Online Safety Policy
August 2021

Reviewed by – Sue Fielding – 5th August 2021 v1

To be reviewed annually – 5th August 2022

Signed: **5th August 2021**

Sue Fielding – Managing Director

Table of Contents

What is online safety?

Online safety is defined as being safe from risks to personal safety and wellbeing when using all fixed and mobile devices that allow access to the internet, as well as those that are used to communicate electronically.

It means ensuring that children and young people are protected from harm and supported to achieve the maximum benefit from new and developing technologies without risk to themselves or others. This includes personal computers, laptops, mobile phones and games consoles such as Xbox, PlayStation and Wii.

The aim of promoting online safety is to protect young people from the adverse consequences of access or use of electronic media, including from bullying, inappropriate sexualised behaviour or exploitation. Many of these risks reflect situations in the non-digital off-line world. As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build students' resilience to the risks to which they may be exposed, so that they have the skills and confidence to face and address these risks.

Safeguarding against these risks is not just an ICT responsibility; it is everyone's responsibility, and needs to be considered as part of the overall arrangements in place that safeguard and promote the welfare of all members of the community, particularly those that are vulnerable.

The term 'safeguard' is defined for the purposes of this document in relation to online safety as the process of limiting risks to students when using technology through a combined approach to policies and procedures, infrastructure and education, underpinned by standards and inspection.

Online safety policy statement

The aim of this policy is to ensure staff, students, and volunteers use GFT internet and Information and Communication Technology (ICT) equipment safely and appropriately, ensuring the best possible outcomes for our students.

The main areas of risk for GFT as a learning provider can be summarised as follows:

Content:

- exposure to illegal, inappropriate or harmful material, including online pornography, ignoring age ratings in games (exposure to violence and inappropriate language)
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- content validation: how to check authenticity and accuracy of online content.

Contact:

- being subjected to harmful online interaction with other users
- grooming
- child sexual exploitation
- cyber-bullying in all forms
- extremism and radicalisation
- identity theft and sharing passwords.

Conduct:

- personal online behaviour that increases the likelihood of, or causes, harm
- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being - amount of time spent online (socialising, watching video or gaming)
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- copyright (no thought or consideration for intellectual property and ownership – such as music and film).

Scope

GFT will deal with such incidents within this policy and associated behaviour and anti-bullying policies, and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place outside of GFT

This policy has been created in line with the statutory guidance document **Keeping Children Safe in Education, 2015.**

.

Communication

The online safety policy will be communicated to staff and students in the following ways:

- policy to be posted on the website/ common room/IT suite and classrooms;
- policy to be part of induction pack for new staff;
- GFT will provide a 'Safe Internet' page for parents/carers on our website. Information will include internet safety advice, home web filtering tips and links to recommended online safety websites; and guidance on the amount of time children and young people may spend on a computer, smartphone, tablet or games console;
- acceptable use agreements to be issued to students, usually on enrolment
- acceptable use agreements to be held in student and personnel files;
- All students and tutors will be provided with online safety training.

Handling complaints

- GFT will take all reasonable precautions to ensure online safety. However, owing to the international scale and linked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a GFT computer or mobile device.
- Staff and students are given information about actions to be taken in the event of a complaint or breach of this policy

  These include:
  - Interview with DSL and /or Managing Director
  - informing parents/carers
  - referral to Local Authority, Children's Social Care and/or police.

- The DSL acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Managing Director
- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy; Complaints and/or allegations related to child protection are dealt with in accordance with the GFT and Local Authority child protection procedures:
- All complaints will be dealt with in accordance with our Complaints Policy. https://www.wearegft.co.uk/policies/ https://www.wearegft.co.uk/report-a-problem/

Review and Monitoring

The online safety policy is referenced from within other GFT policies:

- ICT policy,
- Safeguarding and Child Protection policy,
- Anti-Bullying policy,
- Behaviour policy.

The online safety policy will be reviewed annually or when any significant changes occur regarding the use of technologies within GFT

There is widespread ownership of the policy and it has been agreed by the SLT All amendments to the GFT online safety policy will be communicated to all members of staff

The online safety policy will be reviewed annually

Online Safety Lead – roles and responsibilities

The DSL will have responsibility for Online Safety. It is crucial that they develop and maintaining an online safety culture within GFT. The Deputy DSL will cover for them in their absence.

