TOPCATS

OPPORTUNITIES & ACTIVITIES FOR
ADDITIONAL NEEDS IN THE SUFFOLK AREA

TC10 – Computer, Email and Internet Usage Policy and Procedure (e-Safety)

Purpose

As part of the Every Child Matters agenda set out by the government, the Education Act 2002 and the Children's Act 2004, it is the duty of all organisations to ensure that children and young people are protected from potential harm both within and beyond the organisation environment. Therefore, the involvement of children, young people and parent/carers is also vital to the successful use of online technologies.

- To safeguard TOPCATS's IT equipment, communication equipment, and information.

Scope

- All computer equipment, Internet access, and Internet communications.
- All employees, volunteers and Young People.

Aims

This policy aims to explain how parents/carers, children or Young People can be a part of these safeguarding procedures. It also details how children and Young People are educated to be safe and responsible users capable of making good judgements about what they see, find and use. The term 'e-Safety' is used to encompass the safe use of all technologies in order to protect children, Young People and adults from potential and known risks.

- To emphasise the need to educate staff, children and Young People about the pros and cons of using new technologies both within and outside the organisation.

- To provide safeguards and agreement for acceptable use to guide all users, whether staff or children and Young People, in their online experiences.
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the boundaries of the organisation.
- To develop links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of the benefits and potential issues related to technologies.

Policy

- TOPCATS will restrict access and use of its computer equipment, emails and Internet access in order to reduce the risk of contamination of the information stored.
- Where appropriate, duly authorised staff are encouraged to make use of Internet access as part of their official and professional activities.
- Employees of TOPCATS will have regard to their responsibility not to bring their employer into disrepute through the use of IT equipment, email or other internet based communication.
- Employees of TOPCATS will have regard to their responsibility not to breach confidentiality of their employer's information or that of their employer's clients or other employees through the use of IT equipment, email or other internet based communication.
- Attention must be paid to ensuring that published information has relevance to normal professional activities before material is released in the name of TOPCATS.
- Where personal views are expressed a disclaimer stating that this is the case should be clearly added to all correspondence.
- The intellectual property rights and copyrights of the employer or any other person or organisation must not be compromised when publishing on the Internet.
- The availability and variety of information on the Internet has meant that it can be used to obtain material reasonably considered to be offensive. The use of the internet to access and/or distribute any kind of offensive material, or matters not related to the employer's business, will render the individual liable to disciplinary action which could lead to dismissal.

Procedure

Use of computer equipment

- The downloading of active software, in whatever format, on to the organisations IT equipment must be authorised by the Manager, who in turn must check that the software is safe. Be particularly wary of websites delivering active components.
- The introduction of new software must first of all be checked and authorised by the Manager before general use will be permitted.
- Only authorised staff should have access to the organisation's computer equipment.

- Only authorised software may be used on any of the organisation's computer equipment.
- Only software that is used for business applications may be used.

- No software that is used for business applications may be used.
- No software may be brought into or taken from the organisation without prior authorisation.
- Unauthorised access to the computer facility will result in disciplinary action, which may lead to dismissal.
- Unauthorised copying of data and/or removal of computer equipment/software will result in disciplinary action; such actions could lead to dismissal.

Use of email

- In common with all communications from a limited company, any email from an organisation which is a limited company must contain the following information:
  - The full name of the company;
  - The registered number of the company;
  - The place of registration of the company;
  - The registered office address of the company.
- Unauthorised or inappropriate use of the E-Mail system may result in disciplinary action, which could include summary dismissal.
- The E-Mail system is available for communication and matters directly concerned with the legitimate business of The Agency. Employees using the E-Mail system should give particular attention to the following points:
  - It is an offence, in some situations liable to an unlimited fine, for anyone to send unsolicited commercial emails (spam) and text messages to individuals (including unincorporated bodies) who have not explicitly agreed to this in advance. Unless there is already an existing customer relationship with the individual, emails, text messages and other electronic marketing messages can only be sent to individuals with their explicit prior consent – i.e. an opt-in, rather than the currently widely used "tick here if you don't want to hear from us" opt-out.
  - All emails must comply with the organisation's communication standards.
  - E-Mail messages and copies should only be sent to those for whom they are particularly relevant.
- E-Mail should not be used as a substitute for face-to-face communication or telephone contact. Flame mails (i.e. E-Mails that are abusive) must not be sent. Hasty messages sent without proper consideration can cause upset, concern. Break

confidence, compromise privacy, constitute a criminal or civil offence, or cause misunderstanding.

- If E-Mail is confidential the user must ensure that the necessary steps are taken to protect confidentiality. TOPCATS will be liable for infringing copyright or any defamatory information that is circulated wither within TOPCATS or to external users of the system.
- Offers or contracts transmitted by E-Mail are as legally binding on TOPCATS as those sent on paper.
- TOPCATS will not tolerate the use of the E-Mail system for unofficial or inappropriate purposes, including:
    - Any messages that could constitute bullying, harassment or other detriment;
    - Accessing or transmitting pornography.
    - Personal use (e.g. social invitations, personal messages, jokes, cartoons, chain letters or other private matters);
    - Online gambling
    - Social networking;
    - Transmitting copyright information and/or any software available to the user;
    - Posting confidential information about other employees, the employer or its customers or suppliers.

Use of web browsers

- Web browsing is made available for research purposes only, and use of the organisation's IT equipment for browsing for personal purposes is not permitted.
- Only web sites known to be reputable may be accessed using the organisation's IT equipment, in order to protect the equipment from malicious intrusion. The user must take personal responsibility for determining if the site to be accessed is safe, and failure to take reasonable precautions may result in disciplinary action.

