

Urban Circle Newport Digital Safeguarding Policy

1. Purpose and aim of the policy statement

This is an Urban Circle policy. Urban Circle are a youth development charity who use creative platforms and youth and community work to enable young people and to build, promote and sustain constructive community relationships. We provide creative opportunities for young people to pursue their interests, improve their wellbeing and realise their potential across the creative arts, education, youth work and community development fields.

Urban Circle is committed to keeping participating children and adults safe and protecting them from harm. Safeguarding is everybody's responsibility. We all seek to create an ethos which helps children, young people and adults feel secure and able to talk freely, in the knowledge that they will be listened to, and their concerns taken seriously. This policy aims to enable staff to respond to safeguarding and child protection concerns in an informed and confident way. Safeguarding is not prescriptive or a tick-box exercise, only concerned with compliance. Urban Circle strives to create an embedded safeguarding culture where processes are part of the fabric of what we do every day.

This policy recognises that many young people communicate through, and socialise in, online and digital contexts, hence the importance of having a Digital Safeguarding policy that complements the overarching Urban Circle Safeguarding and Child Protection policy. This Digital Safeguarding policy reflects the NSPCC online safety policy statement (2022), The Wales Safeguarding Procedures (2019) *All Wales Practice Guide Safeguarding Children from Online Abuse: [Safeguarding Wales](#)* and guidance from the National Crime Agency Child Exploitation and Online Protection Centre (CEOP) [Professionals | CEOP Education \(thinkuknow.co.uk\)](#). It should be read in conjunction with the Urban Circle Safeguarding and Child Protection policy (v.5, 18.11.23).

Grooming describes the communicative process that abusive adults use to trick a child or young person into believing they are trustworthy so that they can abuse them on and offline. Grooming online can be far easier than offline for perpetrators because:

- Games, social media, live streaming platforms and chat rooms facilitate groomer attempts to contact children.
- Groomers can create multiple online identities and even pretend to be children and young people to trick children into chatting and sharing personal details, which can in turn enable one or more grooming processes (e.g. trust development, compliance testing).
- They can find out a lot about individual children before they make contact by looking at the things the child has posted online.
- Using this information they can target children who are particularly vulnerable and carefully plan how to groom them: what they will say to show an interest in them.

- They can also contact lots of children very quickly in the hope that one or more will respond and engage in conversation with them (Wales Safeguarding Procedures, 2019).

Online abuse is any type of abuse that is facilitated through technology like computers, tablets, mobile phones, consoles and other electronic devices (Wales Safeguarding Procedures, 2019). Online abuse takes many forms and may include:

Cyberbullying [Helping Children Deal with Bullying & Cyberbullying | NSPCC](#)

Online child sexual exploitation (CSE) [Child Sexual Exploitation & How to Keep Your Child Safe | NSPCC](#) and [Online abuse | NSPCC](#)

Online child criminal exploitation (CCE) [Criminal exploitation and gangs | NSPCC](#)

Radicalisation [Protecting children from radicalisation | NSPCC](#)

Sexting and sexual harassment (messages, self-generated images and/or exposure to online pornography) see more here: [Sharing nudes and semi-nudes | NSPCC](#)

Sextortion [Protecting Young People from Sextortion: A Guide for Parents and Safeguarding Professionals - Safer Schools \(oursaferschools.co.uk\)](#)

Sharing of sexualised imagery whether self-generated or not and other sexual communication

<https://www.nspcc.org.uk/globalassets/documents/online-safety/children-sending-receiving-sexual-messages.pdf>

Electronic communication encompasses all forms of online or technology based communication (email, text, messenger, direct message/private message and all forms of social media based communication).

Social media refers to the use of social networking sites such as WhatsApp, Facebook, Twitter, Instagram and other sites of a similar nature. This is not an exhaustive list.

Email communication specifically refers to the use of emails, including written text and/or pictures.

Text communication specifically refers to SMS (short message service), commonly known as text.

The National Occupational Standards for Youth Work (Community Learning Development Standards Council (CLDSC) (2019) set out the responsibility of youth workers to engage with and empower young people to make use of digital media in their daily lives (CLD, YW08) and assist young people to assess risk, equip young people with safeguarding techniques (CLD YW16) and make informed choices in the management of their health and well-being (CLD, YW08). Furthermore, they set out Urban Circle's responsibilities to monitor and review organisational policy and practices for the protection and safeguarding of young people and self (CLD, YW17).

