Online Safety Policy

T:C Partnership
Training • Education • Careers

Change Control

Version:	V1.0
New or Replacement:	Replacement
Approved by:	SMT
Date approved:	8 September 2015
Name of author:	Executive Director of Learner Services
Name of responsible committee:	Safeguarding Committee
Name of Corporation committee:	N/A
Date issued:	April 2022
Review date:	Sept 2024
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'
V1.2	Revision	November 2019	Review
V1.2	Amendment	March 2020	Covid response
V1.2	Amendment	September 2020	Reflect changes in KCSIE 2020
	Review	April 2022	Reviewed and updated

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

Introduction

The TEC Partnership is an educational provider, supporting students from aged 14 +

The purpose of this policy statement is to:

- ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices
- provide staff and volunteers with the overarching principles that guide our approach to online safety
- ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

The policy statement applies to all staff, volunteers, children and young people and anyone employed or working on behalf of the TEC Partnership.

Legal framework

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England

Summaries of the key legislation and guidance are available on:

- online abuse Child abuse and neglect | NSPCC Learning
- bullying Protecting children from bullying and cyberbullying | NSPCC Learning
- child protection Child protection system in the UK | NSPCC Learning
- Teaching guidance Teaching online safety in school | DfE
- RSE and Health Education Relationships Education, Relationships and Sec Education (RSE) and Health Education | DfE
- Framework for a digital life Education for a connected World Framework – 2020 | DfE

We believe that:

- children and young people should never experience abuse of any kind.
- children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are always kept safe.

We recognise that:

- The online world provides everyone with many opportunities; however, it can also present risks and challenges
- We have a duty to ensure that all children, young people, and adults involved in our organisation are protected from potential harm online
- We have a responsibility to help keep children and young people safe online, whether they are using TEC Partnership network and devices
- All children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse
- Working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety
- For many young people the distinction between the online world and other aspects of their life is less marked than for many adults.

This policy has been updated using guidance from the NSPCC website E-safety for schools | NSPCC Learning

We will seek to reduce the risk of harm to children and young people safe by:

- Having clear and specific expectations of Learners, staff and volunteers on how to behave online through Induction, tutorial and training.
- Supporting and encouraging young people to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others.
- Sharing guidance and offering advice / support to parents and carer's around online safety and what they can do to keep their children safe online.
- Have clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child/young person.
- All staff recognising that when learner is working remotely, they are at an increased risk of harmful online activity.
- Reviewing and updating the security of our information systems regularly.
- Ensuring that user names, logins, email accounts and passwords are used effectively.
- Ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate.
- Ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given.
- Providing supervision, support and training for staff and volunteers about online safety.

Online Abuse is any type of abuse that happens on the web, whether through social networks, playing games online or using mobile phones (NSPCC 2015). The college uses an appropriate filter and monitoring system in place, which both learners and staff cohorts are aware of. We have a whole college approach to online safety where learners and staff are regularly updated about processes in place. Where learners have been asked to work from home, they have been provided with advice and guidance around online safety.

If online abuse occurs, we will respond to it by:

- Having clear and robust safeguarding procedures in place for responding to abuse (including online abuse).
- Providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying/cyberbullying, emotional abuse, sexting, sexual abuse, sexual harassment and sexual exploitation.
- Making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole, into account.
- Reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.

An Online Safety Incident is considered to have occurred when a learner, staff member or Governor instigates, or is the victim of, an activity which utilises Information and Communications Technologies (ICT) to endanger the personal safety, mental well-being, or financial well-being of another individual.

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

- 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

Privately owned ICT equipment (including personal mobile phones) is included 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.

Activities which will be considered as Online Safety incidents include, but are not limited to:

- Accessing any type of pornography
- Accessing/Creating/Sharing materials inciting racial hatred or violence
- Accessing/Creating/Sharing materials that are deemed to be in connection with radicalisation or will place learners at risk of radicalisation.
- Accessing/Creating/Sharing other inappropriate content, or materials, as defined by the College's Acceptable Use of ICT policy.
- Cyber Bullying
- Committing fraud or identify theft.
- Undertaking any activities which would be in violation of the safeguarding and child Protection policy, Learner Disciplinary Policy and Anti- Bullying policy.
- Any other incident where it can be reasonably considered that the personal safety, mental wellbeing or financial health of an individual has been endangered using ICT.

The TEC Partnership Online Safety Principles include:

- Safe and healthy online relationships.
- Confident self-image and online identity.
- Positive online reputation.
- No online bullying.
- Efficient management of information online.
- Healthy use of online technologies
- Excellent privacy and security.
- Clear ownership of online content.

