# Basic Knowledge regarding Personal Information Protection

August 2020

Borderlink, Inc.

# Four objectives of this training

① To understand privacy policies

② To understand the benefits and importance of privacy policies.

③ To understand the responsibilities and the roles of management

④ To understand possible outcomes in case of any offenses against the policies

# Policy for protecting personal information

(Objective)

BORDERLINK, INC.（hereinafter referred to as the “Company”）has established the following policy for the protection of personal information. In light of past incidents, the importance of handling personal information during business practice has been recognized and the Company has taken a preemptive stance regarding accidents or other troubles dealing with such personal information

(Fundamental policy)

BORDERLINK, INC.（hereinafter referred to as the “Company”）has established the following policy for the protection of personal information. In light of past incidents, the importance of handling personal information during business practice has been recognized and the Company has taken a preemptive stance regarding accidents or other trouble dealing with such personal information

(Strategies)

The Company believes that protecting personal information is a social responsibility that it must fulfill. The Company will implement the following measures;

**(1) Collection, use and provision of personal information**

Regarding all personal information that the Company uses, our collection, use and provision of it is done appropriately and we refrain from handling it beyond the extent necessary for attaining the specified purposes of usage or other such actions. When the Company intends to handle personal information beyond the extent necessary for attaining the specified purpose of usage, we will obtain prior consent from the person who provided the information to us.

**(2) Laws, regulations, guidelines and rules related to personal information**

The Company complies with laws, regulations and government-set guidelines and rules that are related to personal information.

**(3) Security management of personal information**

The Company implements reasonable preventive and corrective measures in relation to illegal access to personal information and leakage, loss, destruction, alteration, etc. of such information.

**(4) Complaints and requests for consultation related to personal information**

The Company quickly responds to complaints and requests for consultation related to personal information.

**(5) Measures to protect personal information (personal information management system)**

In order to appropriately protect personal information, the Company continuously reviews and improves the measures to do so.

# What is Personal Information (個人情報-Kojin Joho) ？

① Information about a certain person
② And it is identifiable who it is

- Full name
- Email address which can identify individuals by name and organization, such as "taro.suzuki@abc-kk.co.jp"
- Evaluation information of employees
- Any information relevant to the name

etc.

# These are Personal Information as well!

- Photos and videos of students
  They can identify individuals by school uniform or school name
- Recorded voice over an answering machine
  In the case that information can identify individual
- Information containing numbers
  Particular numbers such as bank account numbers, credit card numbers, employee numbers, health insurance numbers can identify the owner
- Contact Lists
  These may contain home address, name and telephone number

# Cases of Personal Information Leaking Incidents

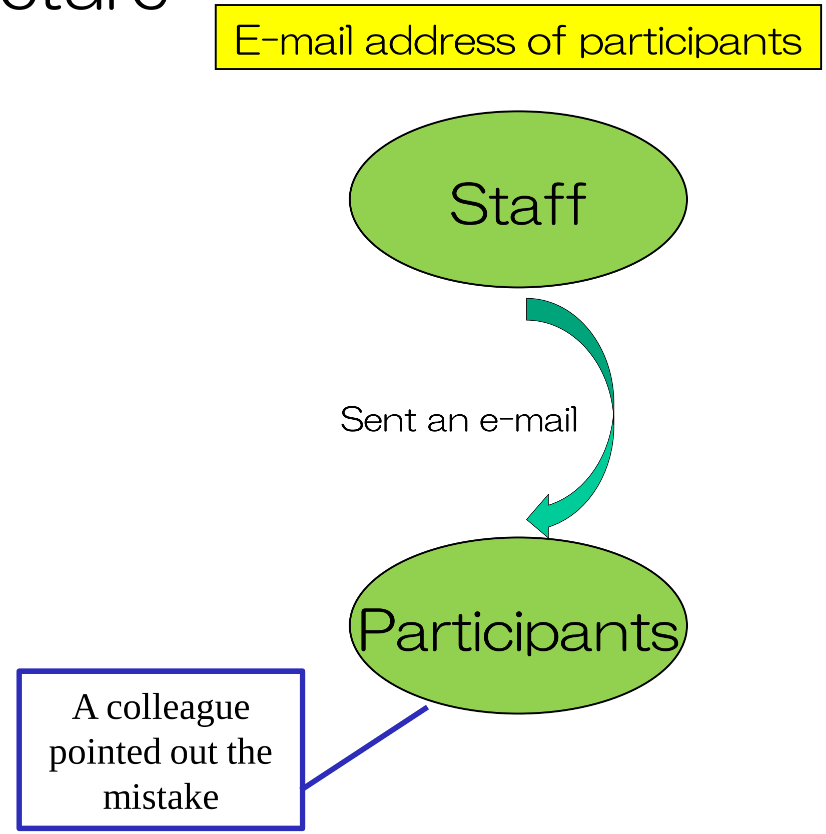
# Case①

## A private college in Gifu prefecture

This case is an e-mail mistake which occurred in a private college in Gifu prefecture. A staff member of the college mistakenly sent an e-mail regarding an online career counseling session.

