E- safety

TEC Partnership

Training • Education • Careers

Change Control

Version:	V1.0
New or Replacement:	Replacement
Approved by:	SMT
Date approved:	8 September 2015
Name of author:	Group Director – Learner Services
Name of responsible committee:	Safeguarding Committee
Name of Corporation committee:	N/A
Date issued:	Sept 2015
Review date:	Sept 2019
Document Reference:	

Revision History

Version	**Type**	**Date**	**History**
V1.0	Replacement	March 2014	Replacement
V1.1	Revision	August 2015	Revision
V1.2	Revision and update	January 2017	Updated on changes to infrastructure
V1.2	Amendment	March 2018	Guidance on 'student chat'

This policy applies to Grimsby Institute of Further & Higher Education (GIFHE) and incorporates the trading styles of TEC Partnership, Grimsby Institute of Further and Higher Education, Scarborough TEC, Skegness TEC, The Academy Grimsby and all wholly owned subsidiary companies of the Grimsby Institute of Further & Higher Education which include Modal, Support Staff Services and Grimsby College Trading.

Contents

1. Introduction

The Grimsby Institute (TEC PARTNERSHIP) recognizes the benefits and opportunities which new technologies offer to both teaching and learning, however the global nature of the internet its accessibility and the variety of technologies that we have to hand mean that we are heightened in our awareness of the potential risks and challenges that go hand in hand with such freedom of access.

E-Safety is about applying the lessons we have learnt about keeping children, young people and adults safe to technology. E-Safety must be responsive to new technologies and new threats and opportunities that may arise.

It is the intention of the group to implement safeguards to support staff and learners to manage and identify risks independently and to seek advice and guidance in an appropriate and timely manner. We believe that this can be achieved through a combination of security measures, training and guidance along with the implementation of associated policies. This policy links in with Staff Code of Conduct and the Staff Disciplinary Process

E-Safety is not simply about virus protection, internet filtering, firewalls or other IT security concerns. E-Safety is also about ensuring that technology is used in a manner that is safe and respectful to others. Due to this E-Safety has a significant overlap with other policies and procedures, particularly those related to child protection, anti-bullying and acceptable use of IT. This policy has been updated using guidance from the NSPCC website https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/e-safety-schools/

2. Scope

This policy applies to all learners and particularly children, young people and adults who may need support and all staff, volunteers, partners and families living and working at College centers, other external facilities, in the workplace or distance learning.

An e-Safety incident is considered to have occurred when a learner, staff member or Governor instigates, or is the victim of, an activity which utilizes Information and Communications Technologies (ICT) to endanger the personal safety, mental well-being, or financial well-being of another individual.
Activities which will be considered E-Safety incidents include, but are not limited to, the use of ICT to

- Access, view, copy or download illegal content, or materials, including, but not limited to:
  - child pornography
  - materials inciting racial hatred or violence
  - materials that are deemed to be in connection with radicalisation or will place learners at risk of radicalisation.
- Access, view, copy or download inappropriate content, or materials, as defined by the College's Acceptable Use of ICT policy.
- Bully or harass an individual or group (Cyber Bullying).
- Commit fraud or identify theft.
- Undertake any activities which would be in violation of the Child Protection, Protection of Vulnerable Adult or Anti-Bullying policies
- Any other incident where it can be reasonably considered that the personal safety,

mental wellbeing or financial health of an individual has been endangered by the use of ICT.

In this context ICT includes, but is not limited to,:

a) College owned equipment, including:
- Desktop PC’s
- Servers
- Laptop/Tablet devices
- Telephones, both fixed and mobile
- Digital video camera or camcorders
- Digital audio recording devices
- Reproduction devices (scanners, printers, etc..)
- Any and all software and IT services provided by the College

b) Privately owned ICT equipment (including personal mobile phones), when:
- Connected to any College owned network
- Utilised to access College software and services
- Made use of on campus, or in the pursuit of College business.

3. Legislation

The legal framework for the role of the Group and the governing body is as follows:

Computer Misuse Act 1990
Makes provision for securing computer material against unauthorised access or modification; and for connected purposes.