The responsibilities of this role are to:

a. Develop an online safety culture at GFT
b. Be the named point of contact on all online safety issues
c. Ensure online safety is included as part of the induction procedures, and all staff and volunteers receive a copy of the **Acceptable Use Policy**, and return a signed and dated version to the DSL
d. Monitor online safety, such as:
    1. ensuring the technology infrastructure provides a safe and secure environment for students and staff, for example by ensuring web address filters and other security management software is in place
    2. Maintaining an online safety incident log on “My Concern”, to record user concerns and incidents
e. Reporting on online safety issues to the SLT, CEO and Governors
f. Ensure that all students, staff, volunteers, and management/Governor members know what to do if they are concerned about an online safety issue

g. Keep abreast of developing online safety issues via attendance at relevant training sessions, conferences or seminars, and recommended websites such as:
    a. http://www.saferinternet.org.uk/
    b. http://www.thinkuknow.co.uk
    c. http://www.ceop.police.uk
h. Ensure that online safety is embedded within continuing professional development (CPD) for staff and volunteers, and co-ordinate training as appropriate
i. Ensure that online safety is embedded across all activities as appropriate
j. Ensure that online safety is promoted to students, parents/carers and others whilst at GFT, the home and the community
k. Review and update online safety policies and procedures on a regular basis and after an incident.

The curriculum

Student online safety

GFT:

- Has clear, progressive online safety sessions embedded as part of the Employability and Apprenticeship programmes. This covers a range of skills and behaviours appropriate to the students' age and experience, including how:
    - to develop a range of strategies to evaluate and verify information before accepting its accuracy
    - to be aware that the author of a web site, blog or Post may have a particular bias or purpose, and to develop skills to recognise what that may be;
    - to understand how search engines work and to understand that this affects the results they see at the top of the search results
    - to demonstrate polite and acceptable behaviour when using software services in an online environment
    - to understand why they must not upload pictures or videos of others without their permission
    - to know not to download any files – such as video or music files - without permission from the copyright holder;
    - to have strategies for dealing with receipt of inappropriate material;
    - to understand why and how some people will 'groom' young people for criminal, anti-social or sexual purposes;
    - to understand the impact of cyberbullying, sexting and trolling, and know how to seek help if they are affected by any form of online bullying.
    - To know how to report any abuse and how to seek help if they experience problems when using internet-connected technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the 'Click CEOP' button.
- plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas

- will remind students about their responsibilities through an end-user **Acceptable Use Policy**, which every student will sign/will be displayed throughout the centre
- ensures staff will model safe and responsible behaviour in their own use of technology during lessons
- ensures that when copying content from the web, staff and students understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright and intellectual property rights;

Staff Training

GFT

- ensures staff know how to send or receive sensitive and personal data, and understand the requirement to encrypt data where the sensitivity of that data requires data protection
- makes regular online safety training available to staff
- provides, as part of the induction process, all new staff [including those on an apprenticeship, and work experience] with information and guidance on the online safety policy and GFT's Acceptable Use Policies.

Parent awareness

GFT:

- Provides advice and guidance for parents, including:
    - introduction of the **Acceptable Use Policy** to new parents, to ensure that principles of online safety are made clear
    - Information on the web site including recommended support and information sites for parents.

Definitions

What do we mean by 'online'?

When we refer to being online we include being connected to the internet or communicating through a wide range of devices or technologies, such as computers, laptops, mobile phones, tablet computers, hand-held devices and games consoles.

GFT

The Training Provider

Parent/carer

The term parent/carer refers to any individual who has a parental responsibility for a child or has care of a child (Student).

DSL

Designated Safeguarding Lead

Use of ICT equipment

Where students are allowed free access to browse the internet, e.g. in break time staff must be vigilant in monitoring the content of the websites the young people visit

Staff who use GFT's ICT and communications systems:

a. must sign and abide by GFT's **Acceptable Use Policy**

b. must use the systems responsibly and keep them safe

c. must maintain safe professional boundaries with parents. This includes not giving their personal email address to students or befriending students on social network sites, such as Facebook or Instagram

d. will have clearly defined access rights to GFT ICT systems. Details of the access rights available to groups of users will be recorded and maintained by Data Productions, and will be reviewed, at least annually, by the Managing Director

e. must treat as confidential any passwords provided to allow access to ICT equipment

f. must ensure integrity of passwords. Network user account passwords should be strong (mixture of letters, number and characters) and be changed periodically, e.g. monthly. If a password is compromised, it must be changed as soon as possible and no longer than within 24 hours;

g. must not install software on the GFT equipment, including apps, freeware and shareware

h. must not use personal devices (e.g. USB memory sticks) to upload or download material onto GFT network or website, or any ICT device

