

Bright Futures Information System (BFIS)

Access Request & Agreement



The BFIS Access Request & Agreement form must be completed before an employee can receive access to the internal and/or admin portals. If this form is not fully completed and signed by all parties, it will not be accepted.

Employee's Information

Full Legal Name:	Job Title:
Agency Name:	
Agency Mailing Address:	
City/State:	Zip Code:
Work Phone:	Work Email:

To Be Completed by Supervisor: Job Function(s)

A State of Vermont Designee will review and approve checked function(s).

(please select all that apply)	
<input type="checkbox"/> Agency of Education	<input type="checkbox"/> Food Program
<input type="checkbox"/> AHS Business Office	<input type="checkbox"/> Northern Lights Staff
<input type="checkbox"/> CDD Staff	<input type="checkbox"/> Reach Up
<input type="checkbox"/> Community Agency Director	<input type="checkbox"/> Referral
<input type="checkbox"/> CIS Child Care Coordinator	<input type="checkbox"/> Referral (Supervisor)
<input type="checkbox"/> CIS Coordinator (Supervisor)	<input type="checkbox"/> SOV Contractor/Agent
<input type="checkbox"/> Credential Worker (VAPC)	<input type="checkbox"/> STARS
<input type="checkbox"/> DCF IT	<input type="checkbox"/> Other (<i>explain in Additional Information box</i>)
<input type="checkbox"/> Dept. of Corrections	
<input type="checkbox"/> Dept. of Health	Extra Functions (For CDD Staff Only)
<input type="checkbox"/> Family Services Division	<input type="checkbox"/> Fingerprints
<input type="checkbox"/> FAP Eligibility Specialist	<input type="checkbox"/> Record Check Variance Request
<input type="checkbox"/> FAP Eligibility Specialist (Supervisor)	<input type="checkbox"/> Hide/Show Site Visits on Public Portal

Additional Information: Please describe the various functions the employee is expected to perform using BFIS.
--

Employee meets required qualifications to perform checked job function(s). <input type="checkbox"/> Yes <input type="checkbox"/> No

Agreements and Understandings

1. Child Development Division's (CDD) General Provisions

- 1.1 The CDD will provide BFIS electronic users access to their account at <http://www.brightfutures.vermont.gov> by issuing an individualized username and secure password.
- 1.2 The CDD will provide Bright Futures Help Desk support during state business hours. You may contact the Bright Futures Help Desk at 1-800-649-2642, option 4, bfis.help@vermont.gov, or by fax at 802-241-0847.
- 1.3 The CDD will disable user account access to the BFIS if inactivity within the system is greater than 3 months. To regain access a new *Internal User Access Request & Agreement* form is required.

2. BFIS Electronic Participants Statement of Agreement and Understanding

- 2.1 I agree to keep my password secret. I understand that for my protection I will be prompted by the BFIS to change my password periodically. I understand without a valid username and password; I will not have access to my BFIS account.
- 2.2 Non-disclosure of data: I will not disclose, in whole or in part, the data available to me to conduct assigned job duties, to any third party not specifically authorized by this agreement. I will not disclose directly to, or use for the benefit of, any third party confidential information. I understand and agree that the obligations of this paragraph shall survive the expiration or termination of this agreement.
- 2.3 I will keep my contact information current by updating my account electronically, or by notifying the Bright Futures Help Desk.
- 2.4 I agree and understand that the CDD is not responsible for my acts or omissions in connection with my electronic participation.
- 2.5 I agree and understand that the CDD has the right to terminate this agreement and my access to the BFIS for any reason at any time.
- 2.6 I understand that the CDD reserves the right to change this agreement and Understandings at any time by notice e-mailed to me at the most current email listed for me in the BFIS.
- 2.7 **I agree to notify the CDD immediately if I can no longer fulfill my responsibilities as an electronic participant for any reason, including termination of employment.**

Employee's Signature

By signing this form, I certify that I have read and understand the above agreements and understandings.

Full Legal Name (Print):	
Signature:	Date Signed:

Supervisor's Information and Signature

By signing I certify that the information provided on this form is true, and accurate.

I understand that it is my responsibility to:

- provide a Contractor/Agent with a copy of the Social Security Administration (SSA)/Vermont Agency of Human Services data exchange agreement and to ensure required training is completed prior to the initial disclosure of SSA data.
- notify the Bright Futures Help Desk when there are changes in this employee's job functions, or when the account needs to be closed.
- ensure that the employee has completed the required training (if *fingerprints* and/or *record check variance request* job functions were selected on page 1), and to obtain my **managers** initials here: _____, and date: _____.