Data Protection Act 1998
Makes provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information.

Malicious Communication Act 1998
Makes provision for the punishment of persons who send or deliver letters or other articles for the purpose of causing distress or anxiety.

Counter-Terrorism and Security Act 2015
From 01 July 2015 all HE institutions, colleges, schools, and registered early years childcare providers are subject to a duty under section 26 of the act in the exercise of their functions, to have “due regard to the need to prevent people from being drawn into terrorism”. This duty is known as the Prevent duty.

The Education Act 2002 - Section 157 & 175
Requires local authorities and governing bodies of further education institutions to make arrangements to ensure that their functions are carried out with a view to safeguarding and promoting the welfare of children, young people and adults at risk. In addition they should have regard to any guidance issued by the Secretary of State in considering what arrangements they may need to make.

Working Together to Safeguard Children / young people (2017)
Provides statutory guidance on the roles and responsibilities of agencies working together to safeguard children/ young people. In addition it sets out the framework for the formation of Local Safeguarding Children Boards and details the allegation management process.

The Mental Capacity Act (2005)
Provides a way in which people who may need help to make decisions can get that help from someone who can be trusted to act in their best interests. Mental Capacity under the Act means being able to make your own decisions. The Mental Capacity Act and its Code of Conduct contain a set of rules, procedures and guidance. The Act applies in full to those aged 18 or over, the entire Act except making Power of Attorney or Making a Will applies to 16 and 17 year olds. The Act only applies to those under 16 in very limited circumstances and these would have to be determined by a Court.

This policy should be read in conjunction with the College's **Anti – Bullying policy** its **Staff Code of Conduct** and **Safeguarding Children, Young People and Adults at Risk Policy & Procedures.**

4. Responsibilities

It is the responsibility of every staff member to give full and active support for the policy by ensuring:

- The policy is accessible, known, understood and implemented.
- All actual and suspected serious e-Safety incidents are reported to the safeguarding team.
- Parents/Guardians, providers, sponsors, employers and other stakeholders have a responsibility to report any e-Safety concerns they may have to the College.
- All learners both Further and Higher education have a responsibility to:
    - Report any e-Safety concerns they may have to a member of staff, this could be a Progression Coach, Tutor or Learner Mentor.
    - Not engage at any time in any form of behaviour which would result in the occurrence of an e-Safety incident.

5. Actions to Implement and Develop Policy

5.1. Reporting

All e-Safety incidents should be reported to a designated safeguarding person who will log the incident in the safeguarding database, and where necessary will engage with external agencies.

5.1.1. Safety and infrastructure.

The group's network is safeguarded using E-safe , is a service that's designed to protect our learners and staff from safeguarding risks - with a **unique triple-lock approach** to monitoring all activity on our IT devices. **Note that the software will monitor and record malicious online activity when any Group devices are being used on your home (or any other) network too.** This program monitors and where possible, filters harmful sites and alerts staff to the sites accessed and the user who used the device. A system is set up that alerts Safeguarding and HR teams and where necessary, further investigations will be made. All known sites that are harmful or enable learners/staff to access illegal or explicit content will be blocked when using the Group network. **The Group firewall will record and monitor all activity on staff members personal devices if those devices have been or are being used to access the college network. Any concerning activity will be investigated and dealt with under the staff disciplinary and code of conduct policy.**

Securing and Preserving Evidence

IT Services should be contacted immediately following the reporting of any serious e-Safety incidents and asked to make copies of relevant access logs, files etc…

If it is believed that an immediate risk of exposure to illegal or inappropriate materials, or mental distress exists to staff or learners, the computer or devices should be turned off immediately. **You should not "shutdown" or log off as this may corrupt, delete or overwrite evidence, the power supply should be turned off at the wall or the battery should be physically removed.**

The equipment should then be moved to a secure location.

5.2. Illegal Material or Activities

Where an e-safety incident is reported to the Group this matter will be dealt with very seriously. The Group will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring. If a learner wishes to report an incident, they can do so to their tutor or to the Intensive support manager/ officer. Where a member of staff wishes to report an incident, they must contact their line manager. Following any incident, the Group will review what has happened and decide on the most appropriate and proportionate course of action. Sanctions may be put in place, external agencies may be involved or the matter may be resolved internally.

