Bright Horizons

POLICY

Privacy and Information Security – Global Policy

This policy is designed to: (1) protect the security, confidentiality, and integrity of Bright Horizons' Protected Information (defined below), including information entrusted to Bright Horizons by its employees, clients, customers, and suppliers; and (2) meet corporate, legal, regulatory, contractual and information security and privacy certification requirements.

All individuals who have access to Protected Information are responsible for adhering to the requirements of this policy and each department head, director, and principal is responsible for their team's compliance.

Protected Information

This policy applies to the following types of information, collectively referred to as **"Protected Information:"**

1. **Personal Information or Personally Identifiable Information (PII)**. Any information that can be used on its own or with other information to directly or indirectly identify, contact, or locate a person is protected. This includes both public and non-public information which may be factual or non-factual regarding a person. Examples of PII include, but are not limited to:
    - Government identification numbers, such as social security numbers, national insurance numbers, driver's license numbers, passport numbers, etc.;
    - Health/medical information;
    - Financial data, including credit card, debit card, and bank account numbers;
    - Employment information, such as background check results, salary and benefit information, race/ethnic information, performance evaluations, and disciplinary records;
    - Telephone numbers, e-mail addresses, and home addresses;
    - Information about children/care recipients, including names, birthdates, medical history, dietary restrictions, custody information, etc.;
    - Photographs of children and clients, except those being used for Bright Horizons' purposes with applicable, signed permissions on file; and
    - Opinions about individual's actions or behavior.
2. **Restricted Information.** All Bright Horizons' business-related information that is not public and which could have a reputational, financial, legal, or operational impact on the organization if disclosed without authorization is protected. Examples of Restricted Information include, but are not limited to:
    - Merger/acquisition related information;
    - Financial statements before public release;
    - Methods of doing business, such as policies, procedures, practices, systems, products, services, business strategies, insurance information, client/vendor relationships, pricing, etc.;
    - Information about software developed for and/or used in the implementation of Bright Horizons' lines of business, services, or corporate functions;
    - Contracts, contract summaries/information, location transitions and closing information, legal documents, and investigative files;

- Financial and accounting information of any kind, including forecasts, budgets, and pricing; and
- Passwords, encryption keys, source codes.

3. **Special Categories of Personal Information.** Information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometrics, or genetic data are protected. In addition, Bright Horizons includes the following types of data in Special Categories of Personal Information: social security/national insurance numbers/BSN, bank account and credit/debit card details, and criminal histories.
4. **Client Information.** Non-public information concerning Bright Horizons' clients, their employees, and families, including all categories of information described in paragraphs 1-3 above are protected.

Use of Personal Information

Bright Horizons only permits the use of Personal Information for the purpose(s) for which Bright Horizons collected it. Personal Information may not be used for any new purpose unless 1) it is compatible with the original purpose; 2) consent is obtained from the individuals, or 3) there is a clear legal obligation for such new use. Any proposed, new use of Personal Information must be reported to the Privacy Team at dataprivacy@brighthorizons.com and approved **before** the new use is implemented.

Rights of Individuals

Some privacy laws give individuals rights to access or delete their Personal Information and require companies to respond within a limited timeframe. Failure to respond in a timely manner could result in fines to Bright Horizons by a government authority. The person receiving an individual's request to access or delete their data must take the following actions immediately:

- If the individual is located in or receiving services in the US, refer them to Bright Horizons Global Privacy Notice located on brighthorizons.com.
- If the individual is located or receiving services in the **United Kingdom, Europe, or Canada,** contact the Privacy Team at dataprivacy@brighthorizons.com.

Disclosure of Protected Information

All Protected Information must be treated as confidential. Only Bright Horizons' employees with a "need to know" and a legitimate business purpose may have access to relevant Protected Information. All third parties (e.g., suppliers, clients, etc.) may only have access to relevant Protected Information if there is a written agreement between Bright Horizons and the third party permitting such access. Unauthorized disclosure of Protected Information could impact an individual's rights and poses a reputational, financial, and legal risk to Bright Horizons.

Security of Protected Information

All employees, contractors, and consultants are responsible for the security of Protected Information in their area of responsibility as follows:

- **Files (physical**). All personnel files (for current and former employees) and client, customer, family and child files (for current or former participants/enrollees) stored at Bright Horizons locations and offices should be **kept in locked cabinets. inaccessible to others.** Access is

restricted to approved staff, until the files are either moved offsite for storage or destroyed. Files should not be removed from a location for any other reason.

