	Personal Email	x
	Personal Phone	x
Performance evaluations	Performance Evaluation Information	
Schedule	Teacher scheduled courses	
	Teacher calendar	
Special Information	Medical alerts	
	Teacher disability information	
	Other indicator information-Please specify:	
Teacher Identifiers	Local (School district) ID number	X
	State ID number	
	Vendor/App assigned student ID number	
	Teacher app username	
	Teacher app passwords	
Teacher In App Performance	Program/application performance	
Teacher Survey Responses	Teacher responses to surveys or questionnaires	
Teacher work	Teacher generated content; writing, pictures etc.	
	Other teacher work data -Please specify:	
Education	Course grades from schooling	
	Other transcript data -Please specify:	
Other	Please list each additional data element used, stored or collected by your application	

Manche.DPA.20240618 Final Clean

Final Audit Report 2024-06-21

Created:	2024-06-19
By:	Ramah Hawley (rhawley@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAABG2QxqmRoZtQj6FdmCnEquAlHFUCq57A

"Manche.DPA.20240618 Final Clean" History

🗎 Document created by Ramah Hawley (rhawley@tec-coop.org)
2024-06-19 - 7:33:19 PM GMT

✉ Document emailed to Cynthia Lehrke (cynthia.lehrke@benefitfocus.com) for signature
2024-06-19 - 7:33:25 PM GMT

🗎 Email viewed by Cynthia Lehrke (cynthia.lehrke@benefitfocus.com)
2024-06-20 - 5:02:48 PM GMT

🗎 Document signing delegated to Suzan LoCascio (suzan.locascio@benefitfocus.com) by Cynthia Lehrke (cynthia.lehrke@benefitfocus.com)
2024-06-20 - 5:43:31 PM GMT

✉ Document emailed to Suzan LoCascio (suzan.locascio@benefitfocus.com) for signature
2024-06-20 - 5:43:31 PM GMT

🗎 Email viewed by Suzan LoCascio (suzan.locascio@benefitfocus.com)
2024-06-20 - 6:59:10 PM GMT

✍ Document e-signed by Suzan LoCascio (suzan.locascio@benefitfocus.com)
Signature Date: 2024-06-20 - 9:11:44 PM GMT - Time Source: server

✉ Document emailed to STEVE CROSS (scross@mansd.org) for signature
2024-06-20 - 9:11:46 PM GMT

🗎 Email viewed by STEVE CROSS (scross@mansd.org)
2024-06-21 - 5:10:21 PM GMT

✍ Signer STEVE CROSS (scross@mansd.org) entered name at signing as STEPHEN CROSS
2024-06-21 - 5:12:36 PM GMT

✍ Document e-signed by STEPHEN CROSS (scross@mansd.org)
Signature Date: 2024-06-21 - 5:12:38 PM GMT - Time Source: server

 Adobe Acrobat Sign

✅ Agreement completed.
2024-06-21 - 5:12:38 PM GMT