Kent County Council

Policy and Guidance on the use of Social Media for Social Workers and Early Help Workers

Version	Date	Notes
V1	25.10.17	
V2	27.10.17	Comments added from reading 1st draft / EPV group
V3	02.11.17	Comments from WKG
V4	09.11.17	Further additions with inclusions from RiP and Community care
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

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 the 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.

Recent HCPC hearings regarding the misuse of Social Media have thrown a spot light 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 specific policy and guidance on how Social workers should regulate their Social Media use, both personally and in particular when working with service users.

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 terms 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, whenever you are operating in the digital world or using Social Media, 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 Workers will these policies and understand what that means for you.

Introduction

The purpose of this joint policy and guidance is to provide advice and support to Social Work staff and Early Help staff when using Social Media and other internet searches when working with children and families, foster carers and prospective adopters. 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 and their families. This may include known and/or suspected associates and absent parents.

3 – The use of Social Media when communicating with young people, their families and other professionals during intervention or assessment.

4 – Social Work and Early Help staff and KCC's response 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 across Social Work and Early Help services.

Wider remit and Legal Consequences

The use of online services and subsequent electronic communication / Social Media use cuts across all aspects of work with families and so Workers 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:

- 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
- CoramBAAF 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/networks, 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 include racist material, pornography, sexually explicit images texts and related material, the promotion of illegal activity, or intolerance of others.

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.

What do we mean by Social Media?

The term Social Media is used in a number of ways, but 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 making contact with people who may share a common interest.

Why Do Worker's use Social Media?

We live in a digital world where the ability to access information is instant. Young people often use Social Media as a means of communicating through the use of modern communication tools and systems. With such a growing array of information available on the internet and expanding methods of instant messaging, Workers can use these tools/systems positively to facilitate communication to achieve better outcomes for children 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

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

The majority of staff working in KCC will have some form of personal Social Media presence, through such applications, as Facebook, Twitter, Snapchat, Instagram, WhatsApp and other online foot prints.

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 (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 the Council, that they 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 you **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; 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 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.

Workers should familiarise themselves with the BASW Social Media policy and KCC Social Media policy: which clearly sets out clear guidance. (see links below)

https://www.basw.co.uk/resource/?id=1515

2 – The use of Social Media to gather information about children and their families/ foster carers / prospective adopters and their families. This may include known and/or suspected associates and absent parents.

Policy

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 clear rationale for carrying out such searches and consideration also given to the frequency of such searches, as frequent searching on the same Service User may be in direct conflict with Investigatory Powers Commissioners Office (IPCO) (www.ipco.org.uk).

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

- To gather information for assessment and supervision purposes where there is a clearly identified need relating to safeguarding / criminal concerns.
- To search for and communicate with absent parents and relevant members of a young person's support network
- To communicate with service users for the purpose of providing advice and support in accordance with the agreed care or family support plan (see section 3)

Principles

- 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 on line or Social Media
- In their practice, Workers should support service users of all ages to use social networking where appropriate with awareness of its potential and risks
- **Workers must seek consent from all 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 Specialist Children's Services, 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 considered to be 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 (ie: 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 are reminded that they 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.
- In order 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 particular Social Media, i.e. Facebook or twitter, Instagram. All discussions and the rationale must be recorded on the child's file.

Procedure

- Every team can set up a Social Media account (Facebook, twitter, Instagram)
- The account must be linked to a KCC email account
- 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
- Where there is a potential risk of harm to a child, or criminal / gang associated activity that requires a covert Social Media investigation, a strategy discussion will be required, and where appropriate actions will be taken by the police to undertake such investigations.
- Where Social Media is used to search for absent parents (eg. absent fathers, support networks), it must be made clear to the known family who and why contact is being made. Data Protection principles (ijn line with the GDPR) must be applied in conjunction with all applicable data protection laws. (Appendix 2)
- Accounts being set up on social media for the above should clearly indicate they are Kent County Council Accounts and should use the following format: **KCC/District/team i.e Facebook – First name is KCC surname Ashford CSWT1**
- These accounts should then have their privacy settings set to **maximum** to prevent other users following these accounts.

3– The use of Social Media when communicating with young people, their families and other professionals during social work intervention or assessment.

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' file. (This is to safeguard both the service user and member of staff).

Contact should be made through the use of 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 associating with gangs / CSE). 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 (such as Facebook or Twitter) Workers 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.

