



JSENSE E-SAFETY POLICY

First Written: March 2022	Last Reviewed: August 2026	Next Inspection: August 2027 Next Review: August 2028
---------------------------	----------------------------	--

JSENSE helpline is an independent and totally impartial and unbiased service.

This policy outlines JSENSE's expectations regarding the safe, responsible and professional use of digital technology, online communication and social media in order to safeguard children, young people, families, staff and volunteers

General guidelines

: DO

- Do inform your line manager about any encounters that worry you

: DO NOT

- Do not behave in a way that could suggest that you are trying to develop a personal relationship with a child
- Do not use your own technology to photograph or communicate with a child, young person, or their

: DO

1. Set your *privacy settings* for any *social networking site*.
2. Ensure your *mobile phone* (any technological equipment) is *password/ PIN* protected.
3. Consider having separate personal and professional online *accounts/ identities* if you wish to have online contact with service users, their families and other professionals.
4. Make sure that all publicly available information about you is accurate and appropriate
5. Remember online conversations may be referred to as '*chat*' but they are written documents and should always be treated as such.
6. Make sure that you know the consequences of misuse of digital equipment.
7. If you are unsure who can view online material, assume that it is publicly available. Remember - once information is online you have relinquished control of it.
8. Switch off *Bluetooth*
9. When you receive any new equipment (personal or private) make sure that you know what features it has as standard and take appropriate action to disable/ protect.

: DO NOT

1. Give your *personal information* to service users -children/ young people, their parents/ carers. This includes *mobile phone* numbers, *social networking* accounts, *personal website/ blog URLs*, *online image* storage sites, *passwords* etc.
2. Use your personal *mobile phone* to communicate with service users. This includes phone calls, *texts*, *emails*, *social networking sites*, etc.
3. Use the *internet* or *web-based* communication to send personal messages to children/young people
4. Share your personal details with service users on a social network site
5. Add/allow a *service user* to join your contacts/friends list on personal *social networking profiles*.
6. Use your own digital camera/ video for work. This includes *integral cameras* on *mobile phones*.
7. Play *online games* with service users.

Purpose and Scope

JSENSE is committed to promoting the safe, responsible and professional use of digital technology, online communication and social media to safeguard children, young people, families, staff, volunteers and trustees.

This policy applies to:

- Employees
- Volunteers
- Trustees
- Contractors and sessional staff
- Students or placement workers acting on behalf of JSENSE

The purpose of this policy is to:

- Protect children, young people and vulnerable families from online harm
- Maintain professional boundaries
- Promote safe online working practices
- Ensure confidentiality and data security
- Reduce risks associated with online communication and digital technology

This policy should be read alongside:

- Safeguarding Policy
- Data Protection and Confidentiality Policy
- GDPR/Data Retention Policy
- Staff Code of Conduct

Safeguarding and Reporting Concerns

Any concerns regarding online safety, inappropriate online behaviour, cyberbullying, harmful content, grooming, exploitation, breaches of confidentiality or unsafe digital practice must be reported immediately to a manager or the Designated Safeguarding Lead (DSL).

Concerns may include:

- Inappropriate communication with service users
- Online grooming or exploitation concerns
- Harmful or extremist content
- Cyberbullying
- Sharing confidential information insecurely
- Suspicious emails, phishing attempts or cyber security incidents
- Accidental disclosure of personal data

All incidents should be recorded in accordance with JSENSE safeguarding and data protection procedures.

Where necessary, concerns may be referred to:

- Children's Social Care
- Police
- Local Authority safeguarding teams
- The Information Commissioner's Office (ICO)

Email **What is AUP in this context?**

Emails (electronic mail) have been around for a long time and most people are very used to communicating using this method. However this is a method of communication where you must have different *email* accounts for your personal and professional use.

