Site Coordinator Training

Coordinator Roles and Responsibilities

According to Publication 5683, VITA/TCE Handbook for Partners and Site Coordinators, coordinators must:

- Follow all site operating procedures.
- Be available while the site is in operation (may be available at the site, by phone, or other electronic means).
- Ensure all volunteers follow the QSR and VSC.
- Share Volunteer Tax Alerts (VTA), Quality Site Requirements Alerts (QSRA), and technical updates with all volunteers during the filing season.

Site Reviews and Visits

SPEC conducts site reviews to ensure adherence to QSR through:

- Field Site Visits (FSV): Tax consultants make unannounced, in person visits to aid or offer guidance, identify and share best practices, and strengthen adherence to QSR. FSV include one return review.
- Remote Site Reviews (RSR): Tax consultants schedule a convenient time to conduct RSR by conference call, video or other approved virtual method with the coordinator and discuss overall site operations.
- Partner Reviews: SPEC strongly encourages partners to conduct reviews to ensure site adherence to all VSC and QSR for efficient operation and high ethical standards during tax return preparation.
- Quality Statistical Sample (QSS) Reviews: QSS reviews are in-person visits to a sample of VITA/TCE sites across the country. QSS reviews include a site review and a review of three tax returns.

Site Coordinator Training and Test

- **All** coordinators and alternate coordinators are required to complete Site Coordinator Training.
    - They must also pass Volunteer Standards of Conduct (VSC) and Site Coordinator Test certifications prior to performing any site coordinator duties.
- The Site Coordinator Test certification requires a passing score of 80%

Continuing Education Credits

- Volunteers requesting Continuing Education (CE) credits must be an Enrolled Agent (EA), Certified Public Accountant (CPA), Attorney, Certified Financial Planner (CFP) or California Tax Education Council (CTEC) Registered Tax Return Preparer.
- The Circular 230 test does not qualify volunteers for CE credits.

Consents

For VITA/TCE sites there are different consent forms for taxpayer data:

- Disclose: the giving out of information, either voluntarily or to comply with legal regulations or workplace rules
  - If a taxpayer denies these consents, the return can still be e-filed.
- Use: the act or practice of employing something
  - If a taxpayer denies these consents, the return can still be e-filed.

Consent to Disclosure of Tax Return Information Form must be completed and signed if the taxpayer would like a CFR Reloadable Focus Card for their refund, or if a City of Detroit HOPE application is completed.

Consents Continued

For VITA/TCE sites there are different consent forms for taxpayer data:

- Relational EFIN:
  - The relational electronic filing identification number (EFIN) process requires the tax preparation software provider to share return data with a third party, generally the primary partner for the purpose of receiving reports.
  - Since taxpayer data is shared when electronically filing, taxpayers must consent to disclose their data.
  - If the taxpayer does not grant consent or does not enter a personal identification number (PIN) and date at a VITA site, the partner **cannot** e-file the return since the relational EFIN process shares the data with the preparing site and the primary sponsor at the point the return is acknowledged.

Consents Continued

For VITA/TCE sites there are different consent forms for taxpayer data:

- Global Carry Forward:
  - Discussed earlier, Form 15080 on back of federal intake
  - Reminder, if a taxpayer denies this consent, the return **can** still be e-filed.
- Virtual:
  - Form 14446, Virtual VITA/TCE Taxpayer Consent, is required when any part of the tax return preparation process is completed without in-person interaction between the taxpayer and the VITA/TCE volunteer.
  - The site must explain to the taxpayer the process used to prepare the taxpayer's return.

