Westgate Youth Project

Policy & Guidance

On the use of

Social Media and Online Safety

April 2022

Contents **Page**

1. Introduction and background 3
2. Principles 3
3. Wider Remit and Legal Consequences 4
4. Social Media – Guidelines, Principles and Procedures with regard to Personal and Professional and use 4
5. Online Communication and Safer Use Technology 7
6. Appropriate and Safe Use of the Internet and Associated Devices 8
7. Use of Personal Devices and Mobile Phones 9
8. Responding to Online Incidents and Concerns 9

Appendices

Appendix 1 Data Protection Principles and Law

Appendix 2 Procedures for Responding to Specific Online Incidents or Concern

1. Introduction

The purpose of this joint policy and guidance is to provide advice and support to Westgate Youth Project trustees and youth workers (both paid and voluntary) when using Social Media and other internet searches when working with children, young people, parents and foster carers. It covers five main areas:

1. The use of personal Social Media and boundaries in regards to personal/professional use.
2. The use of Social Media to gather information about children, young people and their families.
3. The use of Social Media when communicating with young people, their families and other professionals.
4. Westgate Youth Project, in dealing with employees that face harassment/bullying and abuse from other employees/service users on Social Media.
5. The use of Social Media to deliver key messages.

Background

Social Media has become an important part of everyday life and offers exciting opportunities for practice. However, as the ongoing development of Social Media develops and boundaries between our physical worlds and virtual worlds become more blurred, there is a need for professionals working with children to think about how they can practice in a way that embraces these opportunities whilst acknowledging some of the ethical and moral dilemmas that can arise.

As professionals, operating in the digital world, you must always have your professional role in mind and always consider how your behaviour could affect your professional reputation and employment.

There is an expectation that Westgate Youth Project staff will adhere to the policies and guidance that is available and understand what this means for them.

2. Principles

This guidance clearly identifies the key principles expected with regards to the safe and responsible use of technology to ensure a safe and secure environment for

online activities. It supports the application of Westgate Youth Project Policy including Acceptable Use of Technology Policy and Data Protection Policy.

This guidance must be read in conjunction with other relevant policies and guidance including Westgate Youth Project Safeguarding Policy and Procedure.

The guidance applies to all staff, volunteers, visitors and other individuals who work for or provide services on behalf of Westgate Youth Project, as well as children, young people and their carers. It applies to all access to internet and use of communication devices including personal devices or where children, young people or staff have been provided with Westgate Youth Project issued devices for use off-site such as a work laptop or mobile phone.

3. Wider remit and Legal Consequences

The use of online services and subsequent electronic communication such as Social Media use cuts across all aspects of work with young people and so staff should be aware that this guidance should be read in conjunction with WYP Data Protection policy (inclusive of General Data Protection Regulation (GDPR), Social Media policies and relevant legislation and guidance. Workers are further required to familiarise themselves with the following policies and ensure that they adhere to them:

- Data Protection Policy
- The Regulatory and Investigative Powers Act (RIPA 2000)
- GDPR Privacy Notice

All Workers who have access to online services through work equipment/networks, should be reminded of the legal consequences attached to the inappropriate use of those services. Although this list is not exhaustive, examples are inappropriate or offensive material include racist material, pornography, sexually explicit images texts and related material, the promotion of illegal activity, or intolerance of others.

.

4. Social Media-Guidelines and Principles

What do we mean by Social Media?

For the purpose of this guidance, is defined as any electronic communication that enables people to stay in touch online. Social Media includes web and mobile based technology which are used to turn communication into interactive dialogue between organisations, communities and individuals. Social Media provides support for sharing information, images and contacting people who may share a common interest. We live in a digital world where the ability to access information is instant. Young people often use Social Media. With such a growing array of information available on the internet there are expanding methods of instant messaging. Workers can use these tools/systems positively to facilitate communication to achieve better outcomes for young people and their families.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/490001/Social_Media_Guidance_UKCCIS_Final_18122015.pdf.pdf

The use of personal Social Media and boundaries in regards to personal/ professional use

The majority of staff working at Westgate Youth Project will have some form of personal Social Media presence, such as Facebook, Twitter, Snapchat, Instagram, WhatsApp, TikTok and other online footprints.

Whilst WYP supports its staff in the use of such applications and the right to a personal life, it is important for staff to take a sensible approach to the use of such Social Media platforms and consider (a) their security settings in regards to people being able to view personal information and (b) the potential professional implications of any posts they submit, like and/or share.

If Workers make a comment on the internet (blogs, Social Media, twitter etc.) on a personal basis, they must be aware, as an employee of WYP, that they are expected to comply with the standards of conduct and behaviour contained within this guidance.

