**Policy and Guidance on the use of**

**Social Media and Online Safety for**

**Integrated Children’s Services**

**Version 11 – March 2021**

|  |  |  |
| --- | --- | --- |
| **Version History** | | |
| **Version** | **Date** | **Notes** |
| V1 | 25.10.17 |  |
| V2 | 27.10.17 | Comments added from reading first draft/EPV group |
| V3 | 02.11.17 | Comments from WKG |
| V4 | 09.11.17 | Further additions with inclusions from RiP and Community |
| V5 | 24.11.17 | Edited following EPV feedback |
| V6 | 03.07.18 | Further additions to include Early Help in procedure |
| V7 | 07.08.18 | Edited to include online safety leaflet and updates from EHPS |
| V8 | 23.01.19 | Review of Data Protection to GDPR |
| V9 | 06.03.20 | Review of language in line with CYPE and checks of relevant links to documents and added online safety guidance from EHPS combined social media and online safety |
| V10 | 09.10.20 | Edited to include tri-x update use of social media sites by Social Care and Safeguarding staff. |
| V11 | 24.03.21 | Additional amendments |

|  |  |
| --- | --- |
| **Contents** | **Page** |
| Executive Summary | **3** |
| Introduction and background | **4** |
| Principles | **5** |
| Wider Remit and Legal Consequences | **5** |
| Social Media – Guidelines and Principles | **7** |
| The use of personal social media by staff | **7** |
| The use of Social Media by Staff in a Professional Capacity | **8** |
| KCC’s response if Workers are being bullied / trolled on Social Media | **14** |
| Online Communication and Safer Use of Technology | **14** |
| Appropriate and Safe Use of the Internet and Associated Devices | **16** |
| Use of Personal Devices and Mobile Phones | **17** |
| Security and Management of Information Systems | **17** |
| Responding to Online Incidents and Concerns | **18** |

|  |  |
| --- | --- |
| **Appendices** | **Page** |
| Appendix 1 - Formal Consent to Make Further Enquiries | **20** |
| Appendix 2 - Data Protection Principles and Law | **21** |
| Appendix 3 - Procedures for Responding to Specific Online Incidents or Concerns | **24** |

**Executive Summary**

The purpose of this joint policy and guidance is to provide advice and support to staff in Integrated Children’s Services when using Social Media and other internet searches when working with children, young people and families, foster carers, and prospective adopters. It covers five main areas:

* **The use of personal Social Media and boundaries regarding personal/professional use.**

As professionals, you must always have your role in mind and consider how your behaviour could affect your professional reputation and employment. 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 personal online activities.

* **The use of Social Media when communicating with young people, their families and other professionals and/or to gather information. This may include known and/or suspected associates, relatives, or absent parents.**

This is a developing area and caution must be exercised; using Social Media to gather information about or communicate with a service user without their consent may contradict laws laid out in the Regulation of Investigatory Powers Act 2000 (RIPA) and The Office of Surveillance Commissioners (OSC) Procedures and Guidance.

Appropriate arrangements need to be made for setting up dedicated social

media accounts for a team or service. It is not appropriate to use professionals’ personal accounts or ‘fake’ accounts. Always seek authorisation from your manager before using Social Media in this way.

* **Integrated Children’s Services and KCC’s response in dealing with employees that face harassment/bullying and abuse from other employees/service users on Social Media.**

Any form of bullying or harassment is unacceptable and will not be tolerated, whether this takes place in the physical face to face world or in the virtual social media world. If a Worker becomes aware of such issues, then they are to inform their Manager who will follow the appropriate bullying and harassment procedures. A decision will be made as to whether there are grounds for disciplinary action or criminal aspects to the posts that need addressing.

* **The use of Social Media to deliver key messages across Integrates Children’s Services.**

Messages must be overseen, and quality assured by a manager. When sharing key messages, Workers must ensure that the information is provided by a trustworthy source. Workers must make sure that they communicate in a way that supports the Council’s policies including those on equality.

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 with advice sought from a Manager before doing so, if appropriate.

**Introduction and background**

Social Media has become an important part of everyday life and offers exciting opportunities for practice. However, as Social Media develops and boundaries between our physical worlds and virtual worlds become 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.