Depending on the seriousness of the incident. Serious incidents will be dealt with by Senior Management, in consultation with appropriate external agencies.

The Director of IT Services is responsible for involving other senior managers and law enforcement agencies as required. IT Services will assume responsibility for obtaining, securing and preserving appropriate additional evidence. For example, remote screen shots, web filter logs etc.

If it is believed that there is a child protection issue the procedures outlined in the Safeguarding policy should be implemented.

5.3. Indecent imagery.

It is a criminal offence to take, show, and share indecent images of children and young people, those under the age of 18 can face prosecution for taking indecent images of themselves and sharing them with others. (Section 1 Protection of Children Act 1978)

Under no circumstances should any person make copies, including screen shots or print outs, of suspected child/ young person indecent imagery. Taking copies of such materials, even when intended for evidentiary purposes, is a crime.

5.4.1

Youth produces sexual imagery (YPSI) (Sexting) is described as and applies to ;

- Youth produced' includes young people sharing images that they, or another young person, have created of themselves.
- 'Sexual' is clearer than 'indecent.' A judgement of whether something is 'decent' is both a value judgement and dependent on context.
- 'Imagery' covers both still photos and moving videos

- A person under the age of 18 creates and shares sexual imagery of themselves with a peer under the age of 18
- A person under the age of 18 shares sexual imagery created by another person under the age of 18 with a peer under the age of 18 or an adult
- A person under the age of 18 is in possession of sexual imagery created by another person under the age of 18

5.4.2

In the event of an incident relating to YPSI occurring, you must do the following.

- The incident should be referred to the Intensive support (IST) as soon as possible
- The IST should hold an initial review meeting with appropriate school staff
- There should be subsequent interviews with the young people involved (if appropriate)
- Parents should be informed at an early stage and involved in the process unless there is good reason to believe that involving parents would put the young person at risk of harm
- At any point in the process if there is a concern a young person has been harmed or is at risk of harm a referral should be made to children's social care and/or the police immediately.

5.4.3 Viewing the Imagery

Staff should **not** view youth produced sexual imagery unless there is good and clear reason to do so. Wherever possible responses to incidents should be based on what the Intensive support team have been told about the content of the imagery.

The decision to view imagery should be based on the professional judgement of the IST and should always comply with the child protection policy and procedures of the school or college. Imagery should never be viewed if the act of viewing will cause significant distress or harm to the pupil.

If a decision is made to view imagery the IST would need to be satisfied that viewing:

- is the only way to make a decision about whether to involve other agencies (i.e. it is not possible to establish the facts from the young people involved)

- is necessary to report the image to a website, app or suitable reporting agency to have it taken down, or to support the young person or parent in making a report
- is unavoidable because a pupil has presented an image directly to a staff member or the imagery has been found on a school device or network

If it is necessary to view the imagery then the IST should:

- Never copy, print or share the imagery; this is illegal.
- Discuss the decision with the Designated Safeguarding Lead
- Ensure viewing is undertaken by the DSL or another member of the safeguarding team
- Ensure viewing takes place with another member of staff present in the room, ideally the DSL or a member of the senior leadership team. This staff member does not need to view the images.
- Wherever possible ensure viewing takes place on school or college premises, ideally in the office of the IST or the DSL.
- Ensure wherever possible that images are viewed by a staff member of the same sex as the young person in the imagery.
- Record the viewing of the imagery in the colleges safeguarding records including who was present, why the image was viewed and any subsequent actions Ensure this is signed and dated and meets the wider standards set out by Ofsted for recording safeguarding incidents.

The National Police Chiefs Council (NPCC) has made clear that incidents involving youth produced sexual imagery should primarily be treated as safeguarding issues.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609874/6_2939_SP_NCA_Sexting_In_Schools_FINAL_Update_Jan17.pdf

5.4. Inappropriate Material or Activities

Inappropriate material or activities are considered to be any materials or activities which are considered as unacceptable by the Acceptable Use of IT policy.

