Citizens Online

SAFEGUARDING VULNERABLE ADULTS POLICY – UPDATED January 2021.

Aim

Citizens Online is committed to the wellbeing and safeguarding of vulnerable adults, and is determined to ensure all necessary steps are taken to protect vulnerable adults from harm. This policy and the accompanying procedure outlines the principles and values of the company and is designed to ensure that all staff understand their responsibilities in protecting children and vulnerable adults and those requiring protection from harm and neglect. It also identifies the steps staff should take if abuse of an adult occurs or is suspected.

When we refer to staff in this policy, we also mean volunteers and consultants that may be undertaking work on behalf of Citizens Online, for example, Digital Champions.

Roles and Responsibilities

The policy applies to all staff of Citizens Online who may come into contact with vulnerable adults. It also applies to other vulnerable adults in the wider community that come to the attention of Citizens Online staff and or representatives in the course of their work or duties.

Safeguarding is everyone's responsibility and all staff should have a basic understanding of their role in protecting vulnerable adults. Citizens Online requires that all staff undertake a Disclosure and Barring Service (DBS) request for staff working with vulnerable adults as part of the recruitment process.

Line Managers are responsible for ensuring that this policy is being adhered to. The Lone Worker Policy, the Lone Worker Safety Guidance and this policy will be brought to the attention of all staff by their line managers through the mandatory induction programme.

Staff (with support from their line managers) are responsible for:

- Understanding and adhering to the Safeguarding Policy.
- Attending appropriate training related to safeguarding if asked to do so.
- Reporting any concerns to their manager in writing as soon as is reasonably practicable
- Reporting of all adverse incidents, as soon as possible, to their line manager and the Operations Manager.
- Treat all vulnerable adults with whom they come into contact while carrying out their work equally and with respect.

Line Managers

All Managers will ensure all concerns and allegations of abuse are taken seriously and responded to appropriately.

- Provide advice and information relating to safeguarding concerns.
- Receive and record information from staff who have safeguarding concerns.
- Where appropriate assessing the information promptly and carefully, clarifying or obtaining more information about the matter as appropriate.
- Where appropriate, consulting initially with local Adult Services about the concerns as soon as possible, and in emergencies the Police.
- Providing training at the level identified as appropriate for all posts within the organisation and in particular ensuring that all staff who work with or have contact with vulnerable adults are appropriately trained.

Policy Statement

Definition of vulnerable adults
An adult at risk of abuse or neglect is defined as someone who has needs for care and support, who is experiencing, or at risk of, abuse or neglect and as a result of their care needs - is unable to protect themselves. *The Care Act 2014*

Definition of abuse
Abuse is defined as… "a violation of an individual's human and civil rights by any other person or persons." *(Department of Health 2000)*

Abuse of a person at risk may consist of a single act or repeated acts. It may be an act of neglect or omission to act, it may occur where a vulnerable person is persuaded to enter into a financial or sexual transaction to which they do not or cannot consent. Abuse can occur in any relationship and any setting and may result in significant harm to, or exploitation of the individual. In many cases it may be a criminal offence.

What to look out for
All staff have a responsibility to look out for safeguarding issues, however our digital champions are often in the best position to notice these as they are out in the community assisting learners. While assisting learners, Digital Champions (DC's) may come across situations that are concerning. These may include:

Institutional abuse
Institutional abuse occurs when the routines, system and regimes of an institution result in poor or inadequate standards of care and poor practice, which affects the whole environment and denies and restricts the dignity, privacy, choice and independence of an individual.

Example: while visiting delivering a session in a care setting, the learner may mention that they haven't been eating regularly, or haven't been provided with adequate food or water.

Hate crime
Hate crime is defined as any crime that is perceived by the victim, or any other person to be racist, homophobic, transphobic or due to a person's religion, belief, gender identity or disability.

Example: A learner may mention that they someone in their sheltered housing complex has been hurling homophobic abuse at them when they walk past their house.

Mate crime
Mate crime happens when someone is faking a friendship in order to take advantage of a vulnerable person. Mate crime is committed by someone known to the person. A 'mate' may be a 'friend', family member, supporter, paid staff or another person with a disability.

Example: A learner may say to a Digital Champion, "my mate is always borrowing money from me and never returning it."

