BEYOND LIMITS

Policies and Procedures

Beyond Limits provides policies and procedures to promote safe and consistent practice across the Organisation. The framework laid down within our policies and procedures lets everyone know how we work and reflects our values and mission statement. Our policies and procedures are written to help us, employees of Beyond Limits, to make good, safe decisions.

Beyond Limits expects all employees to be familiar with the contents of all policies and procedures relevant to their role and to understand how to apply them within their daily work.

None of these documents stand alone, all fit within the larger framework of the way we work and any associated policies which are particularly relevant will be directly referenced.

Computers/Information Technology (Including Mobile Phones & Social Networking Policy)

This policy should be read in conjunction with the Data Protection Policy, Employee and Friendship Policy, Confidentiality Policy and the Employee handbook.

Computers/IT and Social Networking Policy - what this means to Beyond Limits:

The use of the information technology (IT) including the Internet and Internet enabled devices are part of the lives of our employees and the people we support. IT and the Internet are useful in opening new opportunities, new relationships and to make places and people more accessible. However, with this freedom comes certain risks that should be considered by employees and the people we support.

- **Devices provided by Beyond Limits**
  - Devices such as laptops, mobile phones and tablets provided by Beyond Limits to employees are for the purposes of the organisation only and should not be used for personal use without the permission of your line manager. Beyond Limits have the right to monitor and access all aspects of its systems in compliance with the UK Data Protection Act 2018.
  - Employees will have access to an email account and internet services via the organisation's computer system via Microsoft Office 365. This is intended to provide effective communication within Beyond Limits and its external partners on matters related to business.
  - Messages sent via email should be written in line with Beyond Limits best practice – politely and succinctly and fully in-line with the Data Protection Act 2018 and the EU General Data Protection Regulation (GDPR), with particular care taken to ensure an appropriate level of confidentiality. If referring to a person we support in an internal email it is appropriate to use the person's name. If you are composing an email that is to go to anyone outside of the organisation then you should only use the person's initials e.g. DK instead of Doreen Kelly. Information divulged must only be on a need to know basis. Sometimes, it is better to speak directly to a person rather than email. If in any doubt, ask your line manager.
  - Employees should keep and electronically store email messages sent and received about the people we support and Beyond Limits business as these may be needed to refer to at a later date. Just as you would with paper data, employees should get used to storing information neatly and expediently. By this we mean filing and using a folder system where appropriate. You should not store anything on the desktop or hard drive of a laptop or computer but rather, ensure your work is stored in individual folders on the VPN (Virtual Private Network) or on Office 365 facilities such as OneDrive or SharePoint. This is to ensure any important data is not compromised should the laptop get broken or stolen. However, when using online cloud storage please be mindful about what rules are in place in terms of users accessing the data. If you have any queries about how to do this, or are simply unsure of what this means, please do not hesitate to contact our external IT partners JMV Solutions (support@jmv-solutions.co.uk) or indeed head office (info@beyondlimits-uk.org) who will be able to direct your query to the appropriate person.
  - Records e.g. supervision notes, updates on individualised Working Polices, Service Designs etc. need to be saved electronically by uploading to the relevant SharePoint site, if applicable, or saving in the correct designated folder/file in the Remote drive when connected to the VPN. As a general rule, files that you are happy for the whole team to

see can go on SharePoint. Files of a more private nature, e.g. support & supervision paperwork, should go on the VPN for now. All managers have access to the Remote drive.

It is the responsibility of each employee to ensure all documents regarding the person they support are stored safely and securely this includes on the Remote drive and not left on the desktop of any laptop or anywhere else.

- Employees will be given a set of login details and a password to access their email and another set for Carista. You must change your password on first log-in and keep this private **(never share your login details)** It must be a password that is not easy to recognise.
- If accessing email remotely at your home address you must ensure that no one is able to read your emails other than yourself. If you are accessing Office365 via a personal device you must never save login details and you must log out of accounts associated with work, or have a PIN or password set on your device so that no other person can access it.
- There may be more detail about accessing and circulating information via email regarding the person you support in the person's Working Policy that you should adhere to.
- The person you support may have their own computer/laptop and access to the internet. Any support required with accessing/using this technology will be discussed and recorded in the person's Working Policy. However, employees must not under any circumstances use a computer belonging to a person being supported for their own use.
- Some employees have access to team laptops for use whilst working with a person we support. This laptop belongs to Beyond Limits. Employees must sign the terms and conditions of use. Usage of the laptop will be discussed and agreed within the team.
- Employees must not use the laptop (or similar device) for personal use and internet access must only be for use regarding the person you support. Any unauthorised usage may lead to disciplinary action. If employees have had to use the laptop at any time for emergency personal use then they must inform their line manager immediately.
- Beyond Limits will make random checks on its computers/laptops to ensure they are being used appropriately.
- In the event of a lost or stolen device it is your responsibility to advise your line manager as quickly as possible. Failure to report the loss in a timely manner may lead to disciplinary action and the charge of the device after loss may be deducted from your salary.
- If you damage a device belonging to Beyond Limits this may result in any repair or replacement being deducted from your salary. This does not include repair due to it being

faulty. Any repairs will require the return of the device, charger and any other accessories associated with it.