- **Files (electronic).** Electronic files containing Protected Information must be housed on Bright Horizons' technology that is password protected and encrypted.
- **Technology**. All Bright Horizons devices are encrypted, and password protected. Computers, laptops, or tablets should be secured by activating screen lock or manual password protection when not in use or when the user leaves a workstation. Password protection should deploy automatically after several minutes of inactivity when a device is on.
    - Portable technology should be stored in a locked drawer or area with restricted access when not in use. Encrypted CDs or USB drives containing Protected Information should be secured in a locked drawer and should not be left attached to an unattended PC.
    - Mobile devices should not be left unattended at a workstation. Passwords may not be kept in a place or manner that is visible or easily accessible/ascertainable.
- **E-mail.** Encryption is required while transmitting Personal Information to, from, or within the United Kingdom, Europe, Canada, California, and elsewhere when Personal Information is being sent in bulk. Technical assistance is available by contacting the IT Department via a One Support.
- **Copying, Printing, Faxing, and Scanning**. Protected information may not be copied, printed, faxed, or scanned without valid business reasons. Printers, fax machines, and scanners should be located in an office or other secure area. Active fax machines should be checked periodically during the business day.
    - If Protected Information is being copied or printed, remove the original and/or printout from the printer promptly and secure them.
    - If Protected Information is being faxed, contact the recipient, agree on a time when the document will be sent, and ask the recipient to remove the incoming fax from the machine. If a fax is being received, stay with the fax machine during the transmission. Be sure to remove and secure all documents from the fax machine when the transmission is complete.
    - If Protected Information is being scanned, stay with the scanner while scanning the document, remove the document from the scanner, and secure the original document.

Personally Owned Devices

Protected Information may not be stored on any personally owned device including laptops and tablets unless the Mobile Device Management (MDM) application is installed.

Clear Screen and Desk Requirement

Documents containing Protected Information should be removed from users' workspace and secured in a locked drawer, cabinet, or office when not in use. Keys to these areas should be kept out of public view. Office/conference room white boards that contain Protected Information should be erased at the end of the meeting. Computer screens should be locked when away from the computer.

Offsite Storage

Some inactive Protected Information may be stored off site for designated periods of time. The File Retention Policy sets out categories of information and the retention time requirements. One Support

tickets may be submitted to transfer files to Bright Horizons' approved storage company. Destruction dates are required on all stored files.

Destruction

Protected Information must be destroyed properly, so that the information cannot be read or reconstructed. The following protocols must be observed:

- Documents and hard copy files containing Protected Information should be destroyed when they are no longer needed through cross-cut shredders or disposed of in a secure document disposal bin. If Protected Information is discovered on a printer or out in the open, it should be disposed of in a secure document disposal bin or brought to the responsible manager.
- Electronic files or data should be destroyed or anonymized according to approved data destruction procedures.
- Technology (including desktops, laptops, tablets, smartphones, network, and telecommunication equipment) should be disposed of by IT according to approved data destruction procedures.

Security video and digital recordings in nurseries and childcare centers should be erased in accordance with each geography's policy.

Reporting Requirement

Any employee who believes, observes, or suspects that Protected Information or Bright Horizons' technology has been compromised, accessed by or provided to unauthorized person, lost or stolen, or impacted by an information security weakness/vulnerability must make a report as soon as possible, but no later than 12 hours after becoming aware. The report should be made by email to dataprivacy@brighthorizons.com and with a copy to the employee's supervisor or other Bright Horizons manager.

Information Security and Privacy Objectives

Bright Horizons' information security and privacy objectives are set out in *Bright Horizons Business Management System for ISO 27001 and 2770*1 and *ISMS and PIMS Global Policy*.

Violations

Violations of this policy are reviewed on a case-by-case basis by HR, Information Security and Privacy Teams, and the appropriate supervisor. Violations may result in an Authorized User's loss of access or privileges to Bright Horizons technology. In addition, violations may result in disciplinary action, up to and including termination of employment, contract, or business relationship and/or filing a report with the appropriate government authorities if criminal or illegal activity may have occurred.

Related Policies, Procedures, Forms, and Supplemental Information:

- *Acceptable Use of Technology – Global Policy*
- *Bring Your Own Device – Global Policy*
- *ISMS and PIMS Policy for ISO 27001 and 27701*
- *Bright Horizons Business Management System for ISO 27001 and 27701*