The use of social media in a social care and safeguarding environment is a developing area. Recent HCPC hearings regarding the misuse of Social Media have thrown a spotlight on this area and there are an increasing number of conversations within the world of social work regarding practice that have highlighted the need for a specific policy and guidance on how Social workers should regulate their Social Media use, both personally and when working with service users. This is just as relevant for staff in our Integrated Children’s service, such as Youth Justice teams, Early Help Units and Open Access, Youth and Children’s Centre’s.

Some of these concerning practices may include the covert use of social networking sites to solicit information on service users, setting up group pages involving young people without a clear term of reference on its usage, the lack of recording of decisions or conversations with service users on Social Media on the child’s file or case notes.

***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 staff in Integrated Children’s Services will adhere to the policies and guidance that are available and understand what this means for them.

This chapter is designed to highlight some of the issues to be considered, with links to additional information. It is not intended to provide any legal advice, and legal advice must be sought as appropriate.

**Working from Home/Remote Working**

It is important to remember that principles of data protection and confidentiality apply equally when working in a home environment as they do when working in an office environment. Remember that you are still working, and appropriate standards of professionalism should always be maintained. Do not post anything on personal social media accounts that could inadvertently disclose any confidential work material/issues/identifying information in relation to service- users.

**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 KCC Policy including ICT Acceptable Use Policy, Information Governance Policy, Security Policy, Data Protection Policy,

ICT User- Standards, Secure Email Policy, and Social Media Framework Guidance.

This guidance must be read in conjunction with other relevant policies and guidance including the Kent Safeguarding Children Multi Agency Partnership Board (KSCMP) Policy and Procedures on Safeguarding and Child Protection, KSCMP Online Safety Strategy, Online Safety Guidance for Educational Settings, KSCMP Sexting Guidance, KSCMP Safer Practice with Technology for Professionals and EHPS Safeguarding and Child Protection Guidance.

The guidance applies to all staff, volunteers, visitors, and other individuals who work for or provide services on behalf of the Integrated Children’s service 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 CYPE issued devices for use off-site such as a work laptop or mobile phone.

**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 families and staff should be aware that this guidance should be read in conjunction with KCC Data Protection policy (inclusive of General Data Protection Regulation (GDPR), Social Media policies and relevant legislation and guidance. This includes policy and guidance specifically relating to Social Work practice both at the national and Kent county-wide level. This guidance further builds on the Safer Working Practice Guidance for Adults Working with Children and their Families issued by the Government Offices in England in 2007.

Workers and their Managers are further required to familiarise themselves with the following policies and ensure that they adhere to them:

* Data Protection Policy
* Information Governance Policy
* Kent Code (http://search/pages/Results.aspx?k=kent%20code)
* KCC ICT Security Policy
* KCC Social Media Guidance
* ICT Acceptable Use Policy
* ICT User Standards
* BASW Social Media Guidance for Social Workers
* Coram BAAF Good Practice Guide – Undertaking Checks and References in
* Fostering and Adoption Assessment
* KCC Violent Behaviour at Work Policy
* The Regulatory and Investigative Powers Act (RIPA 2000) GDPR Privacy Notice

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

Social media can be a useful tool and offers new ways of working. For example:

1. Checking the social media accounts of missing children/young people, where they are public, as part of efforts to trace them.
2. Tracing/serving birth parents during court proceedings.
3. As part of assessments, to ascertain the veracity of information provided by parents and others.

***However, this is a developing area and caution must be exercised; using Social Media to gather information about or communicate with a service user without their consent may contradict laws laid out in the Regulation of Investigatory Powers Act 2000 (RIPA) and The Office of Surveillance Commissioners (OSC) Procedures and Guidance****.* This in turn may result in possible legal action from service users and internal disciplinary action from social work regulatory bodies and/or Kent County Council.

RIPA provides a framework to ensure investigatory techniques are used in a way that is compatible with Article 8, right to respect private and family life, enshrined in the European Convention on Human Rights (ECHR). RIPA ensures that these techniques are used in a regulated way and provides safeguards against the abuse of such methods.

Issues that must be considered are:

* Confidentiality and consent of service users.
* The need to process personal data in accordance with data protection principles.
* Professionals’ own right to privacy and private life.
* The need for caution and corroboration – social media accounts can be infiltrated/faked. Service-users may have more than one online persona.

Appropriate arrangements need to be made for setting up dedicated social

media accounts for a team or service. It is not appropriate to use professionals’ personal accounts or ‘fake’ accounts. Employers may wish to set up corporate private profiles with access limited to a small number of staff.