Roles and Responsibilities

Name of organisation: TOPCATS

e-Safety: Safeguarding Lead and Deputy Responsibilities
The responsibility of managing e-Safety can be demanding and challenging, and must therefore be appointed at managerial/committee level to personnel who are available when we are operational. (This will normally be the same person who will lead on child protection, unless your organisation has a lot of technology based activities, in which case you may wish to include an IT expert from your organisation who will liaise with the lead person for child protection).

Our lead is:

Name: Anne-Marie Battrick

Contact details: 01502 531897 / Annemarie@topcats.org.uk

TOPCATS e-SAFETY CODE OF CONDUCT:

TOPCATS expects everyone in the organisation to agree and sign up to our code of conduct:

I will:

1. Use the internet and other forms of communication in a sensible and polite way.
2. Only access websites, send messages or access and use other resources that will not hurt or upset anybody.
3. Seek permission if I want to use personal information or take photographs of other people.
4. Report any concerns to the lead or Floor Supervisor for e-safety immediately.
5. Be clear that I cannot maintain confidentiality if there is a concern about the welfare of a child or Young Person.

WHAT ARE THE RISKS?

There are many potential risks for children and Young People including:

- Accessing age inappropriate or illegal websites.
- Receiving unwanted or upsetting text or e-mail messages or images.
- Being “groomed” by an adult with a view to meeting the child or Young Person for their own illegal purposes including sex, drugs, or crime.
- Viewing or receiving socially unacceptable material such as inciting hatred or violence.
- Sending bullying messages or posting malicious details about others.
- Ignoring copyright law by downloading music, video or even homework cheat material.

WHAT ELSE MIGHT BE OF CONCERN?

A child or Young Person who:

- Is becoming secretive about where they are going to or who they are meeting.
- Will not let you see what they are accessing on-line.
- Using a webcam in a closed area, away from other people.
- Accessing the web or using a mobile or PDA (Personal Data Assistant) for long periods and at all hours.

- Clears the computer history every time they use it.

- Receives unexpected money or gifts from people you don't know.

An adult who:

- Befriends a child/ren or Young Person/People on the internet or by text messaging.
- Has links to children or Young People on their Facebook or other social network site; especially if they work in a position of trust such as a sports coach or youth worker.
- Is secretive about what they are doing and who they are meeting.

WHAT DO I DO IF I AM CONCERNED?

- If you have any concerns speak to the Service Manager (Anne-Marie Battrick) for e-Safety immediately.

CONTACTS FOR REFERRING

If the concern is about:

- A child being in imminent danger, ALWAYS DIAL 999 FOR THE POLICE.
- The welfare of a child, ring the local children's social care services- Customer First: 0808 800 4005, out of hours service: 01473 299669 or access what to do by going to www.suffolkscb.org.uk
  A known person's sexual behaviour or intentions ring the local children's social care services: **Adrian House, Alexander Road, Lowestoft, NR32 1PL, 01502 674773**
- A person who has a "duty of care" in the organisation, ring the local children's social care services. The LADO (Lead Authority Designated Officer) will oversee and advise upon any following procedures.
- An unknown person's sexual behaviour or intentions, report at **www.ceop.gov.uk (Child Exploitation and Online Protection Centre).**
- Harmful content, including child sexual abuse images or incitement to racial hatred content contact **www.iwf.org.uk**

REMEMBER:

1. **DO NOT DELAY.**
2. **DO NOT INVESTIGATE.**
3. **ISOLATE ANY EQUIPMENT AND PREVENT FURTHER USE OF AN ONLINE ACCOUNT.**
4. **MAKE CAREFUL RECORDING OF ANYTHING YOU OBSERVE OR ARE TOLD.**
5. **SEEK ADVICE FROM THE LEAD OR DEPUTY PERSON FOR e-SAFETY.**
6. **REFER IMMEDIATELY.**

MINIMISING THE RISKS:

We will:

- Talk to children and Young People about what they are accessing on line.
- Keep the computer/s in a general space where we can monitor what is going on.
- Explain the risks of giving out personal details online.
- Talk about how people can be anyone they want to be online: by using misleading emails, photographs of other people, telling lies about their age, school, hobbies.
- Encourage children and Young People to think carefully about which photographs or videos they use on line this material can be used and tampered with by other people, or they may not be appropriate.
- Advise children and Young People to only text, chat or webcam to people they know for real.
- Talk about how to identify SPAM/SPIM messages or junk mail and how to delete them. This also applies to messages from people they do not know, or opening attachments.
- Discuss how people hide their identities online and the importance of never meeting new online "friends" for real.
- Make sure children and Young People understand they can talk to us or their parents and/or carers about anything that makes them feel uncomfortable.
- Look on the internet together for information about how to deal with, or report, problems.
- Talk about how, when information or images get onto the net, they can never be erased or retrieved.

Resources

TOPCATS:

- *Can use the Childnet International 'KnowITAll for Parents' CD/online materials (http://www.childnet-int.org.uk/kia/parents/cd/) to deliver key messages and raise awareness for parents/carers and the community.*
- *Ensure that skills around internet use are offered as part of the follow-up training for parents/carers so they know how to use the tools their children and young people are using.*
- *Endeavour to provide access to the internet for parents/carers so that appropriate advice and information can be accessed where there may be no internet at home, subject to arrangement.*