Cyber Security Policy
25

Data Protection

ISO/IEC 27001:2013 – Controls A.14.3.1, A.18.1.4, A.18.2.3

Contents

INTRODUCTION

PowerSchool handles valuable and very confidential information/data belonging to its clients. PowerSchool therefore takes very significant measures in ensuring the security and protection of the data which it handles. The company intends to maintain a relationship of trust and integrity with its clients and other interested parties at all times.

SCOPE

The scope of this policy is the control and appropriate monitoring of information and data exchange in the offices. PowerSchool's clients can therefore rest assured that their information and data is safe and secure.

RESPONSIBILITY

It is the responsibility of the Information Chief Information Security Officer (CISO), who is the central point of contact for all data protection issues. The Security Management Representative ensures company policy and practice are in compliance with the all protection principles listed in this document.

POLICY

DATA PROTECTION PRINCIPLES

- Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
  - At least one of the conditions set out in appendix B are met.
  - In the case of sensitive personal data, at least one of a further set of conditions set out in appendix C is met.
- Personal data shall be obtained for only one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose.

- Personal data shall be adequate, relevant and not excessive in relation to the purpose for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose.
- Personal data shall be processed in accordance with the rights of data subjects under the Act.
- Appropriate technical and organizational measures shall be taken against falsification, unauthorized or unlawful access, release, processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data shall not be transferred to a country or territory outside of United States unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.
- Any legal requests for records under "subpoena for production of evidence" will be limited to the scope of the records request.

DATA PROTECTION: RELATED TO CLIENTS, SUBCONTRACTORS, AND PARTNER ORGANIZATIONS

1) Personal Data gathered from customers, subcontractors, and partner organizations should be for a specific purpose which is made known to the individual and should not be used for any other purpose unless as outlined below. (Typically an application for a particular product or service) A list of acceptable reasons for processing personal data is given in appendix B.

2) The minimal personal data required to allow the required process should be recorded.

3) If the data is intended for any other purpose then, as a minimum, a standard opt-out clause should be included in the agreement. This agreement can in some instances be verbal (e.g. taken over the phone - but the resultant decision should be recorded) (See appendix D).

4) Where the data could be used for electronic marketing communications an opt-in

agreement is required. (see appendix D).

5) All forms of direct marketing will use data which has been subject to data protection permissions unless the individual is aware that the data was gathered specifically for direct marketing purposes. (see appendix D).

6) Email rental lists shall not be used by marketing unless data protection permissions can be demonstrated to have been given.

7) Departments should in general not hold sensitive personal data about an individual (see appendix C) (such data should not be required of clients and generally for employees should be held by HR).

8) All data held on individuals should be accurate and up to date.

9) Data should only be sent outside of the PowerSchool where the requirements in appendix E are met.

10) PowerSchool remains responsible for data sent to partners, subcontractors and suppliers and must take adequate steps to ensure that the data is only used in accordance with instructions.

11) Data must be protected against unauthorized processing, damage, accidental loss or destruction.

12) Data should not be sent outside of United States unless the conditions in appendix H are met.

13) Data should not be retained for a greater period than necessary for the purpose for which it was acquired (see appendix H).

14) Upon request the group must disclose any personal data it holds on an individual. This is called a data disclosure request.

15) Data shall be held in a manner which allows a customer data disclosure request for all permanent form data relating to them to be supplied within 60 days. (Exemptions to

this requirement are listed in appendix E).

16) Records of such data disclosure requests and responses shall be maintained.

17) Where a data subject requests that evaluation decisions concerning them should not be by electronic means alone then alternatives will be established (For example if we were to electronically score and prioritize suppliers).

DATA PROTECTION: RELATED TO EMPLOYEES (existing, past prospective or agency)

Data held on employees shall be the minimal required for the specific purposes related to employment and shall not be used for any other purpose without the positive consent of the employee. A list of acceptable reasons for processing personal data is given in appendix B.

Training on data protection related both to employee data and client data shall be included in induction training. Wherever practicable only HR should have access to sensitive personal data concerning employees (see appendix D).

1) Conditions for the lawful processing of sensitive personal data are set out in appendix C.

2) All data held on individuals should be accurate and current.

3) Data on employees can only be sent outside of PowerSchool where the conditions in appendix F are met.

4) Data should not be sent outside the United States unless the conditions in appendix G are met.