Depending on the circumstances, the viewing of service-users’ social media accounts may constitute overt or covert surveillance.

***Always seek authorisation from your manager before using Social Media in this way.***

**Social Media - Guidelines and Principles**

What do we mean by Social Media?

For this guidance, social media 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 a n d 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 and with such a growing array of information available on the internet there are expanding methods of instant messaging.

**The use of personal Social Media by Staff**

Many staff working in KCC will have some form of personal Social Media presence, such as Facebook, TikTok, Twitter, Snapchat, Instagram, WhatsApp, and other online footprints.

Whilst KCC 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 the following:

It is important to act in a way that does not compromise either the confidentiality of service-users or the safety and security of staff and their families. Social media can blur the boundaries between your personal and professional lives which staff should be wary of.

Professionals should be mindful of the implications for their own right to privacy and private life. Staff need to be vigilant to keep their own identity safe and that of friends and families. They need to consider the implications and risks of putting personal information on social media sites such as work, contact details and photographs of work colleagues and family members, and should not do so if they think their privacy and safety will be compromised. They may want to ask family and friends to bear this

in mind when posting information, as for example inappropriate pictures could open them up to criticism or pictures of their family online could create difficulties.

It should not be assumed that privacy settings will prevent information reaching a wider audience than that intended.

Inappropriate social media postings from personal accounts have led to Health and

Care Professions Council (HCPC) and Social Work England (SWE) proceedings against professionals.

Health and Care Professions Council Guidance on Social Mediasets out these Top Tips for professionals using social media in a personal capacity, to avoid breaching their professional responsibilities:

* **Think before you post**. Assume that what you post could be shared and read by anyone.
* **Think about who can see what you share and manage your privacy settings accordingly**. Remember that privacy settings cannot guarantee that something you post will not be publicly visible.
* **Maintain appropriate professional boundaries** if you communicate with colleagues, service users or carers. It is not appropriate to ‘accept’ service users and their Carers as online ‘friends’ in a personal network, as it creates a personal relationship outside of the workplace.
* **Do not post information which could identify a service user unless you have their permission**.
* **Do not post inappropriate or offensive material**. Use your professional judgement in deciding whether to post or share something.
* **When in doubt, get advice**.
* **IF YOU THINK SOMETHING COULD BE INAPPROPRIATE OR OFFENSIVE, DO NOT POST IT**.

KCC employees are expected to comply with the standards of conduct and behaviour contained within this guidance and within the Kent Code.

Workers must make sure that they communicate in a way that supports the Council’s policies including those on equality. Workers should therefore make sure they do not send/upload/post information on-line which is unlawful, including anything unlawful under the Equalities act 2010 or damaging to the Council’s reputation or which undermines public confidence in the Council.

You must not email, upload, or post confidential or sensitive data relating to individuals, partner organisations or any aspect of the Council’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 both KCC procedures and relevant regulatory bodies.

Social Workers should familiarise themselves with the BASW Social Media Policy:

<https://www.basw.co.uk/resources/basws-social-media-policy>

**The use of Social Media by Staff in a Professional Capacity**

Workers must understand that they should only use Social Media in particular

circumstances when working with and communicating with service users. Such actions must be based upon professional and/or safeguarding need, rather than to meet personal curiosity.

There must be a clear rationale, use must be proportionate, and with managers agreement and oversight.

**Information gathering and Assessment**

Workers may use Social Media in their practice for the following reasons:

1. As part of safeguarding investigations, whilst taking into consideration the importance of working with those professionals who are best placed, and legally able to undertake the task of scrutinising social media and to ensure it is in the service user’s best interest (Police for example)
2. To gather information for assessment and supervision purposes where there is a clearly identified need relating to safeguarding / criminal concerns.

Searches of social media activity of service-users and their associates can offer a useful means of information-gathering as part of the assessment process. For example, it can be used to check some aspects of a service user’s and/or their family’s/associate’s account of current or recent events which might affect the safety of a child or children, such as:

* Possible presence within the family environment of a Person Posing a Risk to Children
* Presence of known risky behaviour, such as drug and alcohol abuse.
* Where there are reasonable grounds to believe that information given by a family as part of the assessment is misleading or untrue e.g., the claimed separation of a couple where domestic abuse is known to be a significant risk factor.

