Social Media Guidelines

These guidelines will be shared with all staff, volunteers and Trustees for KEY. They should be read in conjunction with KEY's Safeguarding and Social Media Policies.

1. We have chosen to use a Facebook page for raising the profile of KEY and advertising activities and events. This is a closed page with the facility to comment and chat turned off. KEY staff have control of the page and are the only people able to post items.
2. It is likely that KEY staff, volunteers and trustees will have personal social networking accounts/profiles. We advise that you do not consciously allow any of the young people, linked to KEY, to have access to your accounts/profiles and that you do not engage with any of the young people, linked to KEY, through social media. This is to safeguard yourselves and to ensure that the young people do not have access to private information about you which may compromise either you and/or the organisation
3. We understand that the Kent Estuary area is a small community and that personal relationships form when working and living in such communities. However, we do expect a separation of your personal relationships when working as a worker/volunteer within the project and that you will maintain confidentiality and not bring 'outside baggage' into the project. We expect you to work with individuals fairly, without judgement and always remember you are acting as a role model to the young people for the organisation.
   We therefore strongly recommend that you do not post any information about yourself on the internet which may be embarrassing, inappropriate, compromising or offensive, no matter who can view it. This includes your use of language, your posting of photographs and your recounting of stories and experiences.
4. In the exceptional case that a young person you have met through KEY contacts you personally via social networking sites or any other media then we recommend that:
   - You keep a copy of any correspondence sent and received
   - You inform your line manager or youth lead
   - You take every reasonable step to ensure that the young person does not form an inappropriate attachment to you. Such an attachment may be misconstrued by third parties and may give the young person false expectations and impressions
5. We recommend that where possible you do not allow young people to have either your personal phone numbers or home address, or any other information about you which may lead to significant contacts away from work which may later be hard to verify or recount i.e. conversations which cannot be recorded and reviewed.
6. You should remember that there is a legal age limit of 13 years old for access to sites such as Facebook.

7. When promoting the work of KEY in any media, all pictures or images MUST have had permission to be used. No names or personal details should be attached to the images in order to safeguard the young people, staff and volunteers.
8. If you become aware, via an internet site, of a situation in which a young person is potentially in danger, you must report it straight away either to your supervisor, your safeguarding officer, the police, the CEOP www.ceop.police.uk or another relevant authority.

Listed below are some of the laws that exist to offer protection:

The Human Rights Act 1998

This Act gives a 'right to respect for private and family life'. People should therefore have a reasonable expectation of privacy and all courts must now interpret existing legislation in relation to the Human Rights Act. No one should include any inappropriate personal information about another person through any social networking/media or email or divulged such information in any other way to any external third party.

The Regulation of investigatory Powers Act 2000

This Act covers the extent to which organisations can monitor or record communications at the point at which they enter or are being sent within the employer's telecommunications system and applies to public and private communication networks. It gives the sender or recipient of a communication the right of action for damages against the employer for the unlawful interception of communications. There are two areas where monitoring is not unlawful. These are:

- Where the employer reasonably believes that the sender and intended recipient have consented to the interception, and
- Without consent, the employer may monitor in certain circumstances, for example, to prevent crime, protect their business or to comply with financial regulations.

Organisations can reserve the right to monitor all internal and external communications in appropriate ways that protect its reputation and integrity.

General Data Protection Regulations 2018 (Replaces The Data Protection Act 1988)

The government's Information Commissioner is responsible for enforcement of the Data Protection Act and has published a code of practice to help employers comply with the provisions of the Act. Organisations should be mindful of information which relates to them, their staff, and those for whom it holds information - in the processing of individual data including the basis for monitoring and retention of email communications and other paperwork containing personnel records.

The Public Interest Disclosure Act (1999)

This Act encourages people to 'blow the whistle' about malpractice in the workplace and is designed to ensure that organisations respond by acting on the message rather than against the messenger. The Act applies to employees and volunteers blowing the whistle about crime, civil offences (including negligence etc), miscarriage of justice, danger to health and safety or the environment and the cover-up of any of these. It applies whether the information is confidential or not and extends to malpractice occurring in the UK and any other country. In addition to employees, it covers trainees, agency staff, contractors and home workers. A disclosure in good faith to a manager should ensure that the whistleblower will be protected if they have reasonable suspicion that the malpractice has occurred, is occurring or is likely to occur.