IRS-Loaned Equipment

Use of IRS-loaned equipment is restricted to preparation and filing of electronic tax returns and related program activities such as:

- Training and educating volunteers and taxpayers
- Promoting VITA/TCE activities and
- Administering volunteer electronic tax return preparation and filing

Equipment may not be used for:

- Commercial purposes
- Games
- Collateral, exchange or sale or
- Personal use

Rules for Safeguarding Equipment

Rules to prevent a loss or theft of equipment include:

- Do not leave the laptop or printer in a vehicle where it is visible. When transporting equipment, lock in the trunk or under cover on the floor of the vehicle.
- Do not store the laptop or printer in a vehicle; use vehicles for transporting only.
- Do not leave the laptop or printer unattended in a public location.
- Do not leave the laptop or printer in a closet or cabinet that does not lock and where access is not limited.
- Do not expose the laptop or printer to extreme weather (hot or cold).
- Keep away from hazards such as liquids, food, and smoke.

Reporting Lost or Stolen Equipment

- Partners agree to **immediately** notify the IRS of IRS-loaned equipment (computers and printers) that is stolen or lost, but **not later than the next business day**, after confirmation of the incident.
- Partners should provide all readily available information to their local SPEC territory office.
- In the event of a theft, the partner must notify law enforcement immediately and file the appropriate reports.
- The SPEC territory office will complete an incident assessment within ten (10) business days to assist the IRS with documentation.

VITA/TCE Security Plan

All VITA/TCE sites must prepare an **annual** security plan to safeguard taxpayer data.

- Prepare and submit Form 15272, VITA/TCE Security Plan, or similar document containing the same information.
- The security plan must be provided annually to the local SPEC territory office by December 31 for review and approval.
- A physical or electronic copy of the approved security plan must be returned to the coordinator and maintained at the site.
- Coordinators must ensure volunteers are familiar with the security and virtual plan policies to keep taxpayer information secure and confidential.

Software Security Features

- Volunteer access to taxpayer data should generally be limited outside of site operating hours. Coordinators should generally use the features in the tax software that restrict volunteer access to tax returns outside of site operating hours.
- When volunteers quit, resign, or are no longer working at the site, the coordinator must immediately deactivate their usernames.
- Modify users' permissions, as appropriate, to ensure users only have the necessary permissions to perform their duties. To minimize security risks volunteers generally should not have multiple user roles in the tax software.

Wi-Fi and Wireless Connections

- IRS recommends the use of wired connections when transmitting taxpayer information via the internet.
- Wi-Fi or wireless connections must be encrypted and password-protected.
- The use of unprotected public wireless networks is prohibited.

Privacy During the Interview

It is important for taxpayer information to be protected during the return preparation process including during the interview and discussions with the taxpayers.

- Arrange tax preparation areas to limit unauthorized access to taxpayer information and ensure privacy. For example, use partitions if available, face tables in different directions, and make use of the space in the area.
- During conversations with taxpayers, personally identifiable information (PII) should not be discussed out loud so others may overhear. PII includes Social Security numbers (SSN), addresses, bank account numbers, etc.

Volunteer Identification and Certification

- Verify that every volunteer (including you) has signed and dated Form 13615, Volunteer Standards of Conduct Agreement – VITA/TCE Programs, prior to working at the site.
- Validate certification tax law levels for each volunteer.
- Validate the identity, name and address of all volunteers using government-issued photo identification prior to the volunteer working at a VITA/TCE site.
- If the volunteer's name and address do not match, the volunteer needs to update their "My Account" page in Link & Learn Taxes with their valid name and address.

Types of Data Breaches

A VITA/TCE data breach occurs when a taxpayer's personally identifiable information (PII) is shared, used or disclosed, whether physically or electronically, without taxpayer permission.

Types of data breaches:

- Unintentional (a mistake) – volunteer mistakenly provided a copy of another taxpayer’s tax return or tax documents in error.
- Intentional (on purpose)– data loss incidents such as accessing a volunteer preparer network without permission and/or theft of PII.

Reporting a Potential Data Breach

When a potential data breach occurs (unintentional or intentional), partners must contact their local SPEC territory office immediately upon confirmation of the incident. The territory office must review the details of the incident and determine if it meets the criteria of a potential data breach.

If it is determined there was a potential data breach, partners must provide the following:

- Date the incident occurred
- Brief description of the data breach
- Full name and telephone number for the point of contact who reported the data breach
- Partner name and address
- Site name and address