*BASW Social Media Policy* [*https://www.basw.co.uk/resources/basws-social-media-policy*](https://www.basw.co.uk/resources/basws-social-media-policy)

This approach has been advocated recently in court cases and a serious case review. In the 2017 **Serious Case Review in relation to Child G**, the following learning was identified (para 1.3):

*‘When conducting assessments and reassessments of vulnerable families, practitioners may find that including internet and social media checks would enhance and triangulate information given by parents”.*

For more related case law see ***Re: T (A Child) [2017] EWFC 19*** where the Honourable Mr Justice Holman highlighted *“that social media may be a useful tool for tracing parents who are being served with a notice of adoption…”.*

***N.B. whilst the above case law highlights the use of Facebook, the principles should be applied to all forms of social media.***

***Courts and local authorities may have local protocols regarding the use of social media for service of court documentation. Legal advice must be sought as appropriate.***

Workers have a duty to act in the best interests of service users and consider their right to respect, privacy and confidentiality whilst also managing and accessing risks online or Social Media

In their practice, staff must seek consent from service users, foster carers and prospective adopters, if in the process of assessment or supervision, they intend to search the Internet using search engines and Social Media platforms. This searching should only take place once during the assessment process and should only happen again if there is clear rationale for a repeat search which should be recorded within the child’s file.

Justification for subsequent searches may include new information regarding an individual that suggests that a child may be at risk (either directly or by association), and / or for foster carers this may include a subsequent search as part of their annual review and or in response to any complaint / allegation (clear rationale for a repeat search should be recorded within the child/Carer’s file).

In their initial contacts with children and families, Workers should inform them that Internet and Social Media searches may be carried out, where deemed appropriate, to safeguard children and to prevent fraudulent/criminal behaviour. For families involved with Children’s Social Work Teams (CSWT), this should be covered within the consent of sharing information document (Appendix 1).

Where Social Media is used for assessment purposes, Workers and their Managers must agree there are reasonable grounds to believe information given by a family as part of the assessment requires further corroboration. This may include information that is misleading, seeking absent parents or other support needs and ensuring the safety of all children including those in foster care.

Should media searches identify issues concerning the child that raise clear safeguarding concerns then this should be acted on accordingly under Kent’s safeguarding procedures.

However, should a media search identify personal information concerning a young person or their parents which professionals know have not been shared with other family members (i.e.: transgender, sexual orientation etc.), a conversation

should be held with the person concerned to consider whether it would be beneficial for them to share this information with other family members. Staff will need to be sensitive to these discussions and need to adhere to the Equality Act 2010 and the Gender Recognition Act 2004 which sets out clear legislation in regards individual status and discrimination if personal information is shared without consent.

To carry out such searches KCC employed Workers will use appropriate established KCC accounts. They will not use personal Social Media accounts or create false profiles.

Where a Social Media account is setup by a team, Workers are responsible for understanding how it is used, by checking the security settings and the implications of Social Media being a public and permanent record.

Before using Social Media for the above purposes, Workers should discuss and reflect the necessity of this as part of professional supervision.

In all situations, Workers must discuss with their Manager, the purpose for

which they are using Social Media. All discussions and the rationale must be recorded on the child’s file.

**The use of Social Media when communicating with service users, and/or searching for parents or known/suspected members of a child or young person’s support network.**

Any attempts to establish contact with Service Users through social media should be discussed with a Manager and the rationale for making such attempts recorded on the child’s file (this is to safeguard both the service user and member of staff).

Contact should be made via established KCC accounts. However, there may be the rare occasion where a separate account using a pseudo name may be needed to communicate with a service user who is only able to communicate in this way due to significant risks (i.e. where a child/young person may be at risk of exploitation). In these circumstances the Worker and the young people involved, must have a detailed discussion, and be fully informed of the implications and their consent must

always be sought. All discussions in this regard must be recorded clearly on their individual case files and linked to any associated risk management plan.

When engaging service users through social media in this way, the Worker must choose a closed platform with no public access. There are many available which will have no personal footprint for service users to view each other’s personal data. Sites already used by KCC to this end may include Mind of My Own (MOMO).

When communicating through social media sites, staff must not give any identifying details of service users or their connections. Any specific conversations should happen once you have confirmed the person’s identity and Workers should only use private messages, never post to a person’s public profile.

There are occasions when consent cannot be gained when searching for absent parents and/or associates, or other ethical dilemmas may present themselves which may contradict KCC’s Data Protection policy (inclusive of General Data Protection Regulation (GDPR). In this instance Workers must seek agreement from a manager and if necessary, from KCC’s Information Governance Specialists in the Information Resilience & Transparency Team for further advice.

