

## ICT, COMPUTER USE, ONLINE AND SOCIAL MEDIA at JAMES



### POLICY

The Project recognises that within the ICT data transfer both incoming from any source and outgoing to any recipient, internal or external, there are considerable responsibilities attached. Supervision of young people/ service users is a **MUST** and staff must at all times monitor computer related work closely enough to be able to see what is being viewed and typed and ensure that it is appropriate within the terms of 'acceptable use of data', below.

It is absolutely necessary that all **staff, volunteers, service users and young people** having access to computers use such equipment responsibly. Any inappropriate use, as defined below, may be considered to be **gross misconduct** which will be subject to the organisation's disciplinary procedure and is likely to result in the dismissal of the person, or persons committing, or condoning such behaviour. (*The list is not comprehensive but is indicative of unacceptable actions.*)

With social networks such as; Facebook, Instagram, and Twitter, it is **inappropriate and not acceptable** for any JAMES worker, (including volunteer, or placement) to accept a request to become a personal contact, or friend of any young person engaged in a JAMES project. We do however want to ensure we can provide help in difficult circumstances and in that case, or if in doubt, the worker must obtain advice from their line manager before taking action if contacted by social media. We also do not advise that keyworkers accept friend requests from clients before or after engagement with their family, to prevent blurred lines between professional boundaries.

We have a JAMES Facebook page which is monitored regularly and clients can be 'friends' with us on there. We also have a Positive Futures Twitter account and JAMES Instagram account (currently used limitedly). Positive Futures has a Facebook page solely for young people and PF staff to create a safe zone for young people – young people can be friends on there.

JAMES workers should consider their personal sites and ensure they **do not** contain publicly accessible postings which are inadvisable and/or unprofessional. We advise that staff set personal accounts to 'private' to prevent anyone from accessing their posts and finding information about them. Due to the nature of our roles, staff must not under any circumstances post comments that are offensive and upsetting to others and any posts negatively portraying

JAMES, it's staff, or clients will be classed as misconduct or gross misconduct. Any discrimination against/bias/negativity to any protected characteristics under the equality act, such as; age, race, gender, sexual orientation, disability, heritage or religion will be viewed as misconduct and will initiate JAMES' disciplinary policy. Staff and volunteers must also ensure they do not post names, or photos on their social media sites of young people/ service users from JAMES projects.

All JAMES social media posts will be done through or with agreement from the management team. Projects can have Facebook sites to engage and liaise with young people/clients but these pages must not contain personal data and opinions of staff and volunteers and must contain information that is relevant to the project and only have photos on when media consent has been given for those individuals in those images.

The **acceptable use of data**, including that accessed via; phones, film, computers, video, DVD or other data transfer equipment requires that an employee, volunteer, service user, young person or any other person in contact with JAMES members and venues **shall not** obtain, post, transmit, re-transmit or store material on, or through any JAMES systems, services or resources, and shall not be enabled to share with JAMES members; media obtained on their own equipment that;-

- is pornographic; visually or textually.
- is indecent, discriminatory, obscene, offensive, threatening, abusive, defamatory, libellous or hateful, encouraging conduct that may constitute a criminal offence, may give rise to civil liability or otherwise violate any law; or that could otherwise affect any individual, group or entity.
- violates the rights of any person including rights protected by copyright, trade secret, pattern or other intellectual property laws including, but not limited to the installation or distribution of software products that are not appropriately licensed for use by JAMES.
- amounts to any form of hacking; seeking to gain access to restricted internal or external areas.
- endangers computer operation via a virus, worm, Trojan or other means of threatening system integrity.

N.B.1. The definition of ownership of resources and information in respect of JAMES includes the; IT systems, services and resources provided by the organisation, including but not limited to the network, the computer, Wi-fi, the e-mail system. These are all JAMES property and as such may only be used for authorised organisational purposes.

N.B.2. Information created by, distributed with or stored on JAMES equipment is also JAMES property.

N.B.3. Any personal internet use must be authorised by the line manager and must not encroach on time which should be made available to JAMES. Access is further denied to unsuitable sites which include dating websites and –unless specifically cleared by a senior manager (for relevant issues)- chatrooms and to any other area of the internet which may be specified by your line manager as inappropriate. This includes use of personal devices in time you are being paid to work.

**Viewing content online and any video or audio content must be done via legal means and paid subscriptions and not illegal streaming in any form and must be age appropriate.**

**Suspected Inappropriate Use** - Any member of the organisation suspecting possible inappropriate use from others must report this to their line manager without delay. ***Any such report will be handled in strict confidence.***

**Laptops/ notebooks/ tablets/ phones or computers supplied for home use.**

Any provision of such is for the sole purpose of enabling an employee to carry out work on behalf of JAMES. Whilst additional, approved forms of personal use are not denied, any additional software installed must be certified as free of viruses etc and must have the approval from their line manager. Any inappropriate use of JAMES equipment even out of JAMES bases/offices, will be deemed to be misconduct. For confirmation of continued machine and systems integrity there may be monitoring requests made from time to time, for which the machine(s) must be supplied ***without delay.***

