

Extratime

Staff, Children and Young People's e-Safety Policy

Introduction

Extratime recognises the Internet and other digital technologies provide a vast opportunity for children and young people to learn, socialise and play. More than any other mode of technology, the Internet and digital technologies allow all those involved in working with children and young people to promote creativity, stimulate awareness and enhance learning and communication skills.

However the need to keep them safe from the inappropriate material and abuse of the Internet, digital and mobile technologies is paramount. This policy is therefore aimed at developing an approach to E-safety, to protect children and young people who access the Internet and digital technologies outside the school environment whilst in extratime's care whether using our own facilities or personal mobile phones etc.

Extratime recognises, as part of this policy, that there should be equitable opportunities for all children and young people using ICT technology and that for disabled children and young people it can offer increased opportunities for communication in particular.

Extratime is committed to ensuring that **all** children and young people using it's services will be able to use existing, as well as up and coming technologies safely. We are also committed to ensuring that all those who work with children and young people; as well as their parents, are educated as to the dangers that exist so that they can take an active part in safeguarding children and young people.

For the purposes of this document, Internet usage means any connection to the Internet via web browsing, external email, news groups or messaging services, mobile technologies e.g. mobile phone, including Bluetooth applications, PDA's etc.

Scope

The Policy applies to all after school clubs, playschemes and youth schemes which extratime provides. The policy is also recommended as good practice to all extratime's partner organisations as the minimum level of provision of E-safety for children and young people.

Extratime will seek to ensure that across the service the following elements will be in place as part of its safeguarding responsibilities to children and young people:

- a list of authorised person(s) dealing with child protection issues and E-safety at each setting;
- adequate training for staff and volunteers;
- adequate supervision of children and young people when using the Internet and digital technologies;
- talking and showing children and young people about how to use the Internet and digital technologies safely;
- a reporting procedure for abuse and misuse by children, young people and adults.

Policies and Practices

Use of Internet facilities, mobile and digital technologies

This policy aims to ensure that the Internet, mobile and digital technologies are used effectively for their intended educational and recreational purposes, without infringing legal requirements or creating unnecessary risk.

extratime expects that all settings ensure that children, young people, staff and volunteers use the Internet, mobile and digital technologies responsibly and strictly according to the conditions below and these expectations are also applicable to any service that provides external services on behalf of extratime:

Users shall not:

- Visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
 - Indecent images of children
 - Promoting discrimination of any kind
 - Promoting racial or religious hatred
 - Promoting illegal acts
 - Any other information which may be offensive to peers or colleagues e.g. abusive images; promotion of violence; gambling; criminally racist or religious hatred material.

Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will be reported to the designated office for child protection within the setting and the Police:

- Indecent images inclusive of abuse (images of children whether they are digital or cartoons, apparently under 16 years old, involved in sexual activity or posed to be sexually provocative)
- Adult material that potentially breaches the Obscene Publications Act in the UK
- Criminally racist or anti-religious material
- Violence and bomb making
 - Illegal taking or promotion of drugs
 - Software piracy
 - Other criminal activity

In addition, users may not:

- Use the extratime facilities (connectivity and services) or an equivalent for running a private business;
- Enter into any personal transaction that involves extratime or partner services in any way;
- Visit sites that might be defamatory or incur liability on the part of extratime or a partner service or adversely impact on the image of extratime
- Upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties outside of extratime, or to extratime itself;
- Reveal or publicise confidential or proprietary information, which includes but is not limited to:
 - financial information, personal information, databases and the information contained therein, computer/network access codes, and business relationships;
- Intentionally interfere with the normal operation of the Internet connection, including the propagation of computer viruses and sustained high volume network traffic

(sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion) that substantially hinders others in their use of the Internet;