Domestic abuse
Domestic violence is defined as "Any incident or pattern of incidents of controlling, coercive or threatening behaviour, violence or abuse between those aged 16 or over who are or have been intimate partners or family members regardless to gender or sexuality. This can be the following, but the list is not limited to these types of abuse:

- Psychological

- Physical
- Sexual
- Financial
- Emotional

Example: A learner may tell a Digital Champion that their partner restricts their movements, such as not allowing them out of the house in the evening to see their friends. Or a Digital Champion may notice that a learner turns up to each session with fresh bruises or other injuries.

Personal budgets, direct payments and self-directed care

People who direct their own care and support should be enabled to manage their personal budgets and direct payments in a safe way. A culture that promotes positive risk taking, based on appropriate person centered policies, supports this approach and seeks to empower individuals.

Example: A learner may say to the Digital Champion, "My son never lets me have access to my personal banking."

Carers at risk of harm

Carers may be at risk by the person they offer care to. In some cases both the carer and the supported person can be considered to be at risk of harm.

Example: A Digital Champion may notice a learner is using abusive language to their carer or is being physically abusive to them (such as lashing out or hitting them)

Carers who cause harm

On occasions carers may cause intentional or unintentional harm. Cases of unintentional harm may be due to lack of knowledge, or the carer's own physical or emotional needs make them unable to care adequately for the vulnerable adult.

Example: A Digital Champion may see a carer using abusive language to a vulnerable adult or physically harming them.

Addiction

Another issue that may be noticed by Digital Champions is addition. This can take many forms, these are some examples:

- the learner has turned up to a session drunk, or smelling of alcohol
- they have mentioned that they have spent their pension money on gambling
- The learner turns up smelling of cannabis or mentions that they use drugs

In these instances, the Digital Champion should adhere to the Lone worker Policy and Lone Worker Safety Guidance, and also report any concerns to their line manager and complete a safeguarding report.

Illegal activity

Should you come across signs that someone is participating in illegal activity, please contact your manager immediately and complete a report. This may be evidence of illegal pornographic materials on someone's computer, or evidence of fraud being committed.

It is important that as an organisation and in your role that you understand the law regarding inappropriate and illegal content. We must not send, distribute, transfer, store, retain, keep, print or request anything that is illegal, inappropriate, indecent, offensive or unlawful.

Illegal Content

- It is illegal to possess, distribute show and make indecent image of a person under the age of 18 years old. The making of indecent images of children includes viewing them on the internet otherwise known as *downloading*.

- It is also illegal to possess extreme p0rn0graphic images or p0rn0graphic images which explicitly and realistically depict rape and other non-consensual sexual penetration of both human and animal.

- If in the course of your role you suspect that an offence as described above has been committed you must report this to your line manager straight away who will be able to provide advice on the next steps.

Who should be contacted?

- If the offence relates to Internal (any offence suspected to be committed or found on devices belonging to a member of staff) then the initial report should be submitted to your line manager. This report will thereafter be forwarded to the Operations Manager, Laura Simpson who will be responsible for any police contact in these instances. The Operations Manager will liaise directly with all parties concerned.

- If the offence relates to External (any offence suspected to be committed or found on devices belonging to a volunteer) the Operations Manager should be contacted in the first instance, who will liaise with the police and all parties concerned.

- Citizens Online refer to indecent images of children as child sexual abuse images to accurately reflect the gravity of the images or video. Please note that child pornography, child porn and kiddie porn are not acceptable terms. The use of such language acts to legitimise images which are not pornography rather, they are permanent records of children being exploited and as such should be referred to as child sexual abuse images.

- At no time should you put yourself at risk, if you feel intimidated, record as much information about the incident and contact your line manager as soon as possible.

- Further advice can be found at https://www.iwf.org.uk/

Concerns and reporting

A person's right to confidentiality is not absolute and may be overridden where there is evidence that sharing information is necessary in exceptional cases.

To prevent:

- Serious crime
- Danger to a person's life
- Danger to others
- Danger to the community
- Danger to the health of the person

The Policy and Safeguarding Report Form is made available on SharePoint for staff to access if and when required. If you are a volunteer and do not have access to SharePoint, please contact your manager who will be able to provide you with one.

We recommend that 'if in doubt, report it'. Whatever the circumstances of the concern, disclosure, allegation or suspicion, it is vital that the staff member records the details and reports to their line manager without delay.

The following points are a guide to help you respond appropriately:

- Listen carefully to what the person is telling you.
- Find an appropriate early opportunity to explain that it is very likely that what they are telling you will need to be shared with others.
- Ask questions for clarification only - never ask leading questions that suggest a particular answer.
- Reassure the person that they have done the right thing in telling you.
- Tell them what you will do next and with whom the information they have given you will be shared.