Full Legal Name (Print):	Job Title:
Work Phone:	Work Email:
Signature:	Date Signed:

Please make a copy for your records and send this completed request to:

Child Development Division
280 State Drive, NOB 1 North
Waterbury, VT 05671-1040
(Fax) 802-241-0847
(Email) bfis.help@vermont.gov

DCF COMPUTER USERS AGREEMENT

DCF employees and contractors who have login access to DCF network files, electronic communications and/or databases acknowledge the following:

ACCESS TO DCF NETWORK AND DATABASES

- Because of the confidential and sensitive nature of information in DCF network folders and databases, use of computers that are part of the DCF network is generally restricted to DCF staff and contractors with valid DCF logins.
- Staff may allow others limited use of DCF computers if that use is appropriately supervised.
- DCF staff shall not access information stored in DCF databases or network files for reasons not directly related to the assessment of risk and delivery of services to children and families.
- These rules are also applicable to staff with login access to databases compiled and maintained by other departments of state government (e.g. PATH and Department of Corrections databases).

ELECTRONIC MAIL AND INTERNET ACCESS

- In accordance with State policy, a limited amount of personal internet use is allowed. This use shall NOT include applications that use excessive network bandwidth (e.g., music or other streaming output via the internet such as constantly updated sport scores or stock prices or instant messaging). This type of application causes network bottlenecks and interferes with the work of others.
- Electronic mail is not a confidential form of communication. Electronic backup copies of all e-mail communication are stored by DCF and may be accessible even if the user has deleted items.
- Users should not access another user's e-mail without the permission of that person or his/her supervisor.
- Material stored on department computers may be used as evidence in civil, criminal and internal investigations.
- E-mail is not to be used for offensive, potentially offensive, harassing or disruptive material, to lobby public officials or to make a profit.
- The user should know and follow the State of Vermont policy on Electronic Communication and Internet Use (Personnel Policy No. 11.7, attached).
- Employees who have state-owned computers in their homes may subscribe to personal internet service providers and use those computers for personal e-mail correspondence if that use does not involve installation of additional software (see section below on installation of software).

SYSTEM SECURITY

- Users should not include their password or any other security-related information in an e-mail message or other electronic file.

- Users will not allow others to use their DCF login/password, or their login/password for other Agency of Human Services databases, except that passwords may be shared with staff of the Division of Planning and Evaluation and/or local designee in order to facilitate computer trouble-shooting. Sharing of files among users should be accomplished by giving specified users electronic “permission” to read and or edit files in certain folders.
- All users should have a unique password. If you feel the security of your password has been compromised, change your password immediately.
- All users should log out when leaving their workstation for the day, in order to minimize security breaches.

USE AND INSTALLATION OF SOFTWARE

- Users will not install software on a state-owned notebook or desktop PC’s without the permission of the Division of Planning and Evaluation, including freeware or software licensed by the user.
- DCF PC/Workstations are equipped with a standard set of software intended to meet all office automation, client-data access, and web-browsing needs. Staff shall not install any other software on a state-owned computer, including screensavers. Wallpaper is not a software application and may be changed at will.
- Any staff member who has a work-related need for software not included in the standard configuration, should first get approval from his or her immediate supervisor. After approval of district director and division director, the request will be forwarded to DPE who will evaluate the requested software. Approved software may become part of the standard configuration or may be installed on a case-by-case basis.
- At any time, any DCF computer may be replaced by one with a standard configuration. When this happens, any unauthorized software will be lost, as will any files saved on the local hard drive, rather than on the server.

I have read and understand this agreement and the State of Vermont Personnel Policy on Electronic Communications and Internet Use. I agree to abide by their requirements.

Name (please print): _____

District: _____

Signed: _____

Date: _____

Original to Local Personnel File
 Copy to Employee
 Copy to Planning and Evaluation

State of Vermont

Personnel Policies and Procedures

Number 11.7

Effective Date: July 1, 1999

Subject: **ELECTRONIC COMMUNICATIONS AND INTERNET USE**

Applicable to: All classified, temporary and exempt employees of the State of Vermont, including all members of the executive branch and members of the boards and commissions who are authorized to use the State Internet service.

Issued By: Department of Personnel

Approved by: Kathleen C. Hoyt, Secretary of Administration

PURPOSE AND POLICY STATEMENT:

Internet services and e-mail capabilities are a resource to facilitate the work of State government. This policy provides for use by authorized State employees which is consistent with **Personnel Policies and Procedures**, Number 5.6, titled "Employee Conduct" which states that employees shall not use, or attempt to use State personnel, property or equipment for their private use or for any use not required for the proper discharge of their official duties. That policy has been interpreted to allow a limited degree of personal use of State telephones for private calls when such use meets certain guidelines. Similar allowances will be applied to Internet services and e-mail capabilities where personal use meets all of the following tests. No such use will be allowed where any of the following is not met.