5) PowerSchool remains responsible for data sent outside of the group and must take adequate steps to ensure that the data is only used in accordance with instructions.

6) Data must be protected against unauthorized processing, damage, accidental loss or destruction.

7) Data should not be retained for a greater period than necessary for the purpose for which it was acquired (see appendix H).

8) Data shall be held in a manner which allows an employee access to data held about them upon request. Note that where data also relates to other employees then this need not necessarily be included. (Exceptions to this requirement are listed in appendix E).

9) Records of such data disclosure requests and responses shall be maintained.

10) Where a data subject requests that evaluation decisions concerning them should not be by electronic means alone then alternatives must be established. (e.g. electronic scoring of employees performance).

11) The business makes use of CCTV for reasons of security and occasionally to provide data on events such as incidents in the car parking area. Access to this data is strictly limited to those who need to know and no personal data will be disclosed other than for the business purposes described.

DATA PROTECTION: RELATED TO IT

Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Consideration should be given to technical security arrangements, both internal and external, including password protection, virus protection software, firewalls, data encryption, and building security measures.

Security must be borne in mind also where personal data is being destroyed.

IT should aspire to the data security requirements as set out in ISO 27001:2013.

Test data shall be selected carefully, protected and controlled.

Where personal data is to be carried out by a data processor (mailing houses, printing companies etc.) on behalf of the organization the selection criteria must include guarantees in respect of the technical and organizational measures governing the processes to be carried out (see appendix F).

Data must be protected against unauthorized processing, damage, accidental loss or destruction.

Data should not be retained for a greater period than necessary for the purpose for which it was acquired (see appendix H).

Data shall be held in a manner which allows data disclosure request for all permanent form data relating to them to be supplied within 60 days (Exemptions to this requirement are listed in appendix E).

Records of such data disclosure requests and responses shall be maintained.

EXCEPTIONS

Any exceptions to this policy must be approved, in writing, from the sponsor of this document.

REFERENCES

The Digital Privacy Act (latest version), and
The Personal Information Protection and Electronic Documents Act (PIPEDA) (latest version)

RELATED DOCUMENTATION

- Information Security Policy
- Password Security Policy
- Acceptable Use of Assets Policy
- Access Control Policy
- Supplier Security Policy

REVISIONS

This policy shall be reviewed and revised yearly and updated as needed

CHANGE CONTROL

Version	Date	Comments	Author	Owner
1.0	5/30/2017	Created	Thomas Orban	Nigel King
1.1	8/21/2017	Update for release of records under "subpoena for production of evidence" to be limited to the scope of the request.	Nigel King	Nigel King

Appendix A

Definitions

1. Data Subject

An individual who is the subject of personal data including:
- Employees
- Past employees
- Prospective employees
- Customers
- Partners
- Prospective customers
- Agency staff
- Subcontractors
- Suppliers

2. Personal Data

Any information that an organization holds and/or uses on individuals, including:
a) Employees
- Name and address
- Age and date of birth
- Telephone number
- Salary details and bank account information
- Appraisal disciplinary and holiday records
- Sickness and medical records
- Previous work history

b) Clients, subcontractors and suppliers
- Name of company and address
- Application data
- Visit reports

• Submitted information such as training or registration certificates
• Bank account details
• Telephone number

2. Data Controller
The organization that determines how personal data will be used.

3. Data Processor
An organization that processes personal data on behalf of a Data Controller, e.g.
• Mailing Houses
• Printing Companies

Appendix B

Reasons for using Personal Data

Personal data shall not be processed unless one of the following legitimizing conditions applies.

1. The data subject has given consent to the processing
2. The processing is necessary; for the performance of a contract to which the data subject is a party *or* for the taking of steps at the request of the data subject with a view to entering into a contract.
3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.
4. The processing is necessary in order to protect the vital interests of the data subject.
5. The processing is necessary:

   A.) for the administration of justice,
   B.) for the exercise of any functions conferred on any person by or under any enactment, or
   C.) for the exercise of any functions of the government.

for the exercise of any other functions of a public nature exercised in the public interest by any person.

the processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

Appendix C

Sensitive Personal Data and The reasons for using Sensitive Personal Data

Sensitive personal Data is:

a) The racial or ethnic origin of the data subject.
b) The subject's political opinions.
c) Religious beliefs or other beliefs of a similar nature.
d) Membership of a trade union.
e) Physical or mental health.
f) Sexual life.
g) Criminal activity.