He sent the e-mail to 11 recipients who were going to attend the online career counseling session. Instead of putting their email addresses in the ‘Bcc’ field,  he put their e-mail addresses in the  ‘To’ field and sent the e-mail. Eventually, their addresses were accidentally exposed to the other recipients.

After sending the e-mail, he was able to recognize his error when one of his co-workers pointed out the mistake to him. The college asked the all recipients to delete the e-mail.



E-mail address of participants

Staff

Sent an e-mail

Participants

A colleague pointed out the mistake

# Case②

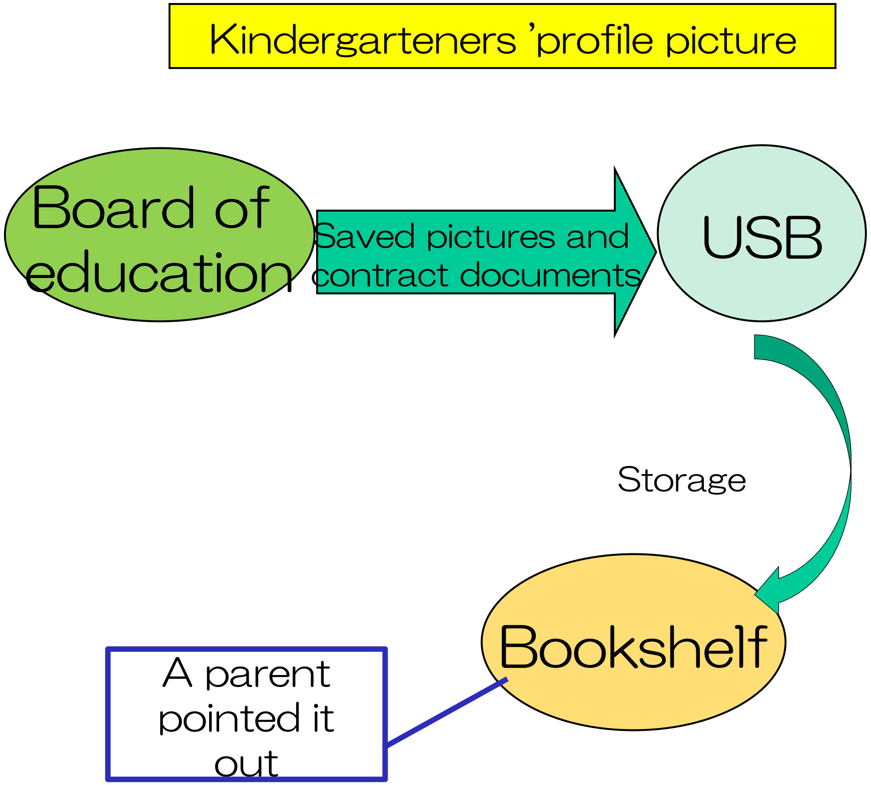
## Board of education in  Shiga prefecture

One of the departments of Board of education in Shiga prefecture lost a USB memory device in which some kindergarteners’ profile pictures were saved.

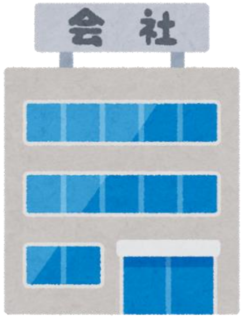
In the USB memory, some pictures in which the children’s faces were clearly seen were saved along with other documents such as important or sensitive contracts.
A password was set to the USB memory.

The loss become apparent as the USB was not found on the bookshelf where it should have been.

The department decided to store that kind of memory device in  a lockable storage area.