2. Scope of the policy statement

The purpose of this policy is to protect children and adults from harm and provide staff with the overarching principles that guide our approach to safeguarding and child protection in an online context. This statement aims to:

- ensure that the safety and wellbeing of participants is paramount when they are using the internet, social media or mobile devices.
- provide staff and volunteers with the overarching principles that guide our approach to online safety.
- ensure that, as an organisation, we operate in line with our values and the law in terms of how we use online devices.

Although Urban Circle is a youth organisation we also work with young and older adults and therefore the principles and processes set out in this policy apply to work with adults as well as children. Youth work often works with children and young people from the age of 8 and up to 25 years. In safeguarding terms, older young people aged 18 to 25 years are termed 'adults at risk' (NYA, 2023).

The word staff is used throughout. This refers to all employed and/or voluntary Urban Circle representatives including trustees, paid staff, volunteers and freelance colleagues/consultants/occasional staff. This policy applies to all working at Urban Circle in any role, and all should follow it.

The word parent is used to refer to any adult with guardianship, caring and parental responsibility for the child or young person.

3. Context

The legislation and guidance underpinning the overarching Urban Circle Safeguarding and Child Protection policy (v.5 18.11.23) are relevant to this policy. The Wales Safeguarding Procedures 2019 *All Wales Practice Guide Safeguarding Children from Online Abuse* can be read here: [Safeguarding Wales](#). This policy has been drawn up based on legislation, policy and guidance that seeks to protect children in Wales. Other legislation and guidance relevant to this Digital Safeguarding policy are:

Communications Act 2003 which makes it an offence to make improper use of a public communications network. Section 127 specifically makes it an offence to send an electronic message that is grossly offensive or of an indecent, obscene or menacing character.

Malicious Communications Act 1988 which makes it an offence to send a communication with the intention of causing distress or anxiety.

Across the UK, the legislation setting out sexual offences also applies to online child sexual abuse, including:

- sexual communication with a child;
- causing or inciting a child to engage in sexual activity

- causing a child to watch a sexual act
- paying for sexual services of a child
- causing or inciting sexual exploitation of a child
- engaging in sexual activity in the presence of a child.

Trafficking and modern slavery legislation across the UK makes it an offence to traffic and/or enslave children for sexual exploitation and makes provisions for sentencing offenders. These can also apply to trafficking children for online sexual exploitation.

Sexual Offences Act 2003: The age of consent (the legal age to have sex) in the UK is 16 years old. The laws are there to protect children. They are not there to prosecute under-16s who have mutually consenting sexual activity but will be used if there is abuse or exploitation involved. To help protect younger children the law says anyone under the age of 13 can never legally give consent. This means that anyone engaging in sexual activity with a child who is 12 or younger will be subject to penalties set out under the Sexual Offences Act 2003. The law also gives extra protection to young people who are 16 to 17 years old. It is illegal to take, show or distribute indecent photographs.

Serious Crime Act 2015 criminalises conduct where an adult intentionally communicates (for example, by e-mail, text message, written note or verbally) with a child under 16 (whom the adult does not reasonably believe to be aged 16 or over) for the purpose of obtaining sexual gratification if the communication is sexual or intended to encourage the child to make a communication that is sexual (new section 15A (1) and (2)).

Counter-Terrorism and Security Act 2015 places a legal duty on specified authorities, including the Police, to have due regard to the need to prevent people from being drawn into terrorism. This is also known as the 'Prevent duty'. It places a number of responsibilities on those authorities and their partners.

4. Policy statement

We believe that:

- Children and young people should never experience abuse of any kind.
- Children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

We recognise that:

- The online world provides everyone with many opportunities; however, it can also present risks and challenges.
- For many children and young people using the internet is a typical part of their lives and has a significant impact on their social development.
- We have a duty to ensure that all children, young people and adults involved in Urban Circle are protected from potential harm online.

- We have a responsibility to help keep children and young people safe online, whether or not they are using Urban Circle's network and devices.
- Working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.
- All children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse. Many of the children and adults we work with are additionally vulnerable because of the impact of previous experiences including racism, their family, educational, social and cultural backgrounds as well as their learning needs. This must also be considered.
- Working educatively and in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible and empowered in their approach to digital safety.

We will seek to keep children and young people safe by:

Appointing an Online Safety Coordinator. This is Mohamed Miah

Adhering to the guidance on online safeguarding (Wales Safeguarding Procedures (2019), utilising this as a consistent reference point and source of information.

Supporting and encouraging participants to use the internet, social media platforms and mobile phones in a way that keeps them safe and shows respect for others.