The following procedures should be followed in each situation:

- Take the allegation or concern seriously.
- If it is an emergency contact 999 immediately.
- If you feel in danger leave the situation as soon as possible (see Lone Worker Policy and Lone Worker Safety Guidance)
- Let you line manager know about the situation immediately
- Complete a Safeguarding Report form as soon as possible, giving all the details that you are aware of.
- Forward the report to your line manager and copy in the Operations Manager as soon (laura.simpson@citizensonline.org.uk) as possible, either by hand in a sealed envelope marked 'Confidential', or by a secure email with a 'read receipt' option.
- The senior management team will discuss the situation and respond accordingly.

Supporting the team

We want you to be safe at work, and to enjoy the work you are performing. However we are aware that at times, there may be incidents that occur that can cause distress to you. An example, may be that you while working as a volunteer you find something illegal or upsetting on a service users computer. In the first instance please talk to your line manager and complete a report form. This will help us to look into the incident and report the incident to relevant authorities if needed. We can then ensure we offer you adequate support.

If you are working during the Covid – 19 pandemic you may speak with colleagues and service users who have experience bereavement, illness or loneliness. Or this may be something that you are experiencing yourself.

If this is affecting your wellbeing, you may like to discuss this with your line manager in the first instance. If you feel you need additional support please visit the Time to Change website (link below) where there is a list of useful contact details for organisations that can offer support and advice.

https://www.time-to-change.org.uk/what-are-mental-health-problems/mental-health-help-you/other-useful-organisations

Non Compliance

Non-compliance with this policy may be subject to the disciplinary procedure.

Further guidance
This video provides a useful overview of Safeguarding and we would recommend you watch it during your induction https://www.youtube.com/watch?v=UXaqvE4y09c

Please also read the Lone Worker Policy and Lone Worker Safety Guidance available on SharePoint

Supporting you

APPENDIX 1 – COVID -19 UPDATE

Many of us are now using online systems to keep in contact and offer support. This is a guide on how to keep safe online during the Covid-19 pandemic.

Volunteers will have the same expected professional behaviours and safeguarding roles as set out above, as they would in a face-to-face setting. We will require volunteers to have a basic DBS check and will get these conducted as soon as it reasonably practical. Citizens Online will conduct a risk assessment for the Covid-19 rapid response project.

All volunteers will be provided with a script that must read at the start of any session.

If either the client or yourself wish to record the session, that is fine, but you must advise the client that recording has commenced. Most video conferencing software has built in recording systems which you can use. However, at the moment Citizens Online does not have a way of recording telephone calls.

Video conferencing

Many people are now using video conferencing tools, such as Zoom to catch up with family, friends and colleagues. However, there have been a number of meetings hijacked by an anonymous person who has then been able to share inappropriate content or shout abuse to the others in the meeting. For the purposes of this policy, we will be talking about Zoom as that is the system you will use most often. However, the policy does relate to any other online system being used.

Zoom has upgraded its security, but **please be aware of this risk and make sure you are following best practice with Zoom meetings** (as well as other video-conferencing platforms) at all times.

There are a number of simple steps you can take to manage meetings safely. Most of these can be set as default settings, or should be adjusted for individual meetings. Those having a Zoom account used to host meetings should ensure that their settings are appropriate (if you are simply joining someone else's meeting, the settings are less important).

Seven Host Actions:

1. **Always require a password when scheduling meetings** (Settings – Schedule meeting), From 5 April, Zoom has turned this on by default.
2. **If you have people joining the meeting by phone also require a password.** (Settings – Schedule meeting)
3. **Don't share the password or meeting ID publicly** – email it to participants and ask them not to forward it on.

4. **For really secure meetings you could turn on authentication and even two-factor authentication.** (Settings – Schedule meeting or this can be turned on for individual meetings) For most church purposes this may be a step too far – as it may make it harder to enable people you want to join who are less tech savvy to do so.
5. **Enable the 'waiting room'.** (Settings – Schedule meeting or this can be turned on for individual meetings).This has been turned on by default from 5th April. This puts people into a 'waiting room' before the host or co-host allows them to join the meeting.
6. **Prevent participants from sharing their screen (unless you need them to do so in order to offer support)** by setting the screen sharing to 'host only'. (In meeting settings). You can also disable users ability to use the Group Chat (message to all) or Private Chat (Message to another participant), to share using the Whiteboard facility or make annotations. (Settings – In Meetings Basic).You can also prevent participants from unmuting themselves if you wish to do a webcast with no verbal participation.
7. **Have someone who is responsible for managing Zoom if possible** (who may be different to the person leading the meeting). If you have set up the ability to have co-hosts (Settings – In Meetings basic), the host can share this function with another participant once they have joined the meeting (click on their name in the manage participants tab, and click 'Make Co-host'). They will then have access to the 'Manage Participants' screen, and can admit participants from the waiting room, mute or unmute them. You can also temporarily put them on hold, back in the waiting room or even remove them from the meeting should that be necessary.