    1. GFT provides encrypted USB memory sticks for staff to use (Please see the Data/Admin manager if these are required)

i. Agree any use of cloud storage systems (e.g. Dropbox, Google Drive, etc.) will be approved by the Managing Director

j. Must comply with any ICT security procedures governing the use of systems in GFT, including anti-virus measures

k. Must report known breaches of this policy, including any inappropriate images, messages or other material which may be discovered on GFT's ICT systems

l. Must ensure that the systems are used in compliance with this online safety policy

m. Will be provided with online safety training.

n. Understand that system use, including but not limited to internet usage and system logs may be monitored.

Online safety and use of digital devices

At all times, staff, parents, students, and volunteers will treat others with respect and will not undertake any actions that may bring GFT into disrepute.

Mobile phones, tablets and other digital devices can present several problems when not used appropriately.

a. Mobile/smartphones, tablets and other personal devices can allow wireless and 3/4/5G internet access via alternative ISPs, and thereby bypass the GFT's security settings and filtering;
b. Mobile/smartphones with integrated cameras could lead to child protection, bullying and data protection issues, with regard to inappropriate capture, use or distribution of images of students
or staff.

Equipment

GFT is responsible for ensuring that the network infrastructure, computer equipment and internet provision is as safe and secure as is reasonably possible, and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities.

All computer equipment is installed professionally and meets current health and safety standards. Equipment is maintained to ensure health and safety standards are followed.

Internet access

GFT Internet Service Provider (ISP) is BT. Internet filtering based on the Internet Watch Foundation (www.iwf.org.uk) model via Gobalview, a service that is activated on the gateway router to capture all users of the internet facility.

There will be situations when students will need to research topics that would normally result in internet searches being blocked, e.g. racism; drug use; discrimination; freedom of speech, etc. When such a situation is anticipated to arise, staff can request that the Data Productions temporarily relax the standard filtering regime for the defined period of study only. Any request to do so must be requested in writing, with clear reasons for the need, and be authorised by The Managing Director.

Students must be taught in all lessons to be critically aware of the website content they access online, and be guided to validate the accuracy of information

Students must be taught to acknowledge any source of information they cite or use, and to respect copyright when using material accessed on the internet.

Email

GFT uses Office 365 for emails which includes online projection to detect and block viruses, spam, phishing, Trojan, and other malicious message types.

All staff use standard GFT-issued email addresses

a. Staff and volunteers will use only a GFT email account for their professional use
b. All digital communication between staff and students and parents/carers (email, Messaging) must be professional in tone and content
c. Students should be taught about email safety issues, such as the risks attached to the sharing or revealing of personal and private details and opening attachments. They should also be taught strategies to deal with inappropriate communication and be reminded of the need to write emails clearly and correctly and not include any unsuitable, illegal or abusive material.

d. Staff, volunteers, Governors and all those connected professionally with GFT will not send material that is illegal, obscene, upsetting or defamatory, or that is intended to annoy or intimidate another person. Should such content be received, it must not be forwarded to anyone, and must be reported to the DSL, who will take appropriate action
e. Users should not attempt to send any emails known to contain viruses or be considered as spam or phishing, Trojan and other malicious attachments are a danger to GFT systems
f. Users should be aware that email communications may be monitored

Digital still and video images

a. We gain written parental/carer permission for use of digital photographs or video involving their children as part of the agreement form when their child joins GFT
b. We do not identify students in online photographic materials, or include the full names of students in any published company-produced video materials
c. Staff must not take still or video images of students with their personal mobile phones
d. Digital images/videos of students are stored by staff in a secure, hidden "Student images" folder on the GFT e-drive, which only SLT have access to. All Images are deleted at the end of the contract year (July).