Supporting and encouraging parents to do what they can to keep their children safe.

Ensuring that usernames, logins, email accounts and passwords are used safely.

Reviewing and updating the security of our information systems regularly.

Ensuring personal information about Urban Circle participants is held securely and shared only as appropriate.

Ensuring that images of participants are used only after their written permission has been obtained, and only for the purpose for which consent has been given.

Examining, critically reflecting upon and risk assessing any social media platforms and new technologies before they are used.

Providing supervision, support and training for all staff and volunteers on dealing with all forms of abuse, including bullying or cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation.

Providing clear and specific directions to Urban Circle staff and volunteers on how to behave online through detail within our Urban Circle Code of Conduct.

Developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult, child or young person.

Introducing an Online Safety agreement (Appendix C) with Youth Leaders and young people in relevant roles.

Recording and reporting online abuse.

All staff should follow the Urban Circle Safeguarding and Child Protection policy, recording and reporting concerns in line with both this policy and the Wales Safeguarding Procedures 2019.

Information, concern or the identification of possible risk or abuse obtained via online communication tools should be treated with the same vigilance as face-to-face disclosures and information.

Any safeguarding concerns that arise should be discussed with the Designated Safeguarding people as per the Urban Circle Safeguarding and Child Protection Policy.

If there is any information to suggest that a child is in current or immediate danger, for example, information that they intend to or have gone to meet a possible perpetrator, contact the Police on 999.

Never ask anyone to forward any images or videos to you and never forward any images or videos via technology yourself, even to the Police. Don't ever screenshot or take photographs of images on another device.

If you suspect that there might be images, chat logs and/or website history on any device belonging to the child then do not delete anything on the device. The device needs to be seized and retained in the state that it's found. If possible establish any PIN and device access details so the device can be examined by the Police in any investigation.

Make sure that your response considers the needs of the person experiencing abuse, any bystanders and Urban Circle as a whole.

5. Contact details for the Urban Circle Online Safety Coordinator (OSC) and Designated Safeguarding people (DSP).

Mohamed Miah	OSC	07760625117	Mohamad.miah@ucnewport.co.uk
Peter Landers	DSP	07860148868	peter_landers@hotmail.com
Loren Henry	DSP	07376053476	loren.henry@ucnewport.co.uk

6. Other helpful information:

Keeping safe online - Hwb (gov.wales)
www.askaboutgames.com
www.thinkuknow.co.uk
https://www.itai.info/downloads/
Stop It Now! Helpline: 0808 1000 900
NSPCC Online Safety Helpline: 0808 800 5002
www.ceop.gov.uk

7. Dates

We are committed to reviewing our policy and good practice annually. This policy statement will be implemented from 1st April 2024. It does not replace any other policy.

This policy will be reviewed before 1st April 2025.

Signed: Loren Henry

A handwritten signature in black ink that reads "L. Henry". The signature is written in a cursive style with a large, sweeping flourish at the end of the word "Henry".

Date: 01 April 2024

APPENDIX A: Procedures

1. Young people engaged in digital, IT, communications and media activity as part of Urban Circle activity

1. Up-to-date risk assessment and checks must be made to ensure activity is safe for use and age-appropriate.
2. All activity should be appropriately supervised.
3. When in use IT equipment should be visible, rather than out of sight.
4. Young people should be inducted, and staff should not assume that young people will instinctively know what appropriate and inappropriate digital behaviour looks like. This is an educative process, and it is our responsibility to support and challenge young people in this respect.
5. Staff should educate children and young people as to the risks of sharing personal information online.
6. Where possible staff should limit the amount of time children and young people spend online.
7. Staff should ensure that online safety filters are up to date and in use.

2. The use of Urban Circle IT and digital equipment

1. Usage of Urban Circle equipment or internet must follow the relevant Acceptable Use Policy.
2. It is prohibited for anyone to browse, download, access or share content which is illegal, harmful, violent, extremist, sexually exploitative, abusive, offensive or otherwise inappropriate using equipment or internet which has been provided by Urban Circle unless this is required for their role e.g. if in safeguarding and investigator roles.
3. Parameters for acceptable usage of equipment are set by Urban Circle, and Urban Circle may use software to limit the range of apps or tools staff or participants are able to access.
4. Equipment provided by Urban Circle should ensure that technical solutions are in place to protect the user, e.g. anti-virus, monitoring and filtering software.
5. Appropriate monitoring should take place based on the level of risk of the people involved (e.g. children, young people, vulnerable adults), and the content they will be accessing.