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 will avoid any of 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 in to 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

4 - KCC's response if Workers are being bullied / trolled on Social Media by other KCC employees or by Service Users.

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 on line 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.

General guidelines –

- Remember 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 libelous either on your personal profile or one created in KCC’s name
- DO NOT post any comments that exhibit or appear 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 proper DATA Protection procedures and consent from service users
- All decisions must be appropriately recorded.

5 – The use of Social Media to deliver key messages across Social Work and Early Help services.

Open access services often use social media in order to promote key messages and advertise their services to their local community. Facebook, Instagram and Twitter are helpful platforms for this to happen.

Principles

- 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 on line or Social Media

- In their practice, Workers should support service users of all ages to use social networking where appropriate with awareness of its potential and risks (appendix 4 – e-safety leaflet)
- 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.
- Platforms used by open access to promote key messages etc

Procedure

- Every team can set up a Social Media account (Facebook, twitter, Instagram.)
- The account must be linked to a KCC email account
- 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 to ensure that it is in line with Government and Local initiatives (such as UNICEF baby friendly initiative and youth hub curriculum)

- Accounts being set up on social media for the above should clearly indicate they are Kent County Council Accounts

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

- 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; or
    - harasses, bullies or stalks another person.

- All posts should follow general guidelines as cited page 7

- 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.

Web Sources of information

www.ceop.gov.uk

http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/collecting_
personal_information_from_websites_v1.0.pdf

www.ico.gov.uk

http://police.homeoffice.gov.uk/publications/operational-policing/social-networking-guidance/

http://police.homeoffice.gov.uk/publications/operational-policing/moderation-document-final.pdf

www.iabuk.net

www.icpo.org.uk

http://www.nspcc.org.uk/Inform/cpsu/Resources/Briefings/PhotographsAndImagesOfChildren_wdf
60645.pdf
https://actnowtraining.wordpress.com/2015/09/10/facebook-social-networks-and-the-need-for-ripa-authorisations/

https://osc.independent.gov.uk/wp-content/uploads/2016/07/OSC-Procedures-Guidance-July-2016.pdf

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: __________

Name of child: ________________________________ Date of Birth: __________

I, (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 Early Help (where applicable)	
CRI		Internet & Social Media searches	
Any other Local Authority Departments		Any Other – Social worker to identify	

Signed: ____ Date: __________

Print Name: _______________________________________

Appendix 2 - The Seven Golden Rules for Sharing Information

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:

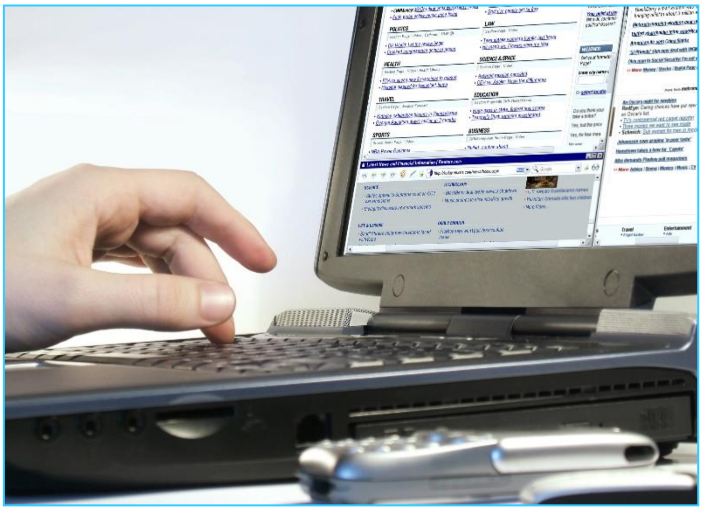
HM Government (2018) Information sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/721581/Information_sharing_advice_practitioners_safeguarding_services.pdf

AAppendix 3 - E-Safety Leaflet

Kent County Council kent.gov.uk

Sure Start Children's Centres

Protect Your Family On-line



Kent County Council kent.gov.uk

Social networking

Social networking sites can be fun, interactive and a quick way to stay in touch with friends and family online.

Be careful what you put online

Review your privacy settings regularly - make sure only the people you want to know about you can read your profile and updates. Also, review where you're tagged in photos.