All communication and/or attempts at communication, should be recorded in the service users file, and be made via a KCC account as detailed above, in order to be visible and overseen by a manger.

When communicating with children or young people via social media Workers must check any age restrictions applicable to that platform and do not encourage a child or young person to access a platform which is not suitable for their age. There may be exceptions to this, whereby Workers can gain Parental Consent and communicate alongside and/or via the parent’s account (eg. to make a video call to both parent/carer and child)

As Social Media evolves and new sites, platforms or apps become available, agreement must be sought from a manager before communicating with service users or setting up a new account or group. A risk assessment must be undertaken, and staff would need to consult ICT and submit a software request with a valid business case.

Workers are advised against setting up groups via social media, as this approach will mean that service users may be able to see each other’s personal profile, which may then have unintended consequences (i.e. bullying / grooming). On smartphone applications (i.e.

WhatsApp) it is possible for users to see each other’s personal numbers (if a service user group) and this would again breach their personal data security.

Therefore, any such groups will need clear discussions with a Manager and authorisation given only if there is a clear rationale for the group to be set up, with a clear plan as to how the group, and the information within the group will be used and managed. This could include signed agreements between the service users and/or those with Parental Responsibility which agree safe use and privacy rules. This will avoid any issues highlighted in the previous paragraph. The rationale and decision making for setting up such groups should be clearly recorded on the child’s file. (This is to safeguard both the service user and member of staff).

Communicating over social media or other online platforms in other languages can be done by using online translation services (such as Google Translate). Workers should be aware that a “footprint‟ will be left of the information you type into this, so they should not use any identifying words and keep any use of these services short and with a view to an authorised translated conversation as soon as possible.

Online translation services are not always accurate and should under no circumstances be used for formal or lengthy KCC communications. In these instances, Workers should refer to KCC services. Workers should avoid informal personal contact with young people, children or service users they work with directly, or their Carers., through Social Media sites (e.g. do not add them as a „friend‟, „follow‟ them or link with them), or by using your own personal computer, laptop, tablet and/or smartphone (e.g. e-mail, text, calls).

Workers must not use Social Media to harass, bully, stalk or behave in any other way that could damage their working relationships with colleagues, members of the public or elected members or call into question your professional integrity.

Staff should discuss and reflect on dilemmas related to the use of social media in specific situations as part of professional supervision. Decisions should be made on a case-by-case basis and consider the best interests of those concerned.

**The use of Social Media to deliver key messages across Integrated Children’s**

**Service**

When sharing key messages, Workers 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/family record.

***Messages must be overseen, and quality assured by a manager.***

**General guidelines**

You are responsible for any data you share, promote or research on Social Media. This includes communication with service users.

* DO NOT behave in a way that could suggest that you are trying to develop a personal relationship with a service user with the view of covertly soliciting information for assessment purposes.
* DO NOT post any content that could be deemed defamatory, obscene or libellous either on your personal profile or one created in KCC‟s name.
* DO NOT post any comments that exhibit or a pp ear to endorse grossly irresponsible behaviour or law breaking of any kind.
* DO NOT create a page or profile in the name of KCC involving service users without following DATA Protection procedures and consent from service users.
* All decisions must be appropriately recorded.

**Procedure**

A team or service should set up a Social Media account. The account must be linked to a KCC email account. The email address and/or username and password should be shared with the manager and any other staff member within the team, if authorised by the manager.

* The account must be created by a single member of the team with full knowledge and approval by the Manager.
* All accounts must be supervised and regulated by the Manager.
* Any information must be checked by a Manager prior to posting.
* Accounts being set up on social media for the above should clearly indicate they are