- The user must be authorized to use the equipment by management. Managers will exercise reasonable discretion in determining which employees will be denied personal use of Internet services, including when such use is denied because of abuse or violation of this policy.
- The use must not interfere with an employee's performance of job duties.
- The use must not impose a burden on State resources as a result of frequency or volume of use.
- The use must not otherwise violate this policy, including the prohibition on access of sites that include potentially offensive or disruptive material. The fact that the use occurs in a private setting or outside of scheduled work hours does not affect this prohibition.

The State of Vermont purchases Internet services for use by State agencies to meet the operational and programmatic needs of their units. This policy provides guidelines for acceptable access and use and prohibits any Internet use by State employees that violates Federal or State laws or regulations.

As defined by this policy, systems and information are State property. All systems and information therein are, and shall remain, the property of each agency, subject to its sole

control. Each agency owns all legal rights to control, transfer, or use all or any part or product of its systems. All uses must comply with this policy. Nothing in this policy shall be construed to abridge any rights of an agency to control its systems, their uses or information. ***This policy does not impair the right and obligation of agencies to limit access to systems and records that contain information that is subject to any statutory, regulatory, or common law privilege or obligation to limit access, nor does it alter any agency's rights or obligations under the Vermont public records law (1 V.S.A. § 315, et seq.).***

Each State agency has full control and access as defined below:

Control. An appointing authority of an agency reserves and intends to exercise all rights relating to information used in its systems. An agency may trace, review, audit, access, intercept, block, restrict, screen, delete, recover, restore, publish or disclose any information at any time without notice.

Access. Passwords, scramblers or various encryption methods may not be used without agency approval, access and control. No user may attempt to access, copy, forward, delete, or alter the messages of any other user without agency authorization. An agency system may not be used to attempt unauthorized access to any information system.

DEFINITIONS

"Agency" means a state board, commission, department, agency, or other entity or officer of state government, other than the legislature and the courts.

"Agency systems" or "systems" means all agency software, electronic information devices, interconnections, intranet and technical information related to them. Systems include other systems accessed by or through those devices, such as the Internet, e-mail, or telephone services. Systems include designs, specifications, passwords, access codes and encryption codes.

"Electronic communications" means electronic mail and Internet service access.

"Information" means information of any kind, used in any way, in agency systems.

Examples include messages, communications, e-mails, files, records, recordings, transmissions, signals, programs, macros, and data.

GUIDELINES FOR GENERAL USE OF SYSTEMS OR INTERNET SERVICES

1. Employees with access to systems or the Internet have the responsibility not to disclose their access codes or passwords.
2. No employee shall send e-mail that is, or appears to be, sent from another employee's e-mail or that attempts to mask identity.
3. State employees must conform to reasonable professional standards for use of Internet services as detailed in this guideline. This includes a prohibition against any activity that impairs operation of any state computer resource. Such activities include, but are not

limited to, sending junk mail or chain letters, injecting computer viruses or mass mailings via e-mail.

4. Employees must respect intellectual property rights at all times when obtaining information over the Internet. Copyrighted or licensed information shall be used only with full legal right to do so.
5. Use of the Internet is for State business. The only exception is for personal use that fully complies with the limited personal use described by this policy. Any use that is not for State business or authorized limited personal use consistent with this policy may result in revocation of Internet access, other appropriate administrative action, or disciplinary or corrective action.
6. Use of agency systems or printers for offensive or disruptive purposes is prohibited. This prohibition includes profanity, vulgarity, sexual content or character slurs. Inappropriate reference to race, color, age, gender, sexual orientation, religions, national origin or disability is prohibited.
7. State agencies have the right to monitor the systems and Internet activities of employees. Monitoring may occur, but is not limited to, occasions when there is a reason to suspect that an employee is involved in activities that are prohibited by law, violate State policy or regulations, or jeopardize the integrity and/or performance of the computer systems of State government. Monitoring may also occur in the normal course of network administration and trouble-shooting, or on a random basis. ***Agencies must ensure that systems administrators and technicians involved in monitoring, or who otherwise have access to systems and records that contain information that is subject to any statutory, regulatory, or common law privilege or obligation to limit access, are appropriately trained on the requirement to respect such privilege or confidentiality and directed to do so.***
8. Use of fee-for-service providers is not allowed unless the necessary approvals and funding have been obtained in advance. An employee who obligates a State agency to pay for services without prior approval may be held personally liable for those costs and may be subject to disciplinary action up to and including dismissal.
9. Prohibited activities also include, but are not limited to the following: lobbying public officials or asking others to lobby in their behalf, printing and/or distributing information from the Internet that is obscene, potentially offensive, harassing or disruptive.
10. Using or allowing others to use State Internet services or e-mail accounts to conduct transactions or advertising for a personal profit-making business is strictly forbidden.

Signed By Kathleen C. Hoyt, January 11, 2000

Approved, Secretary of Administration