E-SAFETY POLICY

E-SAFETY POLICY

1. Introduction

Thomas Estley Community College (TECC) recognises the Internet and other digital technologies provide a vast opportunity for children and young people to learn. 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.

As part of our commitment to learning and achievement we at Thomas Estley want to ensure that the Internet and other digital technologies are used to:

- Raise educational standards and promote pupil achievement
- Develop the curriculum and make learning exciting and purposeful
- Enable pupils to gain access to a wide span of knowledge in a way that ensures their safety and security
- Enhance and enrich their lives and understanding

To enable this to happened we have taken a whole school approach to E-safety as promoted by British Education Communication Technology Agency (BECTA), which includes the development of policies and practices, the education and training of staff and pupils and the effective use of the School's ICT infrastructure and technologies.

The College, 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 pupils increased access to the curriculum and other aspects related to learning.

The College is committed to ensuring that **all** its pupils 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 risks that exist so that they can take an active part in safeguarding children.

The nominated senior person for the implementation of the School's e-Safety policy is **Chris Freeman, Vice Principal and Designated Senior Person for Child Protection.**

2. Scope of Policy

The policy applies to:

- all pupils
- all teaching and support staff (including peripatetic), school governors and volunteers
- all aspects of the School's facilities where they are used by voluntary, statutory or community organisations

The College will ensure that the following elements are in place as part of its safeguarding responsibilities to pupils:

- a range of policies including acceptable use policies that are frequently reviewed and updated
- information to parents that highlights safe practice for children and young people when using the Internet and other digital technologies
- adequate training for staff and volunteers
- adequate supervision of pupils when using the Internet and digital technologies
- education that is aimed at ensuring safe use of Internet and digital technologies
- a reporting procedure for abuse and misuse

3. Infrastructure and Technology

3.1 Partnership Working

3.1.1 The College recognises that as part of its safeguarding responsibilities there is a need to work in partnership. One of our major partners is the East Midlands Public Service Network (emPSN) who provides the network, services and facilities that support the communication requirements of the East Midlands learning community. As part of our commitment to partnership working, we fully support and will continue to work with emPSN to ensure that pupil and staff usage of the Internet and digital technologies is safe.

3.1.2 The College will, as part of its wider safeguarding responsibilities, seek to ensure that voluntary, statutory and community organisation take an approach to their activities that see the welfare of the child as paramount. To this end, we expect any organisation using the school's ICT or digital technologies to have appropriate policies and procedures that are aimed at safeguarding children and young people and reporting concerns.

4. Policies and Procedures

We at Thomas Estley understand that effective policies and procedures are the backbone to developing a whole-school approach to E-safety. The policies that exist within the College are aimed at providing a balance between exploring the educational potential of new technologies safeguarding pupils.

4.1 Use of Internet facilities, mobile and digital technologies

4.1.1 The College will seek to ensure that Internet, mobile and digital technologies are used effectively for their intended educational purpose, without infringing legal requirements or creating unnecessary risk.

4.1.2 The College expects all staff and pupils to use the Internet, mobile and digital technologies responsibly and strictly according to the conditions below:[1] These expectations are also applicable to any voluntary, statutory and community

[1] 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.

organisations that makes use of the school's ICT facilities and digital technologies.

4.1.3 Where third party users require access to the College wifi, eg Teaching school course participants/ official meetings; then users will be provided with temporary log ins and informed that their activity on line will be subject to College filtering.

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

4.1.4 The School recognises that in certain planned curricular activities, access to otherwise deem inappropriate sites may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned and recorded and also permission is given by senior leaders, so that the action can be justified, if queries are raised later.

4.1.5 Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will be reported to the Police:

- Images of child 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
- Extremism

4.1.6 **In addition, users may not:**

- Use the emPSN or an equivalent broadband provider's facilities for running a private business;

- Enter into any personal transaction that involves emPSN or Thomas Estley Community College or its Trustees in any way, unless under a personal designated delegation of authority to do so;
- Visit sites that might be defamatory or incur liability on the part of emPSN or member Local Authorities or adversely impact on the image of emPSN;
- Upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties outside of emPSN, or to emPSN 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.
- Transmit 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.
- Assist with unauthorised access to facilities or services accessible via emPSN
- Undertake activities with any of the following characteristics:
  - Wasting staff effort or networked resources, including time on end systems accessible via the emPSN 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 emPSN 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 emPSN has requested that use cease because it is causing disruption to the correct functioning of emPSN;
  - Other misuse of the emPSN network, such as introduction of viruses.
- Use any mobile or digital 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.