The nineteen reasons for the lawful processing of sensitive personal data one of which must be met are as follows:

1) Explicit consent of the data subject.
2) Compliance with employment law obligations.
3) Vital interests of the data subject.
4) Processing by not for profit organizations.
5) Information made public by the data subject.
6) Legal advice and establishing of defending legal rights.
7) Public functions (administration of justice. Etc.)
8) Medical purposes.
9) Records on racial equality.
10) Detection of unlawful activity.
11) Protection of the public.
12) Public interest disclosure.
13) Confidential counseling.
14) Certain data relating to pensions.
15) Religious and health data for equality of treatment monitoring.
16) Legitimate political activities.

17) Research activities that are in the substantial public interest.
18) Police processing.
19) Processing by elected representatives.

Appendix D

Opt Out and Opt in for Customer Personal Data

Where customers and partners personal data may be used for a purpose other that for which the data was obtained then permission for that use must be obtained typically by use of an opt out or opt in clause. Where the data will be processed electronically to allow it to be used for other purposes then an opt in permission is required.

Examples of opt out and opt in clauses are as follows:
Example 1: Opt Out
PowerSchool would like to keep you informed of other activities carried out by the organization which may be of interest to you. Please tick this box if you do not wish us to keep you informed.

Example 2: Opt In
Please tick this box if you would like PowerSchool. to keep you informed of other activities carried out by the group which may be of interest to you.

Appendix E

Exemptions to Right of Subject Access

The right of subject access is extremely wide ranging and unless a relevant exemption applies (see below) an individual is generally entitled to see their personal data.

Exemptions

- Management forecasting – personal data used for this purpose is exempt from disclosure for as long as the management forecasting activity continues.
- Negotiations – personal data used for this purpose is exempt from disclosure for as long as the negotiations continue.
- Disproportionate effort – Rarely, it may be possible for a data controller to show that the effort that it would take to retrieve the requested information is too great.
- Confidential references – the author of a confidential reference is exempt from the need to disclose that reference.
- Prevention / detection of crime.
- Material disclosing third party information.
- Legal professional privilege (e.g. communication with the organization's lawyers concerning an employee).

Appendix F

Using third parties to process data

Where data is sent outside the group to be processed then responsibility for that data remains with PowerSchool and safeguards to ensure its protection must be taken including:

- Ensuring that the third party provides sufficient guarantees in respect of the technical and organizational security measures governing the process being carried out (typically by agreeing a contract which includes contractual requirements on data protection).
- Taking reasonable steps to ensure compliance with these measures (This can be limited to the above for simple processes but could extend to visits to the third parties premises where greater control is appropriate) Examples of third parties are call centers, printers, mailing houses, website hosts, etc.
- Considerations in contracts and controls applicable to third parties should include:
- Ensure that the processing by the third party is only in accordance with the PowerSchool's instructions.
- Ensure that the processing is undertaken only for the purposes and in the manner stated in the contract.
- Ensure the third parties staff are trained in data security measures.

- Ensure that there is a contractual undertaking in place which includes requirements to implement personal data security measures.
- Ensure that where appropriate the group has the right of access to the third party premises to ensure the security measures are being implemented.
- Restrict the third parties ability to sub-contract the process and its obligations.

Appendix G

Sending Data Abroad

'Personal data shall not be transferred to a country or territory outside United States unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.'

The principal derogations:
1. The data subject has given his consent to the transfer.
2. The transfer is necessary:
a) For the purpose of a contract between the data subject and the data controller.
b) For the taking of steps at the request of the data subject with a view to his entering into a contract with the data controller.
3. The transfer is necessary:
a) For the conclusion of a contract between the data controller and a person other than the data subject which is entered into at the request of the data subject or is in the interests of the data subject.
b) For the performance of such a contract.
4. The transfer:
a) Is necessary for the purpose of, or in connection with, any legal proceedings.
b) Is necessary for the purpose of obtaining legal advice,
c) Is otherwise necessary for the purposes of establishing, exercising; or defending legal rights.
It is strongly recommended that where data is transferred outside of United States that the Managing Director is consulted to allow the process to be legally compliant.

Appendix H

Data Retention Times Recommendations

Accounting Records: As required by taxation, customs and excise (usually 10 years).

Employee Records: Tax records for 7 years, Personnel records for 5 years after data subject leaves then a summary record for a further 5 years.

General Correspondence: Current and Previous year.