Kindergarteners ’profile picture
Board of education
Saved pictures and contract documents
USB
Storage
Bookshelf
A parent pointed it out

# Case ③

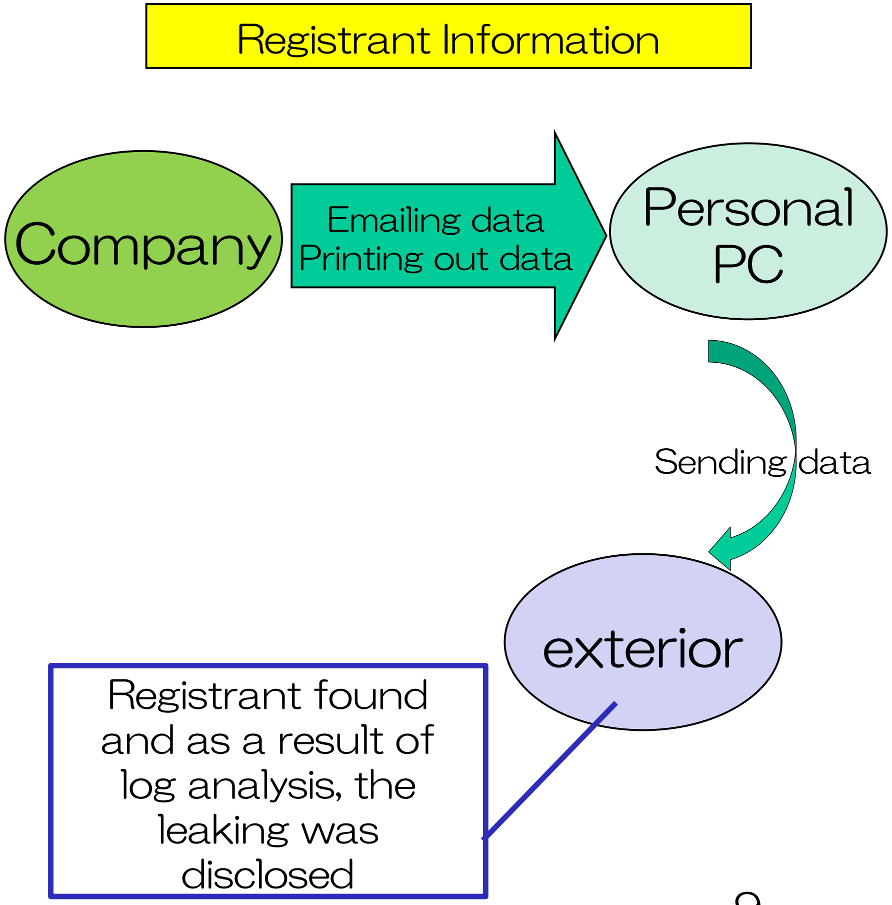


## Staffing Company

A resigned employee sent registrants' personal information to his private computer and printed out the data since February 2015.

15 thousands registrants' information (name, address etc.) was taken out from the company and these were sent to exterior via email. It did not include the information that could lead a financial damage, however, hourly wage rate of some of the registrants were also leaked.

Before resigning, the employee had launched a new company and brought out data for use in the sales of the new company. With the consent of the employee, all data was erased from his computer.



Registrant Information

Company

Emailing data
Printing out data

Personal PC

Sending data

exterior

Registrant found and as a result of log analysis, the leaking was disclosed

# Measures for preventing incidents

① External takeout restriction

② Data access control

- Access restriction
- Restriction of data download

③ Prohibition of use of personal IT devices

④ Better security of storage area of personal information and  keeping records

⑤Confirmation of address/numbers before sending emails and faxes

⑥ Exchange of document on confidentiality

⑦ Raising awareness about handling of personal information

- training

⑧ Refraining from having conversations including personal information in public places

# Company Rules to Prevent Personal Information Leakage

# Rules of PC usage

- Policies of PC usage
  - Password for PC should be changed regularly within a certain period of time (every month).
  - When you are away from the PC, screensaver should be act in order to prevent from being seen or accessed by inappropriate personnel.
  - When sending a file which contains personal information to outside the company, it should be protected either with encryption or password.
  - Laptop computer should be stored in a locked storage when work is done for safety precaution.
- Policies of taking PC out from the office
  - Taking IT devices out from the offices is only allowed with the proper authorization. When taking them out, you should use encryption or protect files with a password for the protection against data loss and leakage.
  - Bringing personal IT devices inside the company/school is prohibited. When needed, you need to get approval from the company/school.

# Rules of sending emails

- When sending emails
  - ＣＣ： Emails address can be seen from the receivers
  - ＢＣＣ： Emails address can’t be seen from the receivers

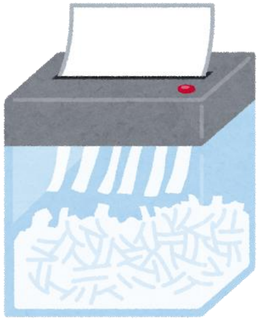
ＣＣ should not be used for mass email!!

It may be used depending on who is involved and what the topic of email is.