4.1.7 Where KCOM (provider of Internet connectivity and associated services to schools) and/or emPSN 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.

4.2 Reporting Abuse

4.2.1 There will be occasions when either a pupil or an adult within the school receives an abusive email or accidentally accesses a website that contains abusive material. When such a situation occurs, the expectation of the school is that the pupil or adult should be report the incident **immediately**.

4.2.2 The School also recognises that there will be occasions where pupils will be the victims of inappropriate behaviour that could lead to possible or actual significant harm, in such circumstances LSCB[2] Procedures should be followed. The response of the School will be to take the reporting of such incidents seriously and where judged necessary, the Designated Senior Lead for Child Protection within the School will refer details of an incident to the lead agencies involved in safeguarding children, namely Children's Social Care and the Police.

The School, as part of its safeguarding duty and responsibilities will, in accordance with LSCB Procedures[3] assist and provide information and advice in support of child protection enquiries and criminal investigations.

5. Education and Training

5.1 The College recognises that the Internet and other digital technologies can transform learning; help to improve outcomes for children and young people; promote creativity; all of which add up to a more exciting and challenging classroom experience.

5.2 As part of achieving this, we want to create within the College an accessible system, with information and services online, which support personalised learning and choice. However, we realise that it will be necessary for our pupils 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.

5.3 To this end the College will:-

- Enable all pupils to exercise the skills of critical awareness, digital literacy and good online citizenship as part of the school curriculum.
- Educate school staff so that they are equipped to support pupils in gaining positive experiences when online and can help pupils develop strategies if they encounter a problem.

[2] Chapter 9 of the LSCB Procedures
[3] Chapters 5, 9, 12 and 13 of the LSCB Procedures

- Support parents in gaining an appreciation of Internet safety for their children and provide them with relevant information on the policies and procedures that govern the use of Internet and other digital technologies within the school.

6. Standards and Inspection

Thomas Estley recognises the need to have regular inspections of policies and procedures in order to ensure that its practices are effective and that the risks to pupils are minimised.

6.1 Monitoring

6.1.1 All pupils, staff and other users of the College's ICT equipment are required to read, sign and agree to the ICT Acceptable Use Policy (AUP) (Appendix A&B). Records of returned pupils AUP agreements are logged onto SIMs via Reception. Reception retains AUP's as appropriate for affiliated/extended services groups. The Personnel Assistant retains the Staff Acceptable Use Policy on personnel files.

6.1.2 Monitoring the safe use of the Internet and other digital technologies goes beyond the personal use of the Internet and electronic mail a pupil or member of staff may have. The College recognises that in order to develop an effective whole school E-safety approach there is a need to monitor patterns and trends of use inside school and outside school (Education and Inspections Act 2006, Section 89(5)).
To this end, contraventions of this policy which become apparent from web filtering reports which are logged by the Network Manager (or teacher where network filtering is undertaken) and deal with in line with the College's Positive Behaviour for Learning Policy. The log is shared with the E-Safety nominated Safeguarding Office, Christine Freeman at least termly who reviews pattern of incidents with Team Leaders which may lead to further appropriate interventions.

6.1.3 With regard to monitoring trends, within the school and individual use by school staff and pupils, the College may audit the use of the Internet and electronic mail in order to ensure compliance with this policy. The monitoring practices of the school are influenced by a range of national guidance documents and will include the monitoring of content and resources.

6.1.4 Another aspect of monitoring, which our school will employ, is the use of mobile technologies by pupils, particularly where these technologies may be used to cause harm to others, e.g. bullying (see anti-bullying policy for further information). We will also ensure that school staff understand the need to monitor our pupils, and where necessary, support individual pupils where they have been deliberately or inadvertently been subject to harm.