- If your employment ends at any time it is your responsibility to return any device or other accessories issued to you to the office and you will receive a receipt for it.

- **Employees should not:**
  - Use email for personal use (i.e. to receive product alerts, book holidays, internet shopping). This can compromise the security of the account.
  - Give organisational email details to personal contacts
  - Use any internet enabled device of a person we support unless it is to support them to access the internet for themselves
  - Use the team laptop/device for personal use or use it inappropriately
  - Access pornographic, racist and other inappropriate or unlawful material
  - Download or disseminate copyrighted material
  - Forward chain letters
  - Download and/or play computer games
  - Access social networking sites during working hours
  - Download, display, send or receive materials that insult, cause offence or harass others (this includes joke emails)
  - Browse the internet unless it is work related
  - Tell anyone else your password for any device or account

> When employees leave Beyond Limits all information technology, data, software and devices must be handed back to the Organisation.

Multi Factor Authentication

Beyond Limits employees will be asked to setup Office 365 Multi-Factor Authentication to sign into Office 365 services. Multi-Factor Authentication (MFA) increases the security of user login for cloud services above and beyond just a password. With MFA for Office 365, users are required to acknowledge a phone call, text message, or an app notification on their smartphone after correctly entering their password. Only after this second authentication factor has been satisfied can a user sign in.

MFA should be used wherever possible because it immediately neutralises the risks associated with compromised passwords. It adds an additional layer of security to protect highly sensitive personal information. Following advice from our IT partners JMV Solutions and Microsoft, we believe having this additional security keeps our information secure and limits cyber-attacks.

Devices belonging to people we support

For the people we support, having internet access has made communicating and getting responses from professionals much faster.

Having a device with access to the internet can be a useful way of making life more accessible for the people we support. This includes making information more accessible, helping access events and things to do in the community, shopping, using social network sites, booking holidays and keeping in touch via email, Skype, Facetime etc. However, any device belonging to a person we support must only ever be used on behalf of the person and employees must be made aware that misuse of equipment belonging to someone we support could result in disciplinary action.

The decision to buy a device should be made by the person and/or those people that know them well not made by their support team in isolation. If the person lacks the capacity to make this decision and it is felt to be in their best interests, their Court of Protection Deputy or Care Coordinator should be asked to inform/make the decision. To make this decision, time should be spent costing out the different models and broadband costs so that an informed decision can be made, and people will know if they can afford it. It is a good idea to discuss and agree the parameters of use with the person's advocates e.g. any sites that are to be barred, protection against misuse by employees and auditing use. The parameters should be recorded in the person's Working Policy.

Social Network Sites

Comments made on social networking sites are available for members of the public to see. Once published on a site, information you supply can be accessed by anyone. You should always ensure you stay within the legal framework and are aware of libel, defamation, copyright and data protection laws.

This policy applies to social media sites, personal web pages, dating websites, personal space provided by internet providers and internet presence including blogs, Facebook, Twitter, Instagram, Myspace and other messaging services. However, this policy also applies to any sites which make personal views available to the general public.

The purpose of this policy is to protect the reputation of employees of Beyond Limits and the reputation of the organisation as a whole from abuse.

Employees are advised not to write about their work or refer to Beyond Limits on external web pages i.e. in blogs or on social networking sites.

Communications regarding work-related issues should not be posted on the Beyond Limits Facebook page, and should be sent instead through the workplace channels e.g. email, phone.

With the advent of social media, the definition of the "workplace" has expanded to include on-line activity. This policy seeks to warn employees that on-line harassment and bullying of colleagues will not be tolerated. Beyond Limits will take action against those employees whose conduct puts them in breach of this policy, specifically any form of harassment, bullying, explicit sexual content or references, disclosure of confidential information and any derogatory comments about the organisation, people we support, families and other professional partners.

- **Employees must not:**
  - Disclose information that is confidential to Beyond Limits or anyone we support
  - Disclose personal data or information about an individual/colleague/person we support (including photos) which could be in breach of the Data Protection Act or this policy
  - Disclose any information (including photos) that is not already in the public arena
  - Post illegal material, e.g. images of child pornography, child abuse or material that incites racial hatred
  - Link their own blog/personal web page to Beyond Limits website without consent of the Director
  - Include any information sourced from Beyond Limits that is in breach of copyright
  - Make defamatory remarks about Beyond Limits, colleagues or people we support
  - Publish any material or comment that could undermine public confidence in Beyond Limits
  - Misrepresent Beyond Limits by posting false or inaccurate statements about the work of Beyond Limits
  - Use social media to engage in inappropriate conversations or arguments with the people we support and/or their families.
  - Use the Beyond Limits logo on personal web pages
  - Bring the organisation or its employees into disrepute and do not use your site to attack and abuse colleagues or the people we support

- Include contact details or photographs of employees without their permission
- Reveal information that is confidential to Beyond Limits or the people we support

If you intend to include a picture of someone you support on any private or public domain, you must first discuss the appropriateness of this with your line manager and seek the permission of the person in question (if appropriate to do so).

