

## **Leicestershire Children and Young People's Service E-Safety Policy**

### **1. Introduction**

- 1.1 Leicestershire Children and Young People's Service (CYPS) recognises the Internet and other digital technologies provide a vast opportunity for children and young people to learn. More than any other mode of technology, the Internet and digital technologies allow all those involved in the education of children and young people to promote creativity, stimulate awareness and enhance learning.
- 1.2 Hand in hand with the Department's desire for its children and young people to access every opportunity for learning, there will be the need to keep them safe from the perils of the Internet, digital and mobile technologies. With this in mind, the Department has created a policy that is aimed at developing not only a whole school approach to E-safety, but also an approach that seeks to protect children and young people who access the Internet and digital technologies outside the school environment (e.g. foster children, children in residential units, children attending pupil referral units and extended school facilities).
- 1.3 This policy also recognises that there are children and young people who are living in the Leicestershire area away from their immediate homes and families. We have, under Section 11 Children Act 2004, a responsibility to ensure that our normal functions as a Department are discharged in such a way that we have regard to safeguarding and promoting the welfare of these children.
- 1.4 Leicestershire Children and Young People's Service, as part of this policy, holds steadfastly to the ethos that there should be an equitable learning experience for all pupils using ICT technology. We recognise that ICT can allow disabled children and young people increased access to the curriculum and other aspects related to learning.
- 1.5 Leicestershire Children and Young People's Service is committed to ensuring that all children and young people within its remit of care 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.

### **2. Scope of Policy**

#### **2.1 The Policy applies to:**

- all types of maintained educational establishments;
- all educational central services, in particular those that work directly with children and young people;
- all children's social care environments where a direct service is provided to children, young people and their families

The policy is also recommended as good practice to all Leicestershire County Council Children and Young People's Service partner organisations as the minimum level of provision of E-safety for children and young people.

2.2 The Children and Young People's Service will seek to ensure that across the Department 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 per educational establishment, central service department and extended school facility;
- a range of policies including authorised usage policies that are frequently reviewed and updated;
- information to parents that highlights safe practice when using the Internet and other digital technologies in school and at home;
- adequate training for staff and volunteers;
- adequate supervision of children and young people when using the Internet and digital technologies;
- education of 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.

### 3. Policies and Practices

#### 3.1 Use of Internet facilities, mobile and digital technologies

3.1.1 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.

3.1.2 Leicestershire Children and Young People's Service expects the range of educational establishments, residential units, CYPS central services, alternative arrangements for Children in Care e.g. foster care and extended school facilities, to ensure that children, young people, staff and volunteers use the Internet, mobile and digital technologies responsibly and strictly according to the conditions below. These expectations are also applicable to any agency that provides external services on behalf of the Department.

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.

- 3.1.3 The Department recognises that in certain planned curricular activities, access to otherwise considered inappropriate sites may be beneficial for educational use. In such circumstances, such access should be pre-planned and recorded and also permission is given by senior leaders, so that the action can be justified, if queries are raised later.
- 3.1.4 3.1.4 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
- 3.1.5 In addition, users may not:
- Use the embc facilities (connectivity and services) or an equivalent
  - for running a private business;
  - Enter into any personal transaction that involves embc or member Local Authorities in any way;
  - Visit sites that might be defamatory or incur liability on the part of embc or member Local Authorities or adversely impact on the image of embc;
  - Upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties outside of embc, or to embc 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 embc
- Deliberate activities with any of the following characteristics:
  - wasting staff effort or networked resources, including time on end systems accessible via the embc 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 embc 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 embc has requested that use cease because it is causing disruption to the correct functioning of embc;
  - other misuse of the embc 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.

3.1.6 Where Synextrix (provider of internet connectivity and associated services to schools) and/or embc 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.

### 3.2 Reporting abuse

3.2.1 There will be occasions when either a pupil or an adult within an educational establishment, residential unit, CYPS central service, alternative arrangement for Children in Care e.g. foster care and extended school facilities, 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.

3.2.2 Leicestershire Children and Young People's Service 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 LSCB2 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.

3.2.3 All educational and children's social care settings, as part of their safeguarding duties and responsibilities will, in accordance with LSCB Procedures<sup>3</sup>, assist and provide information and advice in support of child protection enquiries and criminal investigations.

## 4. Education and Training

4.1 Leicestershire Children and Young People's Service is committed to harnessing the power of the Internet and other digital technologies to transform the learning of children and young people. We are also dedicated to ensuring that children and young people in Leicestershire have the skills of critical awareness, digital literacy and good online citizenship to enable them to use the Internet and other digital technologies safely.

4.2 As part of achieving the above, the service will seek to ensure that E-safety training is made available to children, young people; and also to those adults that supervise them, manage and/or support the facilities that are being used e.g. network managers, technicians, administrators as well as third party service providers.

## 5. Infrastructure and Technology

### 5.1 Partnership working with embc

5.1.1 Leicestershire Children and Young People's Service recognises that as part of its safeguarding responsibilities there is a need to work in partnership. One of our major partners is embc who provide the network, services and facilities that support the communication requirements of the East Midlands learning community.

5.1.2 Where the range of educational establishments, residential units, CYPS central services, alternative arrangements for Children in Care e.g. foster care or extended school facilities, are using embc services, they are to comply with the conditions of acceptable and unacceptable use of embc services as laid out in embc's Safety and Security Policy.

5.1.3 Where educational establishments, residential units, central CYPS central services, alternative arrangements for Children in Care e.g. foster care or extended school facilities, are not using embc, they should provide a network that includes the following:

- protection of the user from inappropriate content and ensure data security and integrity;
- use a content and email filtering system managed by a provider that works according to the specifications as laid out by BECTA4 ;
- provide safe and secure Internet access for every user of the service;

## 6. Standards and Inspection

The Children and Young People's Service will ensure that the range of educational establishments, residential units, CYPS central services, alternative arrangements for Children in Care e.g. foster care, and extended school facilities adhere to the elements as set in Section 2.2. of this policy.

### 6.1 Monitoring

6.1.1 The first responsibility for monitoring the use of the Internet and digital technologies lies with the range of educational establishments, residential units CYPS central services, alternative arrangements for Children in Care e.g. foster care and extended school facilities.

These should include both physical observation (supervision of use by an adult, where appropriate) and local technical monitoring.

6.1.2 embc 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 embc will be reported to the connected establishment and/or relevant organisation.

## 6.2 Sanctions

6.2.1 The Children and Young People's Service has been careful to develop in conjunction with its partners, policies and procedures to support the innocent in the event of a policy breach and enable establishments to manage such situations with confidence.

6.2.2 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 the behaviour policy of the establishment, 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 the disciplinary process of their home organisation, 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.

6.2.3 If inappropriate material is accessed, users are required to immediately report this to their organisation and embc (via the relevant service desk) so this can be taken into account in monitoring.