Workers must make sure that they communicate in a way that supports WYP's policies including those on equality. Workers should therefore make sure you do not send/upload/post information on-line which:

- is unlawful including unlawful under the Equalities act 2010

- damages Westgate Youth Project's reputation or undermines public confidence in the project.
- includes any defamatory material or statements about any individual, firm, body or organisation; or
- harasses, bullies or stalks another person.

You must not email, upload or post confidential or sensitive data relating to individuals, partner organisations or any aspect of the project's business on the internet.

Workers need to consider that any inappropriate posts that fall under the above may call into question their professional integrity and as such, may result in subsequent disciplinary action through Westgate Youth Project's governing body.

The use of Social Media to deliver key messages from Westgate Youth Project

Principles

Staff have a duty to act in the best interests of young people and consider their right to respect, privacy and confidentiality whilst also managing and accessing risks online or Social Media.

Youth workers should support young people to use social networking where appropriate with awareness of its potential and risks.

When sharing key messages, youth worker must ensure that the information is provided by a trustworthy source (i.e.: Public Health England, NHS Health Visiting Service etc.).

Consent for images of children and young people to be used on social media (often for advertising purposes) must be sought and recorded on the child's file.

Procedure

WYP can set up a Social Media account (e.g Facebook, Twitter, Instagram.)

The account must be created by a single member of the team with full knowledge and approval by the Trustees

All accounts must have at least two admins

All posts must be for marketing purposes or sharing of information relevant to the project

Accounts being set up on social media for the above should clearly indicate they are Westgate Youth Project accounts

For the purpose of sharing key messages and advertising, account settings should be discoverable in order that they and be easily accessed by young people and families

Workers must make sure that they communicate in a way that supports the project's policies including those on equality. Workers should therefore make sure they do not send/upload/post information on-line which:

- is unlawful including unlawful under the Equalities act 2010
- damages the projects reputation or undermines public confidence in
- the project;
- includes any defamatory material or statements about any individual, firm, body or organisation; or
- harasses, bullies or stalks another person.

In response to key messages and advertising posts, children and young people may respond with comments and/or questions. These need to be responded to in a timely fashion.

5. Online Communication and Safer Use of Technology

Publishing images and videos online

All staff will ensure that all images are used in accordance with the Use of Camera and Images Policy and WYP guidance on the potential misuse of photographic images and how we can effectively safeguard children, young people and families.

In line with WYP guidance, written permission from parents or carers will always be obtained before images or videos of children and young people are electronically published.

6. Appropriate and Safe Use of the Internet and Associated Devices

- Westgate Youth Project staff and service users must adhere to the WYP Technology AUP.

- Any breaches may result in criminal, disciplinary or civil action being taken and this will depend on the age of those involved and the circumstances of the wrong committed. Action will be in accordance with the relevant WYP policies such as anti-bullying, allegations against staff, safeguarding and child protection.

Westgate Youth Project will use the internet to enable young people to communicate and collaborate in a safe and secure environment. The project provides access designed to enhance and extend provision. Members of staff will evaluate websites, tools and apps fully before use in the youth club or recommending for use at home.

Westgate Youth Project is aware that the internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace. Emerging technologies will be examined and appropriate risk assessments carried out before use is allowed.

Westgate Youth Project will take all reasonable precautions to ensure that young people access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a WYP computer or device. **Westgate Youth Project will ensure that appropriate filtering systems are in place to prevent young people from accessing unsuitable or illegal content.**

The youth work manager will audit technology use to establish if the online safety guidance is adequate. Methods to identify, assess and minimise online risks will be reviewed regularly. Filtering decisions, internet access and device use by young people and staff will be reviewed regularly.

Westgate Youth Project staff will ensure:

- The use of internet-derived materials by them and young people complies with copyright law and acknowledges the source of information
- Access levels to the internet are reviewed to reflect provision requirements and the age and ability of service users

- Young people use age and ability appropriate tools to search the internet for content
- Young people are encouraged to be critically aware of the materials they read and shown how to validate information before accepting its accuracy
- Young people are informed that network and internet use is monitored
- Supervision of children and young people to ensure safe and responsible use and be aware that they cannot rely on filtering alone to safeguard children and young people

The supervision of young people will be appropriate to their age and ability:

- Children and young people aged 10 years and over will be appropriately supervised when using technology, according to their ability and understanding in line with Fraser guidelines

7. Use of Personal Devices and Mobile Phones

Westgate Youth Project recognises that personal communication through mobile technologies is an accepted part of everyday life for young people and staff, but requires that such technologies need to be used safely, responsibly and appropriately during Westgate Youth Project sessions.

8. Responding to Online Incidents and Concerns

All Westgate Youth Project staff must follow the procedure for reporting online safety concerns (such as breaches of filtering, cyberbullying, illegal content etc.)