DO NOT

Don't use your personal *email* account to communicate with children/ young people, their parents/ carers

This includes email via mobile phones or web based software

Best practice

DO

Your organisation should provide an *email* account for you to use for professional communications

Safe practice

Check your organisation policy (*AUP*) regarding use of your work account for personal use e.g. shopping

Poor practice blurs the professional boundaries and can make workers vulnerable to *bullying/ harassment/ allegations*. If it's a breach of the *AUP* then it may result in capability/ disciplinary/criminal proceedings

Poor practice

DO NOT

Don't use your personal *email* account to communicate with *service users* and their families without a manager's knowledge or permission – and in accordance with the appropriate *AUP*.

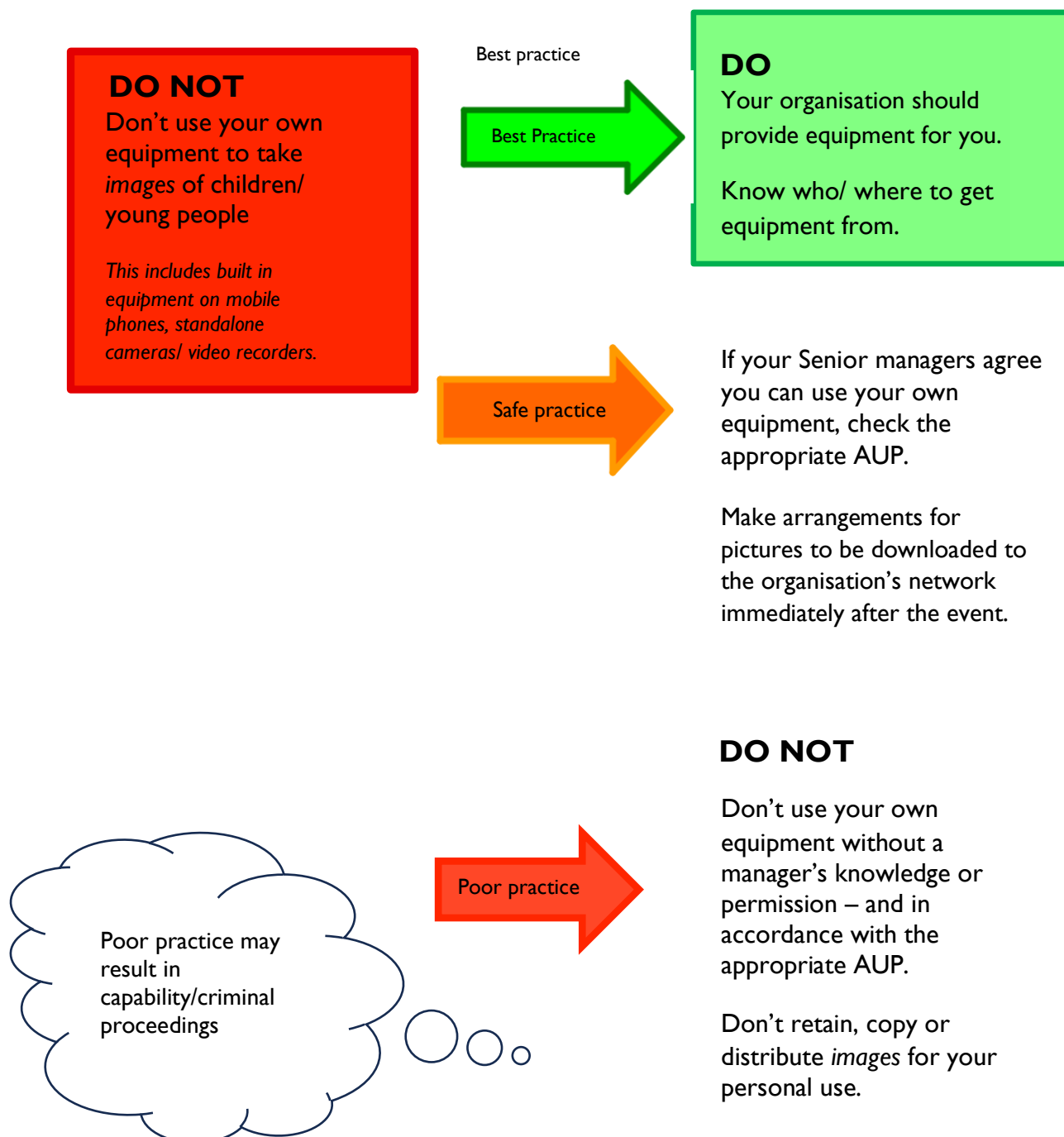
DO

What should be in place?