5.5. Staff Access to Inappropriate Material

Where it is suspected that a staff member has been accessing inappropriate material, or attempting to access, the time and date of the incident should be noted and the concerns raised with the head of Human resources.

5.6. Learner Access to Inappropriate Material

Where it is suspected that a learner has been accessing inappropriate material, or attempting to access, the time and date of the incident should be noted and brought to the attention of the relevant Curriculum Leader or Head of School. The safeguarding team should be contacted who may then liaise with the IT Helpdesk to take copies of relevant access logs etc…

5.7. Cyber-Bullying

Cyber-Bullying can be defined as making use of IT to undertake to bully. Examples of cyber-bullying include, but are not limited to:

- Sending offensive or abusive e-mails, instant messages, or “text” messages.
- Inviting selected individuals to a chat room or website to discuss another individual who has not been invited.
- Posting offensive, defamatory or abusive messages about an individual or group to a public or members only internet forum.
- Using a digital camera to take humiliating images

Incidents of actual or suspected cyber-bullying should be dealt with in accordance with the Anti-Bullying policy.

5.8. Virus & Malware Protection

The Group will do all that it can to make sure the Group’s network is safe and secure. Every effort will be made to keep security software up to date. Appropriate security measures will include the use of enhanced filtering and protection of Firewalls, servers, routers, work stations etc. to prevent accidental or malicious Access of systems and information. Digital communications, including email and Internet postings, over the college network, will be monitored in line with the Network Usage Policy.

IT Services will make all reasonable efforts to ensure current, up to date, anti-virus and malware protection is installed on all College systems. However, users of the systems have a responsibility to:

- Alert IT Services if they discover a fault with their anti-virus and anti-malware software
- Ensure personally assigned devices (i.e. laptops) are connected to the network at least once per month.

6. Training

Provide mandatory training to all staff on e-Safety awareness and their responsibilities in the event of an e-Safely incident.