Be careful who you 'friend' online - some people may not be who they say they are, while others may say nasty or inappropriate things. Think twice before you allow someone to 'follow' you.

Don't give out personal details - for example, your date of birth or what school/college you go to. It's a good idea to put as little personal information as possible on social networking sites to avoid people knowing too much about you.

Think twice about the information you post online - for example, posting that you're off on holiday (and therefore your house may be empty) or that you have a brand new car. Other people could use this against you and you risk having your property stolen.
Carefully consider what **photos** you share online and what impression this gives (i.e. potential employers).

Hoax and Chain Messages

What is a Hoax or Chain Messages?

A hoax or chain message is any message (received via email, text or website etc) that, either through overt instruction or through compelling content, encourages the reader to pass it on to other people. Chain messages can range from promises of money (such as lottery wins or pyramid schemes), hoax stories promising luck, answering questionnaires, threats to personal safety, to hoax virus alerts.

Chain messages are started and sent for many reasons. The most common reasons are for generating money, harvesting personal data (email addresses), virus attacks, clogging up computer networks or programmes or for collecting email addresses to use to send people junk and unwanted (spam) messages.

What does a chain or hoax message look like?

Common signs to spot a message could be a hoax or chain message is:

- The email states "this is a completely true story," or "it's perfectly legal." If the author feels he or she has to make it clear, then it's probably not
- It relays an account of events that supposedly happened to an unidentified third person (i.e. "the dear son of the neighbour of someone my friend knows")
- It warns that if you don't forward the message within a certain time frame that something unpleasant will happen such as bad luck, a problem with your computer or even death. People are often motivated by extremes and we respond faster when we believe the consequences of our inaction could be swift and severe
- Most importantly a hoax or chain message **asks, begs or bullies you to forward it on to everyone you know**

What can I do if I or someone I know receives a chain message?

The simple and most effective solution is to delete the email or text. But all too often people don't do that. These steps can help to keep you safe:

- Don't send anyone any money, whoever contacts you via email.
- Don't forward the e-mail to friends and family.
- If you are still unsure what to do you can call or report the scam to Action Fraud: www.actionfraud.police.uk or 0300 123 2040

Online Phishing

Phishing is a type of deception designed to steal your personal data to commit identity theft. Criminals send emails to thousands of people which pretend to come from banks, credit card companies, online shops and auction sites as well as other trusted organisations. They usually contain a very compelling and urgent but bogus reason to go to the site, for example to update your password before your account is suspended.

Victims click on an embedded link in the email itself which takes them to a website that looks exactly like the real thing but is, in fact, a fake, designed to trick victims into entering personal information such as a password or credit card number. .

How can I tell if it’s a phishing email?

Criminals can make an email look as if it comes from someone else. Fake emails often (but not always) display some of the following characteristics:

- The sender’s email address doesn’t tally with the trusted organisation’s website address
- The email is sent from a completely different address or a free web mail address
- The email does not use your proper name, but uses a non-specific greeting like “dear customer”
- A sense of urgency; for example the threat that unless you act immediately your account may be closed
- A prominent website link. These can be forged or seem very similar to the proper address, but even a single character difference means a different website
- A request for personal information such as user name, password or bank details
- You weren't expecting to get an email from the company that appears to have sent it

Protect yourself

- Use Anti-virus/Spyware programmes – phishing filters can often be built into web browsers or can be added on
- Delete and report any emails you are suspicious of
- Report the e-mail to the faked or "spoofed" organisation. Go directly to their website via your browser and not via the link provided in the suspicious email
- You can report suspicious or phishing emails online to the Anti-phishing Working Group at www.antiphishing.org/report_phishing.html and Bank Safe Online at http://www.banksafeonline.org.uk/report_scam.html , so that the information can be quickly shared between all the banks
- Never click a link in a suspicious email, always make sure you go to the site via your address bar in your browser to ensure you are visiting the correct website
- If it looks too good to be true then it probably is!
- Visit www.getsafeonline.org to find out more about keeping safe and secure online

Keeping your children safe

The best way to help your child to be safe when using the internet is to ensure they understand these rules:

NICKNAME - never give out personal details to online “friends” (an online “friend” is anyone you have not met in real life). Use a nickname when logging on and do not share full name, email address, mobile number, school name and any photos etc

WHERE - encourage your child to use the computer/laptop/other devices on line in a family area in the house, rather than their bedroom so you can see what they are accessing