Legislation

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

The Data Protection Act

The Data Protection Act 2018 controls how your personal information is used by organisations, businesses or the government.
The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR). Data protection - GOV.UK (www.gov.uk)

Malicious Communication Act 2003

Makes provision for the punishment of persons who send or deliver letters or other articles for the purpose of causing distress or anxiety. Malicious Communications Act 1988 (legislation.gov.uk)

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. Counter-Terrorism and Security Act 2015 (legislation.gov.uk)

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. Education Act 2002 (legislation.gov.uk)

Working Together to Safeguard Children (2018)

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 S afeguarding Partner's (formerly LSCB) and details the allegation management process. This includes providing a coordinated offer of early help when additional needs of children are identified and contributing to inter-
agency plans to provide additional support to children subject to child protection plans. Access is all owed for children's social care from the local
authority and, where appropriate, from a placing local authority, for that authority to conduct, or to consider whether to conduct, a section 17 or a section 47 assessment. Safeguarding arrangements t ake into account the procedures and practice of the local authority as part of the inter-
agency safeguarding procedures set up by the Local Safeguarding Partner's Working together to safeguard children - GOV.UK (www.gov.uk)

Keeping Children Safe in Education (2021)

Sets out the safeguarding statutory responsibilities of schools and colleges, as well as good practice recommendations in relation to children. This covers the relevant legislation; the responsibilities of Governing Bodies and Principals; safer recruitment practice; recruitment and vetting checks;
dealing with allegations of abuse or misconduct against staff; and also, checklists, flowcharts and example. Keeping children safe in education - GOV.UK (www.gov.uk)

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. Mental Capacity Act 2005 (legislation.gov.uk)

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.

Key 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 Online Safety Incidents are reported to the safeguarding team.
- Parents/Guardians, providers, sponsors, employers and other stakeholders have a responsibility to monitor use where possible and report any e-Safety concerns they may have to the organisation.
- The principles of positive relationships apply online, as well as in person.
- It is clear to all learners what to do, and where to get support, with any online issues.
- Opportunities for exploring online safety and positive online relationships are embraced, in whatever setting they occur. Embedding online safety principles throughout the curriculum is essential.
- They help pupils assess any arising online situation, think through the consequences and develop a plan of action.

All learners both Further and Higher education have a responsibility to:

- Abide by the organisation's policies and rules for using ICT and working online.
- Report any online safety concerns they may have to a member of staff, this could be a Success Coach, Tutor or directly to the safeguarding team.
- Keep their login details and passwords secure and not share them with anyone else.
- Not engage at any time in any form of behaviour which would result in the occurrence of an online Safety incident.
- Consider how their information is being used online and how that data may be shared.
- Not share any personal content they would not wish the public to see.
- Ensure they are aware of any age restrictions for any online content or platforms.
- Think carefully about the source of any information gathered online, the purpose of the text and the likely accuracy of the data.
- Make sensible decisions in order to stay safe online.
- Look out for any fake websites or scam emails, and report them.

Actions to Implement and Develop Policy

Reporting and Monitoring Use

All Online 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.

The network is safeguarded using Smoothwall, which is a service that's designed to protect our learners and staff from potential safeguarding risks – with proactive, real-time monitoring of all activity on our organisation's IT devices. (Note that the software will monitor and record malicious online activity when any college devices are being used on your home, or any other, network too.) This program monitors and filters harmful sites and alerts staff to the websites that have been accessed, as well as reporting the user's details.

An internal system automatically alerts the organisation's Safeguarding and HR teams and where necessary, further investigations will be made. All sites that are known to be harmful or enable learners/staff to access illegal or explicit content will be blocked when using the TEC Partnership network. The infrastructure includes firewalls which 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.**

It should be noted the we have a zero tolerance to sexual harassment and any incident – even if off site will be dealt with under gross misconduct and learners face exclusion.

Securing and Preserving Evidence

IT Services should be contacted immediately following the reporting of any serious Online Safety Incidents and asked to make copies of relevant access logs, files etc… for further investigation.

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. Instead, 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 by a trained member of IT Services.

Illegal Material or Activities

Where an Online Safety Incident is reported to the TEC Partnership, this matter will be dealt with very seriously. Staff 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 TEC Partnership 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. 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.

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 still 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.

Youth Produced Sexual Imagery (YPSI) (aka Sexting) is described as young people (under the age of 18) sharing images that they, or another young person, have created of themselves. 'Imagery' covers both still photos and moving videos

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

1. The incident should be referred to the Intensive Support Team (IST) as soon as possible.
2. The IST should hold an initial review meeting with appropriate school staff.
3. There should be subsequent interviews with the young people involved (if appropriate).
4. 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.
5. 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.

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.
(reference: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)

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.

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.