7. Appendices

7.1. Useful links

Iwf.org.uk

Childline.org.uk

Shareaware.org.uk

Netaware.org.uk

Internetmatters.org.uk

Saferinternetday.org.uk

Ofcom.org.uk

Thinkyouknow.co.uk

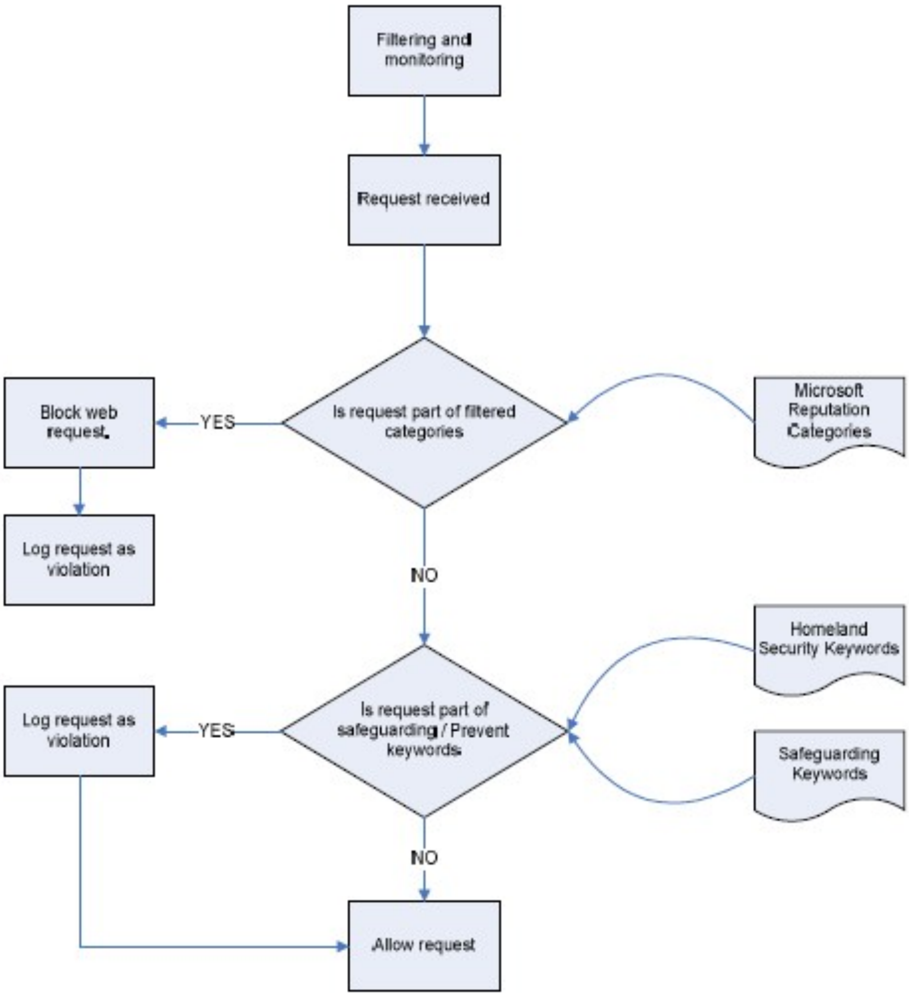
Swgfl.org.uk

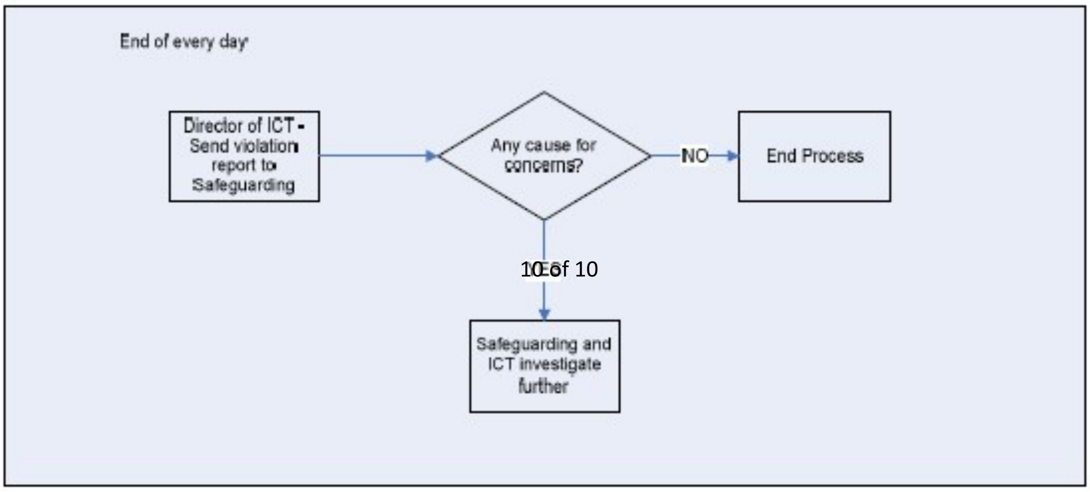
Childnet.com

www.thinkuknow.co.uk
www.thinkuknow.co.uk/teachers

This policy should be read in conjunction with
Safeguarding policy
Anti-bullying policy
Code of conduct policy

7.2. Process for Filtering and Monitoring




End of every day
Director of ICT - Send violation report to Safeguarding
Any cause for concerns?
NO
End Process
Safeguarding and ICT investigate further

TEC Partnership
Training • Education • Careers

Grimsby Institute
University Centre Grimsby
Skegness TEC Training Education Careers
The Academy Grimsby
YOUR FUTURE, FOCUSED

gi International
nel National Employer Training
workforce SKILLS
Little Stars Day Nursery
Doncaster LEARNING CENTRE

distance LEARNING
Skegness Learning Centre
Grimsby Learning Centre
Immingham Learning Centre
Louth Learning Centre
Scarborough TEC Training Education Careers

MODAL TRAINING
ecosh EAST COAST OCCUPATIONAL SAFETY & HEALTH
Transafe TRAINING
FRPERC Food Refrigeration and Process Engineering Research Centre

Nuns Corner, Grimsby, North East Lincolnshire, DN34 5BQ, UK
Tel: 01472 311 222 **Email:** infocent@grimsby.ac.uk **Web:** grimsby.ac.uk