Technology Use and Security Policies and Best Practices

Shawn Michael - NPower Oregon Director and Senior Associate for Technology
Technology Use

- Know what your systems are
- Know how your systems are used:
  - Remote
  - On-site
  - Personal Use
  - External System Integrations
Create Applicable Policies

- Policies that are not enforced can come back to bite you!
- Depending on how your systems are used, and what they are, some “best practice” policies may not be applicable
  - Example: If you have staff that routinely work from home computers on an organizational system, it is impossible to enforce what other software may be installed on that computer.
  - Solution: Make an organizational commitment to providing staff with work stations that they can use remotely
Policies and Best Practices to Consider

- **Standard IT Policies and Procedures Outline**
- Accessibility
- Back Up and Disaster Recovery
- Acceptable Use
- Confidential Data Protection
- Health and Safety
Accessibility

- Making your technology accessible to staff, volunteers and clients with disabilities, if not required by law, certainly is considered best practice.
  - Web site standards
  - Language
  - Alternative input devices
Back Up and Disaster Recovery

Do you have a plan to resume operations if any of these happen?

- Physical Disaster – fire, flood
- System Failure – parts fail, database becomes corrupted
- Attack – hackers attack your network or web site, someone steals your computer
Back Up and Disaster Recovery (cont)

- Make a plan – it does not need to be complicated:
  - Back up your data
  - Take the back up physically off-site or save it off-site
  - Have paper forms to collect data
Acceptable Use

- What is acceptable?
  - Personal email
  - Games during breaks
  - Political information sharing
  - Purchasing new software
  - Offensive Material – who decides what is offensive?
Acceptable Use (cont)

- For items identified as “not acceptable” –
  - How are people informed of the policy?
  - How do you identify a policy breach?
  - What are the consequences – disciplinary action?
Confidential Data Protection

- What information should be considered confidential?
  - Employee personal information
  - Funder/Donor personal or financial information
  - Client personal information
    - Contact Information (address, phone, email)
    - Services provided
    - Assessment data
    - Health-related data

- What do you share with Partners?
  - Do you need a release?
Health and Safety

- Ergonomic Standards
- Options for staff –
  - Furniture
  - Workstation Configuration
  - Peripherals – mouse, keyboard
Helpful Links and Resources

- NPower – Guides and Papers
  - [http://www.npower.org/resources/guides-and-papers](http://www.npower.org/resources/guides-and-papers)

- NPower – Tools
  - [http://www.npower.org/resources/tools](http://www.npower.org/resources/tools)

- Fieldstone Alliance:
  - [http://www.fieldstonealliance.org/productdetails.cfm?PC=60](http://www.fieldstonealliance.org/productdetails.cfm?PC=60)