⇒ Double check if CCing is suitable.

# Rules of storage and disposal

- Storage and disposal of documents
  - Paper documents that contains any personal information should be disposed with shredding machine. In case of storing the documents before shredding, make sure to store it in a place where there is no possibility of it being lost or stolen.
  - Documents which contain any kinds of personal data should be stored in a locked storage.
  - Data files which contain any personal information should be completely deleted after retention period has expired.



# Rules in schools

- Information about students and teachers/staff
  - The documents which contains personal information of students, teachers and staff should not be taken out from the school.

    e.g.) students' list, exam paper

    ⇒It may lead the loss of the information.
- Taking photos
  - Taking photos and filming of students/teachers are not allowed in schools. Even if you get approval of that, make sure not to upload those pictures and videos on SNS, corporate website, brochures etc. without any permission from them.

# Rules of cell phone and smartphone

- Cell phone and smartphone for business use
  - If your company phone is lost or stolen, you should inform that to your supervisor immediately.
  - You should protect your cell phone and smartphone with password in case of it being lost or stolen.
  - As a smartphone running Google Android has not been virus scanned, make sure to install antivirus software as in the case of a PC and keep it updated.
  - Avoid downloading any new and unfamiliar software without careful consideration.

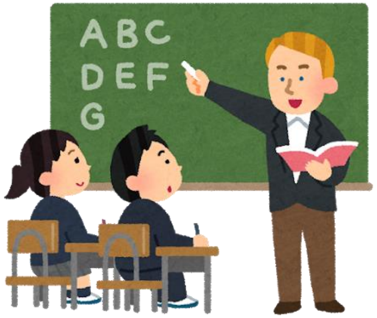
# Rules of SNS

- Be careful not to leak any personal information outside of the company
  - Never have conversations including personal information or any confidential information in public places such as elevator, train or restaurant.
  - Never make comments with any confidential company information or personal information on social media such as Twitter, Facebook and Line.
  - The written comments or uploaded photos may be used or saved by someone and there is also a possibility of it being misused or posted on another site unexpectedly.
  - The comments or photos may be forwarded by a person you do not know. This information can be dispersed widely throughout the Internet. Therefore, careless uploading may cause great trouble to not only yourself but also customers, co-workers or friends.

# Personal Information of Employee

- Never leak information outside of the company carelessly.
  - It is also very important information and should be treated with a great care just as same as other personal information.

⇒” Employee” include board members, full-time workers, contracted employees, temporary staff, part-time workers and any other type of workers.



# Punishment

In case that any accident happens as a result of breaking rules regarding dealing with personal information, there is a possibility of being fired or needing to pay damage compensation according to the company’s work regulations.

# Castigation (excerpt from work regulation)

- In the case personal information or my number is lost or leaked due to negligence
  - reprimand (apology letter), pay cut, suspension, demotion

- In the case of utilizing job duties to collect, use or leak the documents or data, in which personal information and my number are recorded, to make use of them other than for the job duties.
  - displacement, punitive dismissal

# Security Checklist

□ I use photos or work of students with the consent of themselves and their parents.

□ I have not seen irrelevant web pages to my work.

□ The computer’ s user ID and password are managed so as not to be know by others.

□ I always clean up my desk when I go home.

□ The documents and IT devices containing confidential information are destroyed or deleted in an appropriate manner.

□ I am always attentive not to send emails incorrectly.

□ Copied documents and printer output paper are always collected immediately.

# Personnel in charge of personal information

| Role and personnel | Responsibility |
|---|---|
| Company president<br>Yasumasa Yasui | As a CEO, he is in charge of designating the chief administrator and auditor of PMS (Personal information management systems), whom will implement proper PMS procedures. |
| Chief administrator of personal information<br>Yasumasa Yasui | As a chief administrator of PMS, he takes responsibility of handling and managing PMS information. |
| Controller of audit<br>Shiori Kusunoki | Makes sure that employees are in accordance with audit policies of personal information protection. Executes audits for the whole company and reports to the chief administrator. |
| Training supervisor<br>Yasumasa Yasui | Makes sure that the company are in accordance with the training policies, plan and executes training of PMS for all the employees. He reports to the chief administrator. |
| Administrator of PMS document<br>Yasumasa Yasui | Makes sure that the company is in accordance with administrative rules of documents with personal information. Keeps record of editing and in charge of disposing of all PMS documents. |
| IT chief administrator<br>Yasumasa Yasui | Takes responsibility of setting up and operating the company’ s IT system. |
| Entrance and exit administrator<br>Yasumasa Yasui | Takes responsibility of people’ s entrance and exit to the company’ s premises |