Kent County Council Accounts

Social Media accounts linked to KCC in this way, can be accessed via a KCC device or a personal device. Staff should refer to ICT’s  [Using IT for Remote Mobile Working Policy.pdf](https://eur01.safelinks.protection.outlook.com/ap/b-59584e83/?url=https%3A%2F%2Fkentcountycouncil.sharepoint.com%2Fsites%2FKNet%2Fkentdocuments%2FUsing%2520IT%2520for%2520Remote%2520Mobile%2520Working%2520Policy.pdf&data=04%7C01%7Cclare.hall2%40kent.gov.uk%7C85c32fb11ac74244ef7408d8e56ecfec%7C3253a20dc7354bfea8b73e6ab37f5f90%7C0%7C0%7C637511611389438695%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=GSElw3tHOe1LWupsdbqArizih%2BDL3HJrLc0g1YXOrWc%3D&reserved=0) and  [BYOD Policy.pdf](https://eur01.safelinks.protection.outlook.com/ap/b-59584e83/?url=https%3A%2F%2Fkentcountycouncil.sharepoint.com%2Fsites%2FKNet%2Fkentdocuments%2FBYOD%2520Policy.pdf&data=04%7C01%7Cclare.hall2%40kent.gov.uk%7C85c32fb11ac74244ef7408d8e56ecfec%7C3253a20dc7354bfea8b73e6ab37f5f90%7C0%7C0%7C637511611389448690%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=UnWlwJjB0quWtQrsYfYcPjY4GunLS2fa1iPnwv4Swvg%3D&reserved=0) for secure use of personal devices and remote working.

If Staff require access to a social media site on a KCC device (including a KCC mobile phone) they would need to submit a software request with a valid business case. Staff should use the platform’s website in the first instance rather than installation of the app, unless the web version is restricting business requirement.

Account settings should be discoverable in order that they are easily accessed by children and families to share key messages and advertising

Workers must make sure that they communicate in a way that supports the Council’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 Council’s reputation or undermines public confidence in the Council.
* includes any defamatory material or statements about any individual, firm, body, or organisation.
* harasses, bullies, or stalks another person.
* All posts should follow general guidelines as cited on page 11.

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 with advice sought from a Manager before doing so, if appropriate.

**KCC’s response if Workers are being bullied / trolled on Social Media**

It is acknowledged that certain staff groups may be more vulnerable to bullying within and outside the workplace. As outlined in Section 1, KCC staff are reminded that any form of bullying or harassment is unacceptable and will not be tolerated, whether this takes place in the physical face to face world or in the virtual social media world.

As an employee of the Council, workers are expected to comply with the standards of conduct and behaviour in this policy and the Kent Code. Therefore, any posts online that cause upset and distress to fellow colleagues will be treated accordingly in line with Kent’s procedures.

Staff are also reminded of the legislation under the Equality Act 2010 and the Gender Recognition Act 2004. You should only identify a person’s transsexual status if you have permission to do so. „Outing‟ a person as transsexual is classed as direct discrimination under the Equality Act 2010 and could result in criminal charges under the Gender Recognition Act 2004. Disclosure of the fact that an employee has obtained a gender recognition certificate is a criminal act subject to a fine.

If a Worker becomes aware of such issues, then they are to inform their Manager who will follow the appropriate bullying and harassment procedures. A decision will be made as to whether there are grounds for disciplinary action or criminal aspects to the posts that need addressing.

For Workers who become aware of postings on social media about themselves that have been uploaded by service users, they must bring this to the attention of their Manager so that appropriate discussions can take place to agree on how this will be addressed. This may include meetings with the service users to discuss the impact of such posts on the Worker and their working relationship with the family, or in more serious cases where posts may contain offensive material / threats of violence to agree a clear risk assessment and plan in line with Health & Safety legislation. Consideration should be given to possible police action.

**Online Communication and Safer Use of Technology**

**Publishing images and videos online**

Integrated Children’s Service managers and staff will ensure that all images are used in accordance with the Use of Camera and Images in Educational Settings Policy and KCC guidance on the potential misuse of photographic images and how we can effectively safeguard children, young people and families.

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

**Managing email**

All members of staff are provided with a specific KCC email address to use for any official communication. The use of personal email addresses by staff for any official KCC business is not permitted.

Integrated Children’s Service staff must immediately tell their manager or the Designated Person for Child Protection if they receive offensive communication and this will be recorded in the online safety incident log.

In line with KCC policies, staff must adopt a responsible approach when using email:

 The forwarding of any chain messages or solicited bulk emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider

 Any electronic communication which contains any content which could be subject to data protection legislation must only be sent using secure and encrypted methods

 Sensitive or personal information will only be shared via email in accordance with data protection legislation

Access to external personal email accounts may be blocked



Excessive social email use can interfere with service provision and will be restricted

Emails sent to external organisations should be written carefully

**Staff must not:**

 **Send e-m ai l s that are abusive, malicious, discriminatory, defamatory about any person or organisation or which contains illegal or offensive material or foul language** **Open attachments to emails from unknown sources.**

**Official videoconferencing and webcam use**

All videoconferencing equipment will be switched off when not in use and, where appropriate, not set to auto answer.

