



ANDERIDA ADOLESCENT CARE

INTERNET POLICY -YOUNG PEOPLES ACCESS

Internet usage is a privilege. Internet usage time is set according to the young person's needs, level of maturity and safety aspects but as a general guideline our young people can have from two hours daily. This will depend on their behaviour, engagement in education and any internet usage associated risk taking. This is at the discretion of the team and implemented by the mentors on duty that day unless an internet safety measure has previously been imposed.

Parental controls must be set up on every young person's computer/device via the administrator account. These controls can be used to set usage times for the computer and block or allow websites. Website content can also be restricted so the young person is unable to view any inappropriate material. In addition to this basic safety a Net Nanny will be placed on the computer to track activity and email alerts to the team. All young people should be made aware of CEOP and the work they do in helping young people stay safe online and how to report unsafe activity or advances.

Games consoles must also be set up with a password protected administrator account if access to the internet is granted for online gaming. Parental controls **must** be set up by mentors ensuring that the young person is not given the WEP passkey used to enable internet access.

Mentors are not permitted to put WEP passkeys into young people's mobiles to allow them Wi-Fi access to internet via their phone without the above safety monitoring being applied (Net Nanny, CEOP, restricted timeframes). Although internet access via young people's phone networks cannot be completely monitored or stopped, mentors should not encourage young people to access the internet this way. If a young person is refusing a net nanny on their mobile device, we will suspend phone credit and limit this to landline only access.

Anderida currently utilise Qustodio to monitor online activity on phones and other devices. Qustodio has a location finder, monitors web site/search activity. Qustodio does have the ability to check social media and texts however this is not compatible with iPhones and would only be checked in extreme circumstances on devices where it is able to be activated. Qustodio is usually checked weekly by the allocated E-safety officer to ensure privacy for young people, however if there were ongoing safeguarding concerns the core team may start to access this daily to ensure increased safety and monitoring.

Websites of a sexual nature or containing nudity are not permitted. Games played through the internet must be of an appropriate certificate to the young person. Mentors need to be vigilant with this as even with parental controls set to block sites, access to prohibited sites can still be possible through links on other sites. Internet privileges should be reviewed or removed if the young person is found to be visiting inappropriate sites or using the internet or social networking sites inappropriately (see social networking policy). We want all young people to enjoy their internet time but at the same time we want to ensure that they are using the internet in a safe and responsible manner.

Should YP's disable Qustodio from their devices they will **NOT** be permitted access to the homes WIFI until this is re-installed.

Young people are **NOT** to be given any passwords, codes or WEP passkeys under any circumstances for any computer, games console or mobile phone. WEP passkeys, codes and passwords should be recorded in the internet section in the health and safety section and updated accordingly. If mentors have any reason to think that passwords may have been breached, they should change WEP passwords immediately and update the communication book/file.

Please also refer to social networking policy for guidance on the use of Facebook and other social networking sites for mentors and young people.

Support plans must also be updated to reflect the expectations / boundaries in place with each individual YP. All YP's are different and will have different levels of risk associated with using the internet. Please ensure that you are reading support plans fully if you are not sure.

CHANGING THE WI-FI PASSWORD or SWITCHING WIFI ON/OFF

- Log into Homes Unifi account. This may be auto saved on homes computer or password in comms book.
- Select 'manage' located below the list of active Wi-Fi account on main page once logged in.
- Select which Wi-Fi account you would like to manage E.G. YP Wi-Fi
- Select 'resume' or 'pause'
- Save changes.
- To change the password, click on the selected Wi-Fi account and you can change the password here.

PLEASE NOTE:

YP's are NOT to be given passwords for WIFI at any time. YP's should also never be connected to staff WIFI or know the password for this.

DELETING OLD, AND SETTING UP A NEW, USER ACCOUNTS

This will need to be done on the homes laptop when a young person leaves Anderida Adolescent Care. It ensures that new young people coming in cannot view any of the old young people's downloaded items or personal material saved on the computer.

TO DELETE AN OLD ACCOUNT FROM HOMES LAPTOP SHOULD YP'S USE THIS

- Start up the computer.
- Select the administrator account and enter in the password. The password should be stored in the internet section of the health and safety folder.
- Go into the 'start' menu.
- Select 'control panel'
- Select 'user accounts'
- Select 'manage other accounts'
- Select the young person's account
- Select 'delete account'
- The next screen will ask if you want to keep the young person's files. Select 'delete files' as this will remove everything off the computer and make it ready for the next user.
- Select 'delete account' when it asks you if you are sure.