6.2 Web Filtering

6.2.1 We utilise an internal webfilter that can block ,track and record personal web activity. Reports are emailed directly to the Network Manager and Team Leaders and the E—safety officer on a daily basis for Web Filter Reports there are other reports that the Network Manager will look at if required in the event of a breach or suspicious report.

6.2.2 Web Filter Reports cover:

- Search Queries
- Suspicious Search Queries
- Traffic By Category
- Traffic By Domain
- Traffic By External IP
- Traffic By Internal IP
- Traffic By Internal IP & External IP
- Traffic By Internal IP & External IP & Protocol
- Traffic By Internal IP & Protocol
- Traffic By Protocol
- Traffic By User
- Traffic By User & Internal IP
- Web Activity

6.2.3 Web filtering is done as standard on Networked computers and with Non Networked devices such as ipads / laptops and Mobile phones that use our College WI-FI network.

Categories that are instantly blocked and tracked are:

ADULT – VIOLENCE – RACISM - HATE SPEECH - ALCOHOL – GAMBLING – DRUGS - OFFENSIVE SITES-SUSPICIOUS SITES - SOCIAL NETWORKING - FORUMS – DATING - WEAPONS - SPAM – ADS - SECURITY- MALWARE – ANONYMOUS PROXIES – REMOTE CONNECTION SOFTWARE – SHOPPING –

The web filter works In conjunction with our Anti Virus System (Sophos) which monitors ports and emails for malicious software activity continually 24/7.

6.3 Protected Characteristic Monitoring

6.3.1 If any incident is of extremism; racist/or other protected characteristic nature, the incident will also be logged by the Principal. In turn, the Principal reports

the logged incidents to the Governing Body. The Principal will monitor the action taken and in the event of a recurrence see pupils concerned and inform parents.

6.4 Sanctions

The College 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 the School to manage such situations in, and with, confidence.

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 Positive Behaviour for Learning Policy of the school. Information of misuse will be shared via note in organiser with parent/carer. If behaviour continues, it could 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, 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.

- *Other users – e.g. Affiliated/ Extended Services*

  Contraventions of this policy by other members of the College community will be investigated and if appropriate additional training or information offered, or if appropriate, access to facilities removed or affiliation cancelled.

If inappropriate material is accessed, users are required to immediately report this to Tam Scott, Network Manager and EMPSN so this can be taken into account for monitoring purposes.

7. Working in Partnership with Parents and Carers

Thomas Estley is committed to working in partnership with parents and carers and understands the key role they play in the Internet safety of their children, through promoting Internet safety at home and elsewhere.

We at Thomas Estley also appreciate that there may be some parents who are concerned about the use of the Internet, email and other digital technologies in school. The College will share policies and safeguards both internally and externally with parents to show how to keep children safe on-line both in and out of College.

Useful sites for further information on e-safety are:
http://www.thinkuknow.co.uk
http://www.saferinternet.org.uk

This guide aims to keep parents, teachers and young people well informed on how to stay safe and legal when enjoying entertainment on the internet or via a mobile device.

Copyright law applies to downloading, sharing and streaming just as in the world of physical CDs and DVDs. If you make music, film or TV content available to others on a file-sharing network, download from an illegal site, or sell copies without the permission of those who own the copyright, then you are breaking the law and could face serious penalties.

8. Equality Impact Assessment

Thomas Estley Community College's commitment to equality and diversity means that this policy, via an Equality Impact Assessment, has been screened in relation to the use of gender-neutral language, recognition of the needs of disabled people, promotion of the positive duty in relation to race, age, disability and avoidance of stereotypes.

Based on the Equality Impact Assessment findings, this policy is judged to be of low impact against the equality strands of Race, Gender, Religion, Disability Sexual Orientation and Age. A copy of the Equality Impact Assessment of this policy is available from the Principal's PA.

This Policy is available in alternative formats on request. If you think we can improve the fairness of this Policy, please contact the individual who has responsibility for its update.

9. Policy review

This policy will be reviewed every three years by R&E committee of the governing body, or sooner if requirements change. Appendices will be reviewed annually.