***Staff to be aware and mindful that they are representatives, when both in and out of work, of JAMES and any social media pictures, tags, posts, etc. can have an impact on the organisations, families and young people and staff who are part of it. Any inappropriate behaviour in and out of work time will be viewed as misconduct.***

## **Online platforms and virtual contacts**

**In a world changing quickly with technology we are becoming more dependent on it to engage with; young people, service users and each other (particularly during Covid- 19 pandemic).**

**Any online platforms to engage young people such as; Whatsapp, Messenger, Instagram, Zoom, Teams should be age appropriate and safety measures should be followed to keep yourself and the service users as safe as possible. Please ensure you remain professional with clear boundaries whilst using any communication platform. Behave online in the same professional manner that you would in a face-to-face session.**

**Please follow the guidance below:**

### **Boundaries**

- We are only available at set times during the day / evening as per your hours of work
- If an appointment has been made stick to that time
- Be clear that it is not possible to respond immediately to calls or text, so if an emergency situation occurs then they need to contact emergency services
- If its your personal number please ensure this is kept private – always endeavour to use work phone numbers
- Explain Child Protection Processes and procedures
- Consent explained and agreed

**It's important that we consider risk when we are working with young people and service users. Completing a risk assessment before the start of the session is good practice and highly recommended.**

**Contacting high risk/vulnerable young people** (see further advice within JAMES Safeguarding document):

- Complete an Assessment to gauge risk and look at how to reduce risk
- If you are concerned and the young person is showing signs of harming themselves or others, ask open/not leading questions and report to Designated Safeguarding Lead.
- When you are recording your contact – ensure you are recording all the right information.

- Have all the referral information – parents / cares information / referrer's information. So you can contact them and let them know if you have concerns.
- Follow up actions and calls (if needed) to other agencies – First Response, Police, and Childrens Social Care etc...

## **Online Group Sessions**

### **Set the scene**

- Have a purpose for the session – a reason to run an online group. Be clear what this is.
- Have 2 workers present online when possible – particularly for young people.
- Clear roles for staff during the session, one to lead the session and the other to support.
- Set your space up where you will have minimal interruptions.
- Be careful you don't have any personal information visible or anything that gives away your location – where possible use a space where the wall is plain and clear behind you.
- Have a staff meeting before the session to plan and discuss roles.
- Plan your session, give it structure.
- Clients need to be invited to the session via the staff member in charge. This information should not be shared publicly.
- If possible wear JAMES hoodies / T-Shirts, if this is not possible workers need to dress appropriately.

### **The Session**

- Use the Waiting Room setting to ensure you can manage who enters the session.
- Ask clients to use their real names and not nicknames so they are easily identifiable when joining the group.
- Work with clients to set up ground rules for working online. Include things such as; confidentiality, respect, how to introduce new members and what is appropriate behavior. This needs to be revisited at the start of each session.
- Some may not feel comfortable showing their faces online; this is fine as long as workers know that the client is who they say they are.
- If anyone is behaving inappropriately remind them of the ground rules and give a warning if rules are not followed and if things don't improve remove that person from the session.
- Familiarise yourself with the system / platform you are using and make sure you are confident in how the system works.

- Be aware that live streaming means people could take screenshots and video recordings of the sessions.
- Virtual Sessions should be for clients who are known to the worker, however new members can be introduced if done safely and appropriately.
- New members need to have one-to-one sessions with the lead workers before they attend a group.
- If workers are concerned about a safeguarding concern, then the normal process and policy should be followed.

### **Evaluation and endings**

- Lead worker to end the session or remove participants and ensure clients are not left in the group chat after workers have left.
- Workers to stay online and debrief and evaluate after the session if possible.
- Session notes/date and attendances to be recorded.

### **Online at JAMES for Service Users**

- Leave your phone at home – if you need to contact home, you can always call from reception
- If you do bring your phone you must hand it in to the designated area.
- Computer use will be monitored at all times – you will not be allowed on social media

### **You may lose your place at JAMES – or we may even have to involve the police, if you:**

- Take pictures, video or audio content of other young people, staff or volunteers – you would not like it if they did it to you!
- Post comments about other JAMES young people, staff or volunteers on any social media sites – you would not like it if they did it to you!

### **Top tips for keeping safe online:**

- Be careful what you share - If you wouldn't want your staff or family to see it, it's probably best not to post it. Because once it's online, it's out of your control.
- Be careful who you chat to - If somebody you don't know adds you as a friend, ignore them and

delete their request. Don't share personal information like your address or phone number with somebody you don't know or don't trust (you may know them but think about why they want or need that information and what will they do with it).

- Don't meet people you don't know - Even if you get on with them online, you never know who they really are.
- Use a complex password - It should be hard for other people to guess your password and it's a good idea to change it regularly.

**Online bullying; block it and report it, tell an adult you trust, support someone if they're being bullied, take care of yourself** (<https://www.childline.org.uk/info-advice/bullying-abuse-safety/types-bullying/online-bullying/>)

**You can always speak to a member of JAMES staff if you are worried about online safety.**

Some other good places to go for support:

<https://www.saferinternet.org.uk/advice-centre/parents-and-carers>

<https://www.thinkuknow.co.uk/parents/>

		Issue Dec 2011	Amended June 2020	Updated 2020 (PR)
Updated Jan 2023				