The equipment will be kept securely and, if necessary, locked away when not in use Videoconferencing equipment will not be taken off KCC premises without permission from relevant manager.

Responsibility for the use of videoconferencing equipment outside of KCC working hours will be agreed by the relevant manager.

Staff will ensure that external videoconferencing is suitably risk assessed and that accounts and systems used to access events are appropriately safe and secure.

**Appropriate and Safe Use of the Internet and Associated Devices**

Integrated Children’s Service staff and service users must adhere to the KCC Policy and ICT User Standards.

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 KCC policies such as anti- bullying, allegations against staff, safeguarding and child protection.

All KCC owned devices will be used in accordance with the KCC Acceptable Use Policy and with appropriate safety and security measures in place. All users will be informed that network and internet use will be monitored.

Integrated Children’s Services will use the internet to enable service users to communicate and collaborate in a safe and secure environment. Children’s centres and youth hubs provide access designed to enhance and extend provision. Members

of staff will evaluate websites, tools, and apps fully before use in the children’s centre or youth hub or recommending for use at home.

Integrated Children’s service 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.

Integrated Children’s service will take all reasonable precautions to ensure that service users 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 KCC computer or device. **Integrated Children’s service will ensure that appropriate filtering systems are in place to prevent service users from accessing unsuitable or illegal content.**

Integrated Children’s service managers 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 service users and staff will be reviewed regularly.

Integrated Children’s service staff will ensure:

* The use of internet-derived materials by them and service users 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.
* Service users use age and ability appropriate tools to search the internet for content.
* Service users are encouraged to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
* Service users 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 service users will be appropriate to their age and ability.
* Children up to 7 years of age will be by adult demonstration with occasional directly supervised access to specific and approved online materials.
* Children ages 7 – 11 years will be supervised using age-appropriate search engines and online tools.
* Children and young people aged 12 years and over will be appropriately supervisedwhen using technology, according to their ability and understanding in line with Fraser guidelines.

**Use of Personal Devices and Mobile Phones**

Integrated Children’s service recognises that personal communication through mobile technologies is an accepted part of everyday life for children, young people, staff and parents and carers but requires that such technologies need to be used safely, responsibly and appropriately in KCC buildings such as children’s centres and youth hubs.

The use of mobile phones and other personal devices by young people and adults will be decided by the relevant manager and covered in appropriate guidance including the EHPS Photographic Image and Mobile Phone Use Guidance.

**Security and Management of Information Systems**

All Integrated Children’s service staff must adhere to the KCC ICT Acceptable Use Policy, Information Governance Policy, Security Policy and ICT User Standards. This includes:

Adhering to the principles of the Data Protection Act 2018 and General Data Protection Regulations (GDPR).

 Personal data sent over the internet or taken off site (such as via portable media storage) will be encrypted or accessed via appropriate secure remote access systems

 Portable media will not be used without specific permission followed by an anti-virus scan.

Unapproved software will not be allowed in work areas or attached to email.

Each member of staff has their own unique username and password to

access KCC systems. Staff must always keep their password private and must not share it with others or leave it where others can find it.

The appropriate use of user logins and passwords to access the KCC network will be enforced.

All service users will be informed not to share passwords or information with others and not to login as another user at any time.



All users will be expected to log off or lock their screens/devices if systems are unattended.

Integrated Children’s service children’s centres and youth hubs use KCC filtered secure broadband connectivity.

Any material accessed that Integrated Children’s service believes is illegal will be reported to appropriate agencies such as KCC ICT service desk, Kent Police or CEOP immediately.

**Responding to Online Incidents and Concerns**

All Integrated Children’s service staff must follow the procedure for reporting online safety concerns (such as breaches of filtering, cyberbullying, illegal content etc.) shown in Appendix 3.

The Designated Person for Child Protection will be informed of any online safety incidents which will be recorded in the district 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 KCC complaints procedure.
* Online bullying will be dealt with under KCC 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)

Integrated Children’s service staff will:

* Be informed of the KCC whistleblowing 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.

Integrated Children’s service will:

* Manage online safety incidents in accordance with KCC discipline/behaviour policy, where appropriate.
* 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.