Data security

Refer to GDPR Policy

Mobile phones

a. Staff must take responsibility for their personal mobile phone when they are working with students. These conditions also apply to volunteers
b. Staff mobile phones should only be used using the company Xelion App
c. Staff are not permitted to use their own personal phones or devices for contacting students and their families within or outside of GFT in a professional capacity
    i. The telephone number of GFT using Xelion App should be used by staff in all communication with families, and for emergency contact
    ii. If staff have no option but to use their personal mobile phone for communication with families, they must prefix the dialled number with 141, to hide their own phone number
    iii. All company calls through Xelion will be recorded for training, monitoring and safeguarding purposes

Digital cameras

a. Staff must not use personal devices such as mobile phones or cameras to take photos or videos of students, and will use only work-provided equipment for this purpose;
b. We gain written parental/carer permission for use of digital photographs or video involving their children as part of the agreement form when their child joins;

c. Students can only be photographed with prior written consent from the parents/carers;
d. Personal cameras are not allowed in the setting and should not be used on off-site activities.
e. GFT has digital cameras and mobile tablets for staff and, where appropriate, for students, parents/carers and volunteers to take photographs of students for display, observations or to support evidence of learning
f. Use of video equipment can be a legitimate learning/training aid. students and parents/ carers should be made aware that this could be part of their learning at GFT;
g. Students, volunteers and visitors are not permitted to take photographs or recordings of students without permission from the Managing Director or Department manager without prior written consent from the parents/carers;
h. No one is permitted to photograph or record images in the toilet area.
i. Student images will not be used for promotional or press releases unless parents/carers have given prior written consent.

Internet and social networking sites

a. Internet access at GFT will always be overseen by a member of staff
b. Student access to websites is limited to those agreed by GFT only
c. Staff and volunteers will not intentionally visit internet sites that contain obscene, illegal, hateful or otherwise objectionable materials on GFT equipment
d. Staff must not attempt to bypass or evade GFT's security systems
e. Students will use the internet for educational purposes only
f. GFT will NEVER knowingly disclose or publicise personal information relating to students on any social media platform without explicit consent. Personal information means data which relate to a living individual who can be identified from those data
g. GFT staff will be aware that all internet activity, including records of sites visited, training-related or personal, will be monitored for unusual activity, security and/or network management reasons
h. Staff are instructed not to create or manage social network profiles for student use on a personal basis, or to open up their own personal profiles to their students or the students' families.
i. Staff must not search for, visit or monitor social networking presences of pupils or families.
    1. If a staff member does happen to find such a social network site or presence, they must not enter it. This is uninvited intrusion into a family's life, and you and your employer are liable to investigation if you act outside these guidelines. If you have safeguarding/child protection concerns about a student/young person's behaviour on-line, or if you think a social media platform could provide critical information, for example, if a child is missing or is at risk of harm, raise a concern through "My Concern" the police and children's social care will be contacted by the DSL. If warranted, the only agency that can access these sites is the police.

j. Staff will ensure that in private use:
    1. no reference should be made in social media to students, or parents/carers;
    2. they do not engage in online discussion on personal matters relating to members of GFT staff or its activities in any negative context, and/or actions that may bring an individual, profession or organisation's reputation into disrepute
    3. personal opinions should not be attributed to GFT

GFT Website

a. GFT website will be edited only by an agreed list of named staff. All information placed on the website must adhere to the ethos and values of GFT
b. Personal student information, including home address and contact details, will not be uploaded to the website
c. The website will not publish the surnames of students
d. GFT will ensure that the image files are appropriately named – and do not use students' names in image files if published on the web
e. GFT will ensure the web hosting company has a published security protocol.

Remote Learning Platforms

Due to Covid 19 and the lock down situation the way we interact and teach our students has changed
There are a number of online options that we are now utilising. Ranging from merely setting activities or providing access to online resources, through video tutorials, to interactive video conferencing.
The use of audio and video for real-time online teaching, means we need to consider the following to help safeguard staff and students:

*This policy should be read in conjunction with the **"Remote Learning Guidelines"** document*

Location and Environment

If live video and audio is being used, there should be careful consideration of the location that everyone uses. It is possible that students may be in private spaces or spaces where others are visible, and this may not be appropriate. Staff must ensure they use a conferencing service like ZOOM that you can disable users microphone and video cameras
Staff should also ensure their environment is appropriate for real time online teaching. Staff and students should be dressed appropriately and only use professional language

Behaviour

Staff and students should be clear about the behaviour expectations behaviour (e.g. a 'classroom standard' of behaviour is expected from all participants).
If this is the first time that classes are delivered online, it may take some time in becoming familiar with the new environment

It is worth considering some ground rules at the beginning of each session

- Who can speak and when.
- Respecting others
- The use of the chat box to ask questions
- The use of the hand icon for gaining the tutors attention

Recording

- Staff should follow GFT guidelines for recording video conferences
  - The tutor (host) must be the only person controlling the screen
  - The students should have their microphones and video function switched off on entry until requested to switch on by the tutor
- Staff should always make a note of the conference timing and who participated, including those that arrived/departed early or late.
- Staff should be clear that there should be no external recording of the session
- Staff should make sure that everyone is aware that the session is being recorded.
- Parents/carers should be notified that sessions will be recorded for monitoring and safeguarding purposes
- All recordings will be kept for six months in a digital recording file on the company e-drive. Access will be restricted for safeguarding, monitoring and audit purposes only.