CONTROLS - use parental controls and filtering products on any internet enabled devices (mobile phones, games consoles, tablets etc) but be aware that they can be bypassed

TALK - be aware that mobile devices cannot always be supervised and parental controls may fail so it is important to talk to your child about online risks and how to manage them

UPSET - If your child receives a message that upsets them, remind them not to reply, they should save the message and show you or another trusted adult

LIES - help your child to understand that some people lie online. They should never meet with an online “friend” without an adult they trust

BLOCK - make sure they know how to block someone online and report them if they feel uncomfortable

SOCIAL NETWORKING - it is often against the site regulations for a child under 13 years to set up social networking profiles

BLAME - make sure your child feels able to talk to you, let them know it is never too late to tell someone if something makes them feel uncomfortable. Don’t blame your child, let them know you trust them

Shopping safely online

There are a few steps you can take to shop online safely and keep your financial details secure.

Before you buy

Before you buy online, note down the address, telephone and/or fax of the company you're buying from. Never rely on just an email address.

Always use secure site

Sites with 'https' in front of the web address mean the site is using a secure link to your computer. A yellow padlock symbol will appear in the browser window to show the payment process is secure.

When buying online:

1. Never transfer or receive money for someone else
2. Check the site's privacy and returns policy
3. Print out a copy of your order and any acknowledgement you receive
4. Check your bank statement carefully against anything you buy online
5. Keep your passwords secure
6. Take your time making decisions that involve parting with money
7. Get independent financial advice before making investments
8. Only do business with companies you recognize or have been recommended by someone you trust - don't judge a company on how professional their website looks
9. If in doubt, check a company is genuine by looking them up on Companies House or the Financial Services Authority (FSA) websites

Online dating

Risks

Some of the risks we worry about are:

- Personal safety when meeting someone you met online
- Stalking and harassment
- Meeting people who shouldn't be dating online
- Dating sites being used as vehicles for spam, selling or fraud

In a few cases, criminals find their victims online and attack them when they meet. These are serious risks, but you can protect yourself by following a few guidelines, trusting your instincts and using common sense.

Choose your forum carefully

While you can strike up a friendship in many places online, and this guidance applies to all of them, choosing a well-run, reputable online dating service will provide some additional safety. For example, you should look for a site that will protect your anonymity until you choose to reveal personal information. Also look for a site that will enforce its policies against inappropriate use.

Protect your privacy

You are in control of what happens. Don't let anyone pressure you into giving away more information than you want to.

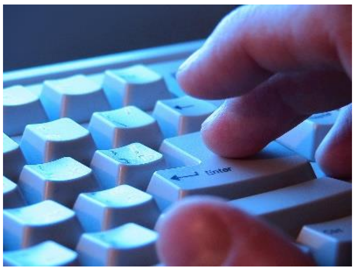
- You wouldn't give your phone number to every stranger on the street. Similarly, don't post personal information, such as phone numbers, in public places on the internet
- Wait until you feel comfortable with an individual before telling them things like your phone number, place of work or address
- A well-run dating site will offer the ability to email prospective dates using an email service that conceals both parties' true email addresses
- As a second line of defense for your privacy, set up a separate email account thatt doesn't use your real name. Similarly, you can use an internet telephone service, such as Skype, to call someone instead of using your own phone
- Pick a user name that doesn't include any personal information. For example, "joe_glasgow" or "jane_liverpool" would be bad choices

Always remember:

- Legitimate businesses such as your bank should not ask you to send passwords, login names or other personal information through e-mail
- Phishing links may contain all or part of a real company's name and are usually masked, meaning that the link you see does not take you to that address but somewhere different, usually an illegitimate web site
- Web addresses that resemble the name of a well-known company may be slightly altered by adding, omitting, or transposing letters. For

  example, the address "www.microsoft.com" could appear instead as

  www.micosoft.com



Useful information and contacts

Childnet International - http://www.childnet-int.org/

Wide range of resources, in particular 'Know IT All for Parents and Carers'.

CEOP - www.thinkuknow.co.uk

Child Exploitation and Online Protection Centre site with education resources from KS1 and Foundation.

Get Safe Online - http://www.getsafeonline.org/

source of unbiased, factual and easy-to-understand information on online safety

Kidsmart - http://www.kidsmart.org.uk/

Resources and information about e-safety