2. Professional use of social media

1. Urban Circle utilise social networking as an engagement tool for children, young people and other participants. These professional accounts serve a specific purpose and approval should be sought from Mohamad Miah before setting one up.
2. Staff responsible for the creation of online content on Urban Circle accounts and platforms should seek advice and sign-off from line managers on sensitive content or where they are concerned about the appropriateness of content.
3. Children, young people and vulnerable adults (who are participants) should not be tagged in online or social media posts.
4. All social media accounts should be password protected and at least 2 members of staff should have access to each account and password.
5. Staff must adhere to laws governing online communication tools. Staff must be mindful of the age requirements for some social platforms.
6. Any superfluous online communication tool or account should be closed at the end of a project, and/or when a staff member leaves.
7. Staff to use separate, designated social media platforms/accounts for the purposes of Urban Circle communications. This account may be checked by the Designated Safeguarding people and should be used for Urban Circle communications purposes only and not as a staff member's personal account.
8. Any communication using Urban Circle platforms/account should be kept public and kept logged. Messages should be saved and kept (both incoming and outgoing) and instant chat recorded and used appropriately.
9. All contact with young people using these platforms/accounts should be appropriate, as it would be in face to face communications.
10. Accounts should only be used within working hours.
11. Facebook Settings: the 'Posting Ability' function in settings, which allows staff to vet all posts before they appear on the page, must be enabled. The 'Profanity Filter' must be set to 'strong'. The 'Tagging Ability' must be set so that only page managers can 'tag'. Settings should be set to ensure that 'timeline and tagging' activity is always reviewed by staff before posts appear on their timeline.
12. Staff should support young people to maximise their own privacy settings, in the promotion of a whole Urban Circle online safety culture.
13. Staff should avoid communicating with young people outside typical working hours.
14. Posts should reflect organisational values and ethos and the typical tone of Urban Circle's communications.

3. Staff use of social media (personally)

1. Staff should maintain strict security on their own social networking profiles to avoid young people accessing personal information, posts and pictures.
2. Staff should not communicate with young people via personal accounts or friends, tag or follow young people from personal social media accounts. If staff have preexisting relationships with people who later become Urban Circle participants, then it is good practice to inform your line manager.
3. Staff should not initiate any form of pre-planned, private, out-of-work communication with Urban Circle participants that does not relate to the work of Urban Circle.

4. Consent

1. Consent for using electronic and online forms of communication is essential and should be explicitly clear on registration forms signed by parents.
2. Staff should ensure that young people are aware of, and consent to, their image (photograph and or video) being utilised across online media platforms, in the promotion of Urban Circle.
3. If a young person is under the age of 18, parental consent for the use of a child's image is required. Young people aged 18 and over can give consent but must still complete a consent form.
4. Consent needs to be routinely sought and renewed annually.
5. Adults, children's parents and, where possible, children must be given enough context to make this context 'informed'. They must be able to understand how their image or likeness may be used and what the consequences of this may be.
6. Participants retain the right to remove any pictures or stories about them from online spaces at any stage and should be made aware of this right.

5. Communication and Boundaries

1. Work phones should be used for electronic communication. Personal phone numbers should not be shared with participants. However, if in temporary, emergency or one-off circumstances this is not possible a line manager should be made aware. Where possible this should be agreed prior to personal phone use.
2. Electronic communication should only be used with children and young people for Urban Circle related matters, such as information about events and sessions, and responsibilities included within staff job descriptions, not for general socialising, contact or chatting.
3. Electronic communication should not be used as a relationship building tool.
4. Conversation (repeated sending of electronic communication such as text, WhatsApp or email between staff and young people) is discouraged.

5. Staff should make their line manager aware when they are using electronic communication to contact individual young people. Communication histories should be kept and dated. They should be accessible to colleagues and line managers as requested.

6. All should take care over the language used. This should reduce the risk of misinterpretation or over-familiarity. This guidance should be balanced with the need to use language that is accessible and understandable by participants.

7. Emails to participants should only be sent from Urban Circle email accounts rather than personal email accounts.

Concerns and complaints

1. If illegal, harmful, violent, extremist, sexually exploitative, abusive, offensive, or otherwise inappropriate content, not in keeping with the values and ethos of Urban Circle, is posted in Urban Circle groups or platforms, this should be hidden or deleted by group moderators, and where appropriate reported to third-party platform hosts.