Personal Data

Staff should not include student's personal data to access remote learning platforms. An email address should be set up for learning purposes only

Safeguarding

- All tutoring staff and students should be offered training on remote learning platforms
- Planning for online or distance learning activities should include GFT safeguarding team as part of the planning process.
- Online tuition must follow best practice and be in-line with the GFT's Safeguarding Policy and Remote Leaning Guidelines.
- Staff should be reminded of their safeguarding obligations. Report any safeguarding incidents or potential concerns through "My Concern"
- Remind students of who they can contact for help or support regarding online safeguarding issues

Online bullying

Bullying is defined in guidance issued by the Department of Education as: 'behaviour by an individual or group, repeated over time, that intentionally hurts another individual or group either physically or emotionally'[1]

What is online bullying?

Online bullying is the use of technology, for example mobile phone, email, social networking sites, chat rooms and instant messaging services, to deliberately upset someone else

- It can be used to carry out different types of bullying, as an extension of face-to-face bullying
- It can also go further as it can invade home/personal space and can involve a greater number of people
- It is an anonymous method by which bullies can torment their victims at any time of day or night
- It can draw bystanders into being accessories
- It includes - threats and intimidation; harassment or 'cyber-stalking'; vilification/defamation; exclusion or peer rejection; impersonation; unauthorised publication of private information or images (i.e. possible breach of copyright); and manipulation;
- It includes sexting - sending explicit images electronically. These images can be subsequently widely distributed
- It also includes trolling; the practice of posting upsetting, provocative, offensive, or off-topic messages in an online community. Trolling comments are posted with the deliberate intent of provoking readers into an emotional response, or of otherwise disrupting normal on-topic discussion.

Impact on the victim

The victim may receive email, chat, text messages or posts on social networking sites that make them feel embarrassed, upset, depressed or afraid. This can damage their self-esteem and pose a threat to their psychological wellbeing. Online bullying can pose a serious threat to their physical and emotional safety.

Responding to online bullying

Most cases of online bullying can be dealt with through GFT anti-bullying policies and procedures.

In all cases of online bullying make sure that you preserve the evidence and report through "My Concern"

Some features of online bullying differ from other forms of bullying and may prompt a particular response. For example:

- Consider the bystanders; they can amount to hundreds of people
- Change the victim's mobile phone number
- Report the bullying to the site where it was posted
- Try to get content removed from the web
- In some cases, the victim may be able to block the perpetrator from their sites and services
- Ask the person bullying to remove the offending content and say who they have sent it on to

- Contact the police in cases of actual/suspected illegal content.

What to do if you have concerns about a student:
Staff and volunteers should follow the same procedures as for all other safeguarding issues and adhere to guidelines set out in Keeping Children Safe in Education September 2021 statutory guidance. GFT require all staff to report an online bullying concern on “My Concern” as soon as possible

How we manage allegations against a member of staff:
Staff and volunteers should follow the same procedures as for all other safeguarding issues and adhere to guidelines set out in Keeping Children Safe in Education September 2021 statutory guidance. GFT require staff to follow the Whistleblowing Procedure.

Conclusion

GFT recognises that the use of the technology, including access to the internet and ICT devices, can substantially and positively impact the quality of teaching and learning of our students and staff. This policy aims to ensure that all such use is done safely and appropriately

#

Permission Form

Please review the Online Safety Policy, sign and return this permission form to the Department Manager

Training Provider Name: Gordon Franks Training Ltd (GFT)

Students Name .....

Date: .....

Parent/Guardian
As the parent or legal guardian of the above student, I confirm I have read the Online safety policy and grant permission for my son or daughter or the child in my care to have full access to technology at Gordon Franks Training (GFT) including access to the internet. I understand that internet access is intended for educational purposes only. I also understand that every reasonable precaution has been taken by GFT to provide for online safety but GFT cannot be held responsible if students access unsuitable websites.

I accept the above paragraph ☐ **I do not accept the above paragraph** ☐

(Please tick as appropriate)

(Please tick as appropriate)

Signature: ..... Date:.....

Address: .....

.....

.....

Telephone: .....