The Designated Person for Child Protection will be informed of any online safety incidents which will be recorded in the incident log. (They will ensure that online safety concerns are escalated and reported to relevant agencies in line with the KCSMP procedures).

Complaints about:

- Internet misuse will be dealt with under WYP complaints procedure
- Online bullying will be dealt with under WYP anti-bullying policy and procedure
- Staff misuse will be referred to the line manager and any allegations against a member of staff's online conduct will be discussed with the Local Authority Designated Officer (LADO)

Westgate Youth Project staff will:

- Be informed of the WYP whistle blowing procedure and confidentiality procedures when reporting concerns
- Be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence

Westgate Youth Project will:

- Inform parents and carers of any incidents of concerns as and when required
- Debrief, identify lessons learnt and implement any changes as required once investigations are complete
- Contact the LADO or Kent Police via 999 if there is immediate danger or risk of harm where there is concern that illegal activity has taken place is or taking place
- Escalate to the LADO if unsure of how to proceed with any incidents of concern

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Kent Police

Useful Resources

www.ceop.gov.uk

https://www.ipco.org.uk/

https://learning.nspcc.org.uk/child-abuse-and-neglect/online-abuse/

https://actnowtraining.wordpress.com/2015/09/10/facebook-social-networks-and-the-need- for-ripa-authorisations/

https://www.net-aware.org.uk/

https://www.internetmatters.org/resources/esafety-leaflets-resources/

https://www.gov.uk/government/collections/data-protection-act-2018

Appendix 1 Data Protection Principles and The Law

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/721581/Information_sharing_advice_practitioners_safeguarding_services.pdf

The seven golden rules to sharing information

1. Remember that the General Data Protection Regulation (GDPR), Data Protection Act 2018 and human rights law are not barriers to justified information sharing but provide a framework to ensure that personal information about living individuals is shared appropriately.

2. Be open and honest with the individual (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.

3. Seek advice from other practitioners, or your information governance lead, if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible.

4. Where possible, share information with consent, and where possible, respect the wishes of those who do not consent to having their information shared. Under the GDPR and Data Protection Act 2018 you may share information without consent if, in your judgement, there is a lawful basis to do so, such as where safety may be at risk. You will need to base your judgement on the facts of the case. When you are sharing or requesting personal information from someone, be clear of the basis upon which you are doing so. Where you do not have consent, be mindful that an individual might not expect information to be shared.

5. Consider safety and well-being: base your information sharing decisions on considerations of the safety and well-being of the individual and others who may be affected by their actions.

6. Necessary, proportionate, relevant, adequate, accurate, timely and secure: ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those individuals who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely (see principles).

7. Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

Taken from:HM Government (2018) Information sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers.

Appendix 2

Procedures for Responding to Specific Online Incidents or Concern

These procedures include the following:

Self-Generated Indecent Images of Children (SGIIOC or "Sexting")

Online Child Sexual Abuse and Exploitation

Indecent Images of Children (IIOC)

Radicalisation or extremism online

Cyberbullying

Online Hate Crimes

If Westgate Youth Project staff are made aware of an incident involving indecent images of a child or young person, online child abuse, indecent images of children, radicalisation or extremism online or cyberbullying they will:

- Act in accordance with KSCMP Procedures and Westgate Youth Project Safeguarding and Child Protection Guidance
- Immediately notify the Designated Person for Child Protection
- Store any devices containing evidence securely
- Carry out a risk assessment in relation to the children and young people involved
- Consider the vulnerabilities of children and young people involved (including carrying out relevant checks with other agencies)
- Make a referral to Children's Social Work Services through the Front Door and/or the Police (as needed/appropriate). Involve or consult the police if it is considered a crime has been committed
- Put the necessary safeguards in place for children and young people e.g. offer counselling support and immediate protection, offer appropriate pastoral support for those involved
- Inform parents and carers about the incident and how it is being managed

- Not view any images unless there is a clear need or reason to do so
- Not send, share or save indecent images of children and not allow or request children to do so
- Take action, regardless of the use of Westgate Youth Project equipment or personal equipment, both on and off the premises
- Take action to block access to all users involved and isolate any images
- Where appropriate involve and empower children and young people to report concerns regarding online child sexual abuse
- Take all reasonable precautions to ensure that children and young people are safe from terrorist and extremist material when accessing the internet
- Make staff aware of online child sexual abuse, including exploitation and grooming including the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns
- Review the handling of any incidents to ensure best practice and review and update procedures, where necessary

Immediately inform appropriate organisations e.g. the Internet Watch Foundation (IWF), Kent Police via 101 (using 999 if a child is at immediate risk), the LADO (if there is an allegation against a member of staff), CEOP by using the Click CEOP report form: http://www.ceop.police.uk/safety- centre/