TO CREATE A NEW YOUNG PEOPLE ACCOUNT ON THE HOMES LAPTOP FOR YP'S:

- Start up the computer.
- Select the administrator account and enter in the password. The password should be stored in the internet section of the health and safety folder.
- Go into the 'start' menu.
- Select 'control panel'
- Select 'user accounts'
- In the list on the window select 'manage another account' (blue writing).
- If you get a window asking for permission to continue, select 'yes'.
- In the resultant screen select 'create a new account'.
- In the resultant screen type young person's name in the new account name field.
- Select standard user by clicking in the circle next to that selection so that it turns blue.
- Click on 'create account'.
- You will see the new account appear in the top of the window.

DO NOT CLOSE ANYTHING DOWN YET AS YOU WILL THEN NEED TO SET UP PARENTAL CONTROLS

- Select this account to change by clicking on it.
- Select 'set up parental controls' from the list in the resultant screen.
- Click on young person's account icon.
- Select 'on, enforce current settings'
- Select 'on' for activity reporting.
- Have a look on the windows settings – you can adjust time setting for when they are allowed on the internet, games certificate ratings and you can block sites from this window. These are all self explanatory, just click on the links and follow the instructions selecting which options you want for each.
- Once you have selected your parental control settings, click 'OK' at the bottom of the screen.
- You will then need to restart the computer for the changes to take effect.

IF YOUR WI-FI OR NETWORK CONNECTION SUDDENLY STOPS WORKING

The most common solution to this problem is to switch off the router for 10 seconds then switch on again. There is usually a small button on the side or back of the router. If you cannot locate this then unplug the power cord. Wait for a few minutes for the router to renew its settings and reconnect. Then try to get on the internet again.

If this doesn't work, then try the following:

Restart computer / laptop

If this doesn't work, then try the following:

- Go into the 'start' menu on the computer that will not connect to the network or internet (the start button is located on the bottom far left of the screen, hover the mouse over it and a small box should appear telling you that it is the start menu).

- Select 'control panel' which is on the right side of the menu.
- Find the 'network and sharing centre' icon and click on it.
- In the window, it will show you the connection status 'connected' or 'disconnected'. If it is showing as connected, it will show the signal strength as 'good' which are the green bars (this may vary according to each computer). Try disconnecting, clicking first on 'disconnect' in blue (halfway down on the right-hand side of the window).
- Then reconnect by clicking on 'connect to a network' and selecting WIFI network required in the resultant window. Then click on 'connect' at the bottom of the window.

If this doesn't work, then try the following:

- Go into the start menu **on the computer that is directly connected to the router** (not the one you are trying to connect wirelessly).
- Select 'control panel' which is in the grey part of the resulting menu.
- Find the 'network and sharing centre' icon and click on it.
- In the 'sharing and discovery' section at the bottom of the resultant window, check that all sections are turned on and have a green dot next to them **EXCEPT** 'password protect sharing' which should be 'off' with no green button next to it. If the 'password protect' button is on, then this needs to be switched off.
- To do this, click on the mini downward arrow to the right of the section then select 'turn password protect off' by clicking in the little circle next to it so that it is highlighted green.
- Once this is done click on 'apply'.

If this still doesn't work or for any other problems you may encounter, contact the organisations IT provider.

Focus Group.

FOCUS GROUP ARE ON SUPPORT 5 DAYS A WEEK

Please report all support issues to the Focus IT Helpdesk

○ **Logging A Support Call**

Contact Focus IT Helpdesk Email focusit@focus-grp.co.uk Telephone 0330 024 2004

○ **Provide Your Details To log a call with the Focus IT Helpdesk**, you will need to provide the following:

- Contact Name
- Contact Telephone Number
- Email Address
- A brief description of the fault, including any error messages or error codes

○ **Call Details**

A support request will be raised on the Focus IT Helpdesk, and an automated response will be returned with:

- A Ticket Number, starting INC
- A copy of all the details raised in your ticket

- **Call Allocation**

Focus aim to allocate all calls within the first hour of them arriving to the helpdesk, once the call has been allocated, you will receive a reply describing the below.

- Severity Rating
- The allocation your ticket has received, which defines how urgent the ticket is.
- Engineer – The name of the engineer who your ticket has been assigned too.