- An *AUP* which should be explicit about the use of personal *email* accounts to communicate with *service users*.
- The *AUP* should be explicit about using work accounts for personal purposes.
- The *AUP* should include sanctions for breaching the policy.
- Staff must only use approved JSENSE email accounts for professional communication.
- Confidential documents containing personal or sensitive information must only be shared using secure and
- password-protected methods where appropriate.
- Staff should remain vigilant to phishing emails, suspicious links and requests for confidential information.
- Multi-factor authentication (MFA) should be enabled where available.
- Personal email accounts must not be used to store or transmit confidential service-user information.

Images

We all love taking photos of children and young people to record and show off their achievements and experiences – particularly for sharing with those who cannot be there to witness the event in person. Do not be tempted to use your personal *mobile phone* or camera to do this. Make sure that you get the relevant consent to take pictures.



DO

What should be in place?

- Use of personal equipment should be made clear in the *AUP*
- Taking *images* of service users should be included in the *AUP*. Parental permission must be obtained which includes taking *images* and use of *images* e.g. on *website*, displays etc
 - Written consent must clearly specify:
 - How images will be used
 - Where they may appear (website, social media, reports, publicity materials)
 - How long images will be retained
 - Who will have access to them
- Images must be stored securely in accordance with JSENSE data protection procedures and deleted when no longer required.
- Staff should know where equipment is available from and the rules for returning it, who is responsible for *downloading* onto the organisation's storage media and deleting from the camera

Internet

The *internet* has totally changed our lives and given us quick access to information, *content* and people! But like any other part of our life we do need to learn what is good – and bad – about using it!

Best practice

Be aware of the organisation policy for the use of the *internet* on your work computer.

Security software may mean that some sites are *blocked* or restrict access.

DO

Understand how to *search* safely online and how to report inappropriate *content* either via your organisation's ICT section.

Safe practice

Be aware that the organisation's *monitoring software* will log your activity.

Be aware that *keystroke monitoring software* does just that. This means that if you are online shopping then your *passwords*, credit card numbers and security codes will all be visible to the monitoring technicians

Poor practice

Misuse of personal information may be a breach of the *AUP*. Workers may be vulnerable to allegations as well as capability/ disciplinary/criminal process

DO NOT

Remember that accessing or *downloading* inappropriate or illegal material may result in criminal proceedings

Breach of the *AUP* may result in confiscation of equipment, closing of accounts and instigation of capability/ disciplinary processes

DO

What should be in place?

Cyber Security

- Staff and volunteers must take reasonable steps to protect JSENSE systems, accounts and data from cyber threats. This includes:
- Using strong passwords
- Keeping devices updated
- Avoiding public Wi-Fi where confidential information is accessed
- Not sharing passwords
- Reporting suspicious emails or cyber incidents immediately
- Locking devices when unattended
- Installing updates and security software where appropriate
- Confidential information must not be downloaded onto unsecured personal devices.

Mobile phones

Mobile phones or smart phones as most are these days are a 'must have' for children and young people – it is how they expect to communicate and be communicated with! We all carry them around too although we probably don't understand or use all that they are capable of doing. However you use your phone do not use your personal phone for professional use.

DO NOT

Don't use your personal mobile phone to communicate with children/ young people, their parents/ carers

This includes phone calls, text messages, email or web -based communications e.g. X/formally know as Twitter as well along with any other forms of social media

Misuse of personal information may be a breach of the AUP. Workers may be vulnerable to allegations as well as capability/disciplinary/criminal process

Best practice

Service users having your personal details may make you vulnerable to harassment or bullying

Safe practice

DO

Your organisation should provide equipment for you.

Know who/ where to get equipment from.

Make sure you know about inbuilt software/ facilities and switch off if appropriate

Poor practice

DO NOT

Don't use your own equipment without a manager's knowledge or permission – and in accordance with the appropriate AUP.