Consult your line manager if you are unsure about anything contained within this policy.

> Failure to adhere to these rules may be viewed as misconduct and may result in disciplinary action being taken which could result in dismissal. Service Leaders will regularly check the computers used by employees as part of their quality audit.

The people we support

As we are supporting people to have lives based in their communities, like everyone else the internet and social networking sites will be accessed via personal laptops, phones, computers and a range of other smart devices. If someone you support begins to access social networking sites including dating websites then person centred approaches to risks should be used and should consider privacy, image use, bullying, sexual safety and theft. The person's Working Policy will provide details about what needs to be recorded and adhered to by their support team. These will consider the balance of what is important to/for the person and what is safe. Where there is a known risk and where internet access may increase risk, these must be shared with the person's multi-disciplinary core team.

Employees may be approached by the person they support to accept them as a 'friend' on Facebook or any other social media site. Employees are advised to read *'employee and friendship policy'* and should refuse such requests on the grounds of professional boundaries and to protect their time away from work. Friendships are not banned but need to be carefully thought through in line with our policies. Employees should discuss any concerns with their line manager.

Employees are advised to use their security settings on social media sites to ensure their private lives, photos etc. are not open to being viewed by people they have not chosen.

Employees should explain to the person they support that a paid relationship (employee) is not a friendship, but a professional friendship with boundaries. This may be hard for some people to understand as they have not had the opportunity to make real friends and have spent much of their

lives surrounded by paid 'people' who they get on with. It is an employee's role to help the person develop real friendships and a circle of people who care about them.

- **Employees should:**
  - Discuss any concerns they have regarding a person's being supported access to social networking sites with their line manager
  - **Not accept** requests to be friends with the person you support on social media sites
  - Explain to the person you support that the 'professional friendship with boundaries' is not the same as being friends and help them make real friends.

Telephones including internet enabled devices

Phones including mobile, landline and online are an essential part of modern life and will open up new opportunities for making and nurturing relationships for the people we support.

Employees will have access to 'team' mobile phones or devices for use while they are supporting a person. This phone belongs to Beyond Limits, but the costs are incurred through the person you support's budget so you should use it sparingly. Employees will sign to agree to the terms and conditions of use. Usage of the phone or device will be discussed and agreed within the team and written up within the person's Working Policy. The phone or device will have emergency numbers programmed in.

Employees must not use a team mobile phone or device for personal use and must not access the internet using the 'team' mobile phone or device. Any unauthorised calls may lead to disciplinary action and the cost of such calls being deducted from your salary. If employees have had to use the phone at any time for personal use e.g. to make an emergency call to a family member, then they must inform their line manager immediately.

All team phones and devices must be password protected. This will be set up before you receive your handset. You must tell your manager if you have changed the password.

Beyond Limits will itemise and review 'team' mobile phone bills and advise when usage is high.

In the event of a lost or stolen device it is your responsibility to advise your line manager as quickly as possible (calls and access can then be barred by an administrator). Failure to report the loss quickly may lead to disciplinary action and the charge of the device and any calls made after loss deducted from your salary.

Damage or loss of devices – if you damage or lose the handset or device this may result in repair or replacement being deducted from your salary. This does not include repair due to it being faulty. Any repairs will require the return of the phone and charger.

If your employment ends at any time it is your responsibility to return any handset, charger, Sim card and any other devices or accessories to the office and you will receive a receipt for it.

The person you support may have a personal mobile phone, landline or similar online services. Employees are not to use the mobile phone, landline or online services of the person you support unless it is to support the person to make a phone call or access services for themselves.
Whilst working for Beyond Limits your own personal mobile should not be used unless in an emergency. Whilst using or talking on your own phone you are not concentrating or giving the time that you have been paid for to the person being supported.

When supporting someone, employees are not to have their personal mobile phone or device turned on. If you are waiting to receive, or needing to make an emergency call, then this should be discussed and agreed with your line manager. Please refer to the person's Working Policy with regards what is / isn't appropriate.

Whilst driving all mobile phones or devices must be turned off, unless you are using appropriate hands-free equipment that meets the recommended safety standards.

- **Employees should not:**
  - Use the 'team' mobile for personal calls unless in an emergency and this should be reported to their line manager
  - Use the 'team' mobile to access the internet
  - Us the mobile phone, landline or Skype of a person we support unless it is to support them to make a personal call
  - Use your own mobile whilst working with a person you support unless it is an emergency
  - Use a mobile whilst driving. The phone **must** be turned off during all journeys, unless you are using appropriate hands-free equipment that meets the recommended safety standards