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 safeguarding team, who may then liaise with the IT Helpdesk to take copies of relevant access logs etc. Appropriate and proportionate action and support will be implemented.

Cyber-Bullying

Cyber-Bullying can be defined as making use of ICT 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 will be dealt with in accordance with the Anti- Bullying policy.

Virus & Malware Protection

The TEC Partnership will do all that it can to make sure the organisation’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 organizational infrastructure and 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 for updates etc.

Staff use of personal devices

Safe use and compliance

In terms of our compliance with GDPR, staff have legitimate interest in using a personal device to capture data as it enables us to evidence the work of our learners. If you are using a personal device to film/ take photos of learners, then you must adhere to the following points as they are paramount in ensuring the safeguarding of staff and learners:

- Where possible please use a college device, instead of a personal one.
- Your personal device is password protected.
- Any data must be uploaded to SharePoint within 7 days.
- All data on the personal device must then be deleted, after 7 days.
- You must not share any photos / videos with learners or their parents/ carers/siblings from your personal device.
- You must not show the photos / videos to learners from your personal device.
- You must not upload any photos / videos to another personal device in your home or a memory stick.
- You must not upload any photos/ videos to your own social media sites.

It is important to note that any staff member found to be in breach of the requirements will face disciplinary action under failure to safeguard.

Training

The TEC Partnership will provide mandatory training to all staff on Online Safety awareness and their responsibilities in the event of an Online Safety Incident.

COVID-19

There have significant changes to learning and support in response to the government guidelines around the outbreak of COVID-19. However, the college's Safeguarding policy remains fundamentally the same – the safety and wellbeing of our learners is our priority and Safeguarding concerns will continue to be responded to in line with our policy as well as updated guidance and processes from the local 3 safeguarding partners/local authorities.

The Intensive Support Team along with our Designated and Deputy Safeguarding Leads, remain available to staff, learners and their families throughout any period of lock-down. In addition to this, the University Centre Grimsby (UCG) will remain open for children of key workers and our most vulnerable learners to access. We will continue to regularly review our position in light of guidance issued by the Government and updates provided by the Local Authority in relation to any future imposed periods of lock-down.

Reporting arrangements

The college reporting procedures continue in line with our Safeguarding policy.
The Designated Safeguarding Lead is: Rachel Ellis – Jones
The Deputy DSLs are: Tamarra Taylor and Sacha Mills
Our approach ensures a DSL or deputy is always contactable within usual opening hours and that staff are aware of procedures and report any concerns for a learner immediately to the Intensive Support Team, whether they are in attendance on site or not. Staff are aware of the need for increased vigilance due to the pressures on families, support services and a probable increase in demand for these services.
The Intensive Support Team will contact Children /Adult's Social Care in line with the relevant local authority.
All college devices that have been provided to learners remain under the Smoothwall network.
Learners have access to a dedicated Canvas page that covers keeping themselves safe online and digital wellbeing.

Peer on peer abuse and online safety

We recognise the potential for abuse online to increase during this time. Our staff will remain vigilant to the signs and disclosures of peer-on-peer abuse, including those between young people who are not currently attending our provision. When contacting learners and parents/carers, staff will offer the opportunity for any concerns to be discussed. Learners will of course use the internet more during this time, much of our teaching and learning will be taking place online. Staff are aware of signs of cyber-bullying and other risks to children online and will continue to report concerns in to the Intensive Support Team. In addition, the TEC Partnership have ensured appropriate filters and monitors remain in place. Our governing body will review arrangements to ensure they remain appropriate. The school/college has taken on board guidance from the UK Safer Internet Centre on safe remote learning and guidance for safer working practice from the Safer Recruitment Consortium. In addition to this;

- Staff have been reminded of the TEC Partnership's code of conduct and importance of using school/college systems to communicate with children and their parents/carers.
- The safeguarding handbook has been updated to reflect remote learning.
- Children and young people accessing remote learning receive guidance on keeping safe online and know how to raise concerns with their Success Coach, Intensive Support Team and/or CEOP as required.
- Allegations or concerns about staff.
- All staff are reminded to immediately report any concern, no matter how small, directly to Steve Butler in HR. Arrangements to contact the Local Authority Designated Officer where required remain unchanged.

Useful contacts

5Rights | Child Online Protection (5rightsfoundation.com)

Home - CEASE / Centre to End All Sexual Exploitation

Internet Watch Foundation IWF - Eliminating Child Sexual Abuse Online | IWF

CEOP Safety Centre

Childline | Childline

Childnet — Online safety for young people

NSPCC | The UK children's charity | NSPCC

Meeting the needs of children abused online | Marie Collins Foundation

TEC Partnership
Training • Education • Careers

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