Don't retain *service user* contact details for your personal use.

Senior managers agree you can use your own equipment. Make sure you know how to employ safety measures like concealing your number by dialling 141 first.

DO

What should be in place?

- Use of personal equipment should be made clear in the *AUP*
- If the need for a *mobile phone* is for a one-off situation e.g. a trip out then workers know where the equipment is available from and the rules for returning it, making sure that it is fully charged and has sufficient credit.
- If the phone is to be used abroad then check that the phone has *network roaming access*.

Online Gaming

Online Gaming is an activity that can be considered purely personal. However this is another means of interacting socially with others – very often anonymous users but who may in fact be children and young people that you have a duty of care for.

Be aware of any organisation policy for online gaming during your working hours or using work computers.

Best practice

DO

Understand all aspects of your personal online gaming activity and take every step to ensure you are not socialising with children and young people that you have a professional duty of care over.

Safe practice

Be aware that the organisation's *monitoring software* will log your activity.

Misuse of personal information may be a breach of the AUP. Workers may be vulnerable to allegations as well as capability/disciplinary/criminal process

Poor practice

DO NOT

Don't encourage the children and young people in your care to socialise with you on gaming sites.

DO

What should be in place?

- The AUP makes explicit the consequences/ sanctions for inappropriate use of the *internet* and using online gaming in work-time.

Social networking (Facebook/X formally known as Twitter along with all forms of social media)

Social networking is software that enables people to stay in touch online via the *internet*. It provides support for sharing information, *images* and making contact with people who may share a common interest. It is very beguiling.

Social networking providers alter their functionality and rules for use on a frequent basis so it is very important to stay alert and check privacy settings.

Facebook and X formally known as *Twitter* are the most well known ones.

Best practice

DO NOT

Don't use your personal Facebook/ X formally known as *Twitter* profile to:

- communicate with
- share *images*
- take images of children/ young people and their parents/ carers

Whether using your personal or organisational equipment

Don't accept children and young people/ parents and carers as *friends* on your personal *page*.

DO

Consider creating a professional *profile* in agreement with your manager/ organisation.

Young people may have several profiles themselves (personal and one for parents to see) so will appreciate this approach.

Make sure that you don't have links to your personal *profile* because this defeats the object!

Regularly check all settings and make sure your security settings are not open access.

Ask your family and friends to protect your professional status and not post *tagged images* of you on their open access *profiles*

May affect your relationship with service users.
May affect professional status through professional body concerns about bringing the profession into disrepute

Make sure your security settings are not open access but set to family and friends only.

Don't accept people you don't know as friends – they could be service users. Go for equality not quantity.

Be aware that belonging to a 'group' can be a 'back door' into your profile.

Remember that posting certain bad/negative comments can sometimes be treated by the police as offences!

DO NOT

Don't have an open access profile that includes inappropriate personal information and images eg:

Holiday snaps, hen/stag nights.

Don't accept service users as friends on your personal profile.
Don't accept service users as friends once the work with them is completed. This means that other service users may gain access too your profile.

Don't accept ex-service users as friends.

Don't collect 'friends' including people you don't know in real life.

Don't use your personal profile to communicate with service users without your manager's knowledge or permission.

Don't write inappropriate/indiscrete posts about colleagues or service users

Poor practice

Breach of AUP. May make you vulnerable to harassment, bullying or allegations.
Disciplinary/capability/criminal processes may be instigated

DO

What should be in place?

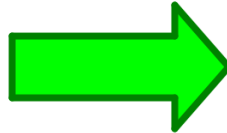
- The AUP should explicitly state that children/ young people and their parents/ carers should not be accepted as *friends* and include the sanctions for the breach of this policy.
- The AUP for the organisation should include guidelines for creating/ monitoring a separate professional *profile* if this is considered an appropriate way of working.
- The use of the *CEOP report* button should be promoted
- The AUP is part of the induction process and includes advice about the need for a professional online presence

Webcams

Webcams are small digital cameras that are either added to computers or are built in. They are a fantastic way of 2-way communicating between family and friends using communication technologies like *Zoom*, *Teams*, and *video-conferencing* for work colleagues who are physically separated. Great as they are there are some good practices to consider.