**Appendix 1**

**STRICTLY CONFIDENTIAL**

**FORMAL CONSENT to Make further Enquiries**

Parent(s):

Name of child: Date of Birth:

Name of child: Date of Birth:

Name of child: Date of Birth:

(print name) , give consent for the agencies listed below to share relevant information about myself and/or my children with Kent County Council in order to gather information relevant to the assessment process.

This information gathered will be stored on the case file. The information gathered will not be shared with other professionals unless there is Child Protection concern or if it is deemed necessary for your child’s wellbeing.

|  |  |  |  |
| --- | --- | --- | --- |
| General Practitioner/Dentist |  | Health Visitor |  |
| School and/or Nursery |  | Police |  |
| Probation |  | Housing |  |
| Family Members |  | Solicitor |  |
| Consent for Early Help (where  applicable) |  | Permission to share assessments  with |  |
| CRI |  | Internet & Social Media searches |  |
| Any other Local Authority |  |  |  |

Signed: Date:

Print Name: Date

**Appendix 2 Data Protection Principles and The Law**

**Data Protection**

Information gleaned from searches of social media sites will constitute ‘personal data’ which

must be processed in accordance with data processing principles. It must be:

* Processed in a way that is lawful and fair.
* For specified, explicit and legitimate purposes.
* Adequate, relevant, and not excessive.
* Accurate and kept up to date.
* Kept for no longer than is necessary.
* Processed in a secure manner.

**Consent**

It is good practice, where enquiries are likely to include searches of social media sites, to make service-users generally aware of this fact by including this in the information which is given to them at the commencement of the process, for example at the commencement of the Assessment.

In specific cases, social media searches, as with other forms of information-gathering for Assessment purposes, should generally take place with the consent of the subject, unless there are valid reasons to the contrary. There may be an ‘overriding public interest’ in obtaining and sharing information without explicit consent. This will depend on the circumstances of each case. For more information, see: Confidentiality Policy. 2.3 Covert/Overt Surveillance and the Regulation of Investigatory Powers Act 2000 Viewing a service-user’s social media content without their specific consent is not necessarily, of itself, unlawful.

However, consideration must be given, in all cases, as to whether viewing the sites constitutes ‘directed surveillance’ under the Regulation of Investigatory Powers Act 2000 (‘RIPA’) and so requires authorisation under that Act. This is a complex area. The existing legislative provisions, the stated views of the Chief Surveillance Commissioner and the current attitudes of the courts are not necessarily easy to reconcile, and this is an area which will, no doubt, continue to develop by way of case-law. In a letter to local authorities in April 2017, the Chief Surveillance Commissioner concedes that:

*‘****These are complex legislative provisions, and without appropriate training and awareness council officers cannot be expected to appreciate and apply them. They may therefore act unlawfully. Ignorance would provide no defence to them personally, nor to the Council for which they were working’.***

Whilst the following general principles apply, each case must be treated on its own facts, and legal advice MUST be sought as necessary:

If the consent of the service-user is obtained, then no further authorisation would be required.

If consent is not obtained but no privacy settings are in operation to prevent viewing, then the material available on the sites can be regarded as ‘open source’, and so a single viewing would not constitute ‘directed surveillance’ under RIPA and no authorisation would be required under that Act; However, the Chief Surveillance Commissioner has made clear his view that repeat viewing of sites by staff may constitute ‘directed surveillance’ and if done covertly (i.e. without the knowledge of that person) then this would be ‘covert surveillance’. This would require authorisation under the Act in the form of a warrant from a magistrate. \* It is for the employer to ensure that any covert surveillance is properly authorised, recorded and, most importantly, legally justifiable. See also the **Covert Surveillance and Property Interference Code of Practice**.

\*(The Protection of Freedoms Act 2012 amended the regulation of investigatory powers legislation to reduce the circumstances in which a surveillance authorisation under RIPA can be granted by a local authority, rather than by a court. A local authority can now only grant an authorisation under RIPA for the use of directed surveillance for the investigation of criminal offences which attract a maximum custodial sentence of 6 months or more or relate to the underage sale of alcohol or tobacco. Surveillance as part of any other investigations, e.g. child welfare/protection, can only be authorised by a court).

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attach ment\_data/file/721581/Information\_sharing\_advice\_practitioners\_safeguarding\_servi ces.pdf](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 3 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 Integrated Children’s service managers and 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 Integrated Children’s service.
* 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 Integrated Children’s service 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/.