Four Participant Actions:

1. **Use your name to log in** – rather than 'iPad'. This allows the meeting host to see who is coming into the meeting.
2. Consider whether you wish to create a **separate login using your email**, rather than login with Facebook or Google ID. Using these ID's can enable data sharing between applications.
3. One of the main security risks of Zoom is **phishing** (e.g. spurious emails posing as zoom invitations, posting malicious links in Zoom chats etc.) so users ALWAYs need to remember to be careful of what links they click on and what info they give out, whatever the platform.
4. Participants joining **any** video conferences should be aware of what they have in their background, make sure there's nothing confidential that can be seen (e.g. password pinned to noticeboard immediately behind them).

Zoom also recommends not using your Personal Meeting ID to host meetings, but rather generate a random ID through the 'schedule a meeting' function. Watch this tutorial on scheduling a meeting.

Zoom itself has put together a blog on how to keep unwanted guests out of your Zoom event.

TeamViewer

If you are supporting a client by using TeamViewer please :

- Always ask the user's permission before connecting to their computer. It may seem trivial, but as well as respecting their time and privacy, it helps build a good rapport with them.
- Always repeat what the client said to you back to them. This ensures you're understanding their question or problem accurately, and it also lets the client know you're actually listening to them.

TeamViewer have some information available on their website about how to use the system to support people, https://community.teamviewer.com/t5/Community-Blog/How-to-Provide-Remote-IT-Support-to-Your-Parents-and-Friends/ba-p/6247#

Telephone calls

Again, please maintains a professional approach when conducting telephone support sessions. Make sure you read the script provided by Citizens Online at the start of the call.
Because you may be using our personal phone, you may wish to hide your phone number when you call clients.

To hide your phone number in the UK, dial "141" before dialing the number you want to call to prevent the other person from seeing your number on their caller ID. You can also hide your number for all phone calls by changing the settings in the "Phone Options" menu of your phone.

141 also works for mobile phones as well as landlines. This article has more details on how to change settings on your phone:

https://bigtechquestion.com/2019/04/17/phones/withhold-mobile-number/

GENERAL COMPUTER SECURITY:
Ensure your computers have strong passwords with required letters, numbers and characters. Those passwords should be changed regularly, Please also be especially wary of fake emails claiming to come from Zoom, Facebook, or other social media platforms and websites.

These emails may be sent with criminal purpose, such as extracting users' data from your systems. Clicking on one of these fake links may well activate such criminal or extremist activity. If in doubt, do not open the email and do not click on the link.

Discourage unnecessary taking of photographs and online postings of online meetings, especially with the backgrounds and workstations of staff. There have been examples of people posting photos of screens/documents with sensitive data on them which give malicious actors further vulnerabilities to exploit.

Top tips

Dos

1. Remember that in the eyes of the general public, you *are* the charity you represent. Govern your behaviour accordingly.
2. Read the instructions you are given and if there's something you don't understand, please ask.
3. Remain friendly with and attentive to the people you are supporting;
4. Be the best listener you can be
5. Contact your line manager of you need advice or support
6. Respect the diversity of beliefs and faith practices of clients and volunteers
7. Maintain a high degree of professionalism and clear boundaries
8. Maintain confidentiality concerning the people we are helping.

Don't:

- Invite clients to come home with you or offer rides to clients
- Give or lend money to clients

- Accept any gifts
- Ask clients any probing or personal questions
- Share information on your faith or belief practices with clients or other volunteers unless asked; sway or attempt to convert clients to your specific religion or opinions
- Don't ask for personal information, such as passwords or financial information

Please remember, you are only working to support the client so please don't offer advice, such as how to fill in a Universal Credit claim, or which bank to use.

We would like you to watch this short, helpful video from Support Cambridgeshire about staying safe while volunteering https://www.youtube.com/watch?v=xKMvMASxiuk

Remember, if at any time you have any concerns, please contact Laura Simpson at laura.simpson@citizensonline.org.uk to discuss

Please also read the:

Lone Worker Policy
Lone Worker Safety Guidance
Safeguarding reporting form

These are available on SharePoint or from your line manager.