DO NOT

Don't use your personal webcam to communicate with children/ young people, their parents/ carers or to make a record of activity without permission



Make sure you know about inbuilt software/ facilities and switch off.

Safe practice

If your Senior managers agree you can use your own equipment, check the appropriate AUP.

Make sure you make arrangements to download images to the organisation network immediately after the event.

Misuse of personal information may be a breach of the AUP. Staff may be vulnerable to allegations as well as capability/disciplinary/criminal

Poor practice

DO NOT

Don't use your own equipment without a manager's knowledge or permission.

Do not retain service user information/activity for your personal use.

DO

What should be in place?

- Use of personal equipment including *webcams* should be made clear in the *AUP*
- If the need to use a *webcam* is for a one-off situation e.g. project, then appropriate organisational safeguards need to be in place
- Arrangements must be made for storing the work on the organisation's network immediately following the activity

Summary of good practice guidelines

DO

1. Set your *privacy settings* for any *social networking site* to ensure only the people you want have sight/ access to the *contents*. Keep these updated. The default settings for most *social networking sites* are set to open access where anyone can see everything.
2. Ensure your *mobile phone* (any technological equipment) is *password/ PIN* protected. This will ensure that other people can't use your equipment and get you into trouble.
3. Consider having separate personal and professional online identities/ *accounts* if you wish to have online contact with *service users* i.e. children and young people, their families and other professionals. Ensure that your manager is aware of your professional online persona.
4. Make sure that all information about you that is publicly available is accurate and appropriate – think particularly about whether photographs/ stories that you may have *posted* in your personal life are appropriate for a person with a professional life and a reputation to lose. If you don't want it to be public, don't put it online.
5. Remember that online conversations may be referred to as '*chat*' but they are written documents and should always be treated as such. Be mindful about how you present yourself when you are publishing information about yourself or having '*conversations*' on-line.
6. Make sure that you are aware of your organisation's policy regarding the use of both organisational and personal digital equipment and the consequences of misuse. Breach of the policy can result in capability/ disciplinary actions by your employer, professional body and criminal proceedings by the police.
7. Err on the side of caution. If you are unsure who can view online material, assume that it is publicly available. Remember - once information is online you have relinquished control of it. Other people may choose to copy it, to edit it, to pass it on and to save it.
8. Switch off any *Bluetooth* capability any device may have installed as standard. *Bluetooth* allows another person to have access to your equipment – they can then pretend to be you.
9. Always be aware that technology is constantly upgrading and improving. You may have access to *websites* via a work-provided *smart phone* that are blocked by your computer. Mobile phones come with *locator software*. Cameras can be a feature of *games consoles*. When you receive any new equipment (personal or private) make sure that you know what features it has as standard and take appropriate action to disable/ protect.

DO NOT

1. Give your personal information to *service users* i.e. children/ young people, their parents/ carers. This includes personal *mobile phone* numbers, *social networking* accounts, personal *website/ blog URLs*, online *image* storage sites, *passwords/ PIN* numbers etc.
2. Use your personal *mobile phone* to communicate with *service users* i.e. children/young people or parents/carers either by phone call, *text*, *email*, *social networking site*.
3. Use the *internet* or web-based communication to send personal messages to *service users* i.e. children/young people, parents/ carers.
4. Share your personal details on a *social network site* with *service users* i.e. children/young people, their parents or carers. This includes accepting them as *friends*. Be aware that belonging to a 'group' may give 'back door' access to your page even though you have set your *privacy settings* to family and friends only.
5. Add/allow *service users* i.e. a child/young person, their parents/ carers to join your contacts/friends list on personal *social networking profiles*.
6. Use your own digital camera/ video for work. This includes integral cameras on *mobile phones*.
7. Play *online games* with *service users* i.e. children, young people, their parents or carers. This can be difficult when the culture is to play with 'randoms'. Check out before you play online with someone you don't know.