Anyone can raise a concern about inappropriate or illegal content which has been posted online relating to Urban Circle activity. Concerns should be raised with Mohamad Miah, or with the Board of Trustees as appropriate so that they can moderate and remove this content and report to the appropriate person. Illegal content or a safeguarding concern should be raised with one of the Designated Safeguarding people so that they can deal with this appropriately and refer to Social Care, the Police or a support service where necessary.

APPENDIX B

Based on Hackett's continuum of children and young people's sexual behaviours (*Hackett, 2010*) and cited in Wales Safeguarding Procedures (2019). To be used as a reference point when reflecting on the nature of sexualised behaviour and related concerns with young people.

Normal – Online behaviours that are developmentally expected/ socially acceptable, consensual, mutual, reciprocal.

Examples: Two adolescents in a consensual romantic relationship send messages to one another, that have sexual content

A child / young person looks up information about body changes / puberty

Inappropriate – Single instances of inappropriate sexual behaviour / socially acceptable behaviour within peer group

Examples: Two adolescents in a consensual romantic relationship send self-produced naked images to one another

A young person looks at pornography occasionally

Child makes a deliberate search for sexual / age inappropriate content, but this is not repeated following sanctions

Problematic – Problematic and concerning behaviours, developmentally unusually and socially unexpected, no overt elements of victimisation

Examples: Young person sends a sexual message to another young person, which is unwanted

Young person sends a sexual picture to another young person that is unwanted

Child makes persistent deliberate searches for sexual / age inappropriate content

Young person persistently views pornography, to an extent that it is impacting on his / her welfare and emotional well-being

Abusive – Victimising intent or outcome, includes misuse of power, intrusive, informed consent lacking or not freely given by victim

Examples: Young person deliberately views / downloads indecent images of children

Young person deliberately makes indecent images of another child / young person, with the intention of sharing this with others

Young person exposes younger or more vulnerable child to sexually explicit content

Young person persistently sends sexual images / sexual messages to other people, without their consent and this may or may not include elements of threat or intimidation

Child regularly views sexually explicit content and is unable to cease this

Violent –

Examples: Child or young person views and reports being aroused to violent / extreme sexual content

APPENDIX C

Urban Circle online safety agreement for use with young people *(based on NSPCC (2019) [Example of an online safety agreement for use with young people](#) (nspcc.org.uk))*

Urban Circle understands the importance of children and young people being able to use the internet for enjoyment, education and personal development. This includes social media platforms, games and apps. We aim to support children and young people in making use of these in our work and take an educative approach to enabling young people to understand appropriate and inappropriate behaviour in online and digital spaces. However, we also recognise that safeguards need to be in place to ensure children are kept safe.

This agreement reflects the Urban Circle Code of Conduct (v. 2 31.01.24) and the Safeguarding and Child Protection policy (v.5, 18.11.23). If you would like to know more about either of these policies please speak to the Urban Circle Designated Safeguarding people or the Online Safety coordinator. They are:

Mohamad Miah	OSC	07760625117	Mohamad.miah@ucnewport.co.uk
Peter Landers	DSP	07860148868	peter_landers@hotmail.com
Loren Henry	DSP	07806431734	loren.henry@ucnewport.co.uk

Young person: please read the following agreement and discuss with your Urban Circle worker and parents/carers. Please sign it.

Parents/carers: please read and discuss this agreement with your child and then sign it, ask your child to sign it, and return it to their Urban Circle worker.

If you have any questions or concerns please speak to Mohamad Miah Communications Manager.

Young person's agreement

I will be responsible for my behaviour when using the internet, including social media platforms, games and apps. This includes the resources I access and the language I use.

I will not deliberately browse, download or upload material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to the group leader.

I will not send anyone material that could be considered threatening, bullying, offensive or illegal.

I will not give out any personal information online, such as my name, phone number or address.

I will not reveal my passwords to anyone.

I will not arrange a face-to-face meeting with someone I meet online unless I have discussed this with my parents and/or Urban Circle worker and am accompanied by a trusted adult.

If I am concerned or upset about anything I see on the internet or any messages that I receive, I know I can talk to [name of Urban Circle worker].

I understand that my internet use at Urban Circle will be monitored and logged and can be made available to my Urban Circle worker.

I understand that these rules are designed to keep me safe and that if I choose not to follow them, Urban Circle will discuss the implications of me not adhering to this agreement with me, and/or discuss with my parents/carers.

Signatures:

Young person:

Date.....

The Urban Circle worker who has discussed this with you

is.....

We have discussed this online safety agreement and [child's name] agrees to follow the rules set out above.

Parent/carer signature... .. **Date**

.....

Young person's signature... .. **Date**