- Use the Internet for soliciting, representing personal opinions or revealing confidential information or in any other way that could reasonably be considered inappropriate.
- The transmission of unsolicited commercial or advertising material either to other user organisations, or to organisations connected to other networks, save where the material is embedded within, or is otherwise part of, a service to which the member of the user organisation has chosen to subscribe.
- Deliberate unauthorised access to facilities or services accessible via extratime computers
- Deliberate activities with any of the following characteristics:
 - wasting staff effort or networked resources, including time on end systems accessible via the extratime network and the effort of staff involved in support of those systems;
 - corrupting or destroying other users' data;
 - violating the privacy of other users;
 - disrupting the work of other users;
 - using the extratime network in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment);
 - continuing to use an item of networking software or hardware after extratime has requested that use cease because it is causing disruption to the correct functioning of extratime systems;
 - other misuse of the extratime network, such as introduction of viruses.
- Use mobile technologies 3G or mobile internet services in any way to intimidate, threaten or cause harm to others. Moreover, mobile technologies should not be used to access inappropriate materials or encourage activities that are dangerous or illegal.
- Where Fastnet (provider of extratime internet connectivity) become aware of an illegal act or an attempted illegal act, they will have to comply with the law as it applies, and will take action directed by the Police if a Regulation of Investigatory Powers Act (RIPA) Notice is issued.

Reporting abuse

There will be occasions when either a child or young person or an adult within a setting, receives an abusive email or accidentally accesses a website that contains abusive material. When such a situation occurs, the expectation is that the child, young person or adult should report the incident immediately.

extratime also recognises that there will be occasions where children and young people will be the victims of inappropriate behaviour that could lead to possible or actual significant harm, in such circumstances extratime safeguarding procedures should be followed. The expected response will be to take the reporting of such incidents seriously and where judged necessary, the Designated Senior Person for Child Protection within the setting refer details of the incident to the lead agencies involved in safeguarding children, namely Children's Social Care and the Police.

All extratime settings, as part of their safeguarding duties and responsibilities will, in accordance with the charities policies, assist and provide information and advice in support of child protection enquiries and criminal investigations.

Education and Training

extratime is committed to harnessing the power of the Internet and other digital technologies to enhance the activities the children and young people choose to be engaged in. The charity is also dedicated to ensuring that it helps the children and young people who access it's services to have the skills of critical awareness, digital literacy and good online citizenship to enable them to use the Internet and other digital technologies safely.

As part of achieving the above, the service will seek to ensure that E-safety awareness is integrated in to appropriate activities for children, young people; and also training will be made available to those adults that supervise them, manage and/or support the facilities that are being used.

Infrastructure and Technology

Partnership working with extratime

extratime recognises that as part of its safeguarding responsibilities there is a need to work in partnership. Two of our major partners are Sussex Central YMCA and The Crew Club who provide the venues and some staff for the youth schemes. Extratime will share this policy with our partners to ensure consistency across venues with regards to E Safety.

Monitoring

Extratime will ensure that all settings adhere to the policy.

The first responsibility for monitoring the use of the Internet and digital technologies lies with the setting supervisors. These should include both physical observation (supervision of use by an adult, where appropriate) and local technical monitoring.

Extratime does monitor and audit the use of the Internet and electronic mail to see whether users are complying with the policy. Any potential misuse identified by extratime will be reported to the connected establishment and/or relevant organisation.

Sanctions

extratime has been careful to develop in conjunction with its partners, policies and procedures to support the innocent in the event of a policy breach.

Where there is inappropriate or illegal use of the Internet and digital technologies, the following sanctions will be applied:

Child / Young Person

- The child/young person will be disciplined according to extratime's behaviour management policy, which will ultimately include the use of Internet and email being withdrawn.
- Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal Internet use or child protection concerns.

Adult (Staff and Volunteers)

- The adult may be subject to extratime's disciplinary procedures, if it is deemed he/she has breached the policy.
- Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal Internet use or child protection concerns.

If inappropriate material is accessed, users are required to immediately report this to extratime management so this can be taken into account in monitoring.

Document version and review control

DATE WRITTEN/REVIEWED	Written by:	Approved by Executive Committee:
September 2011	Becky Jenner	October 2011
Reviewed Sep 15	Sam Price	
Document to be reviewed in September 2019		