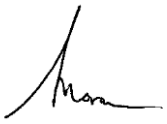
GP Strategies Training Limited

Policies and Procedures
e-Safety Policy

Policy no:	GPSTL-100-OP-26
Revision no:	8.0
Effective date:	13 October 2021
Review frequency	Annual Review
Prepared by:	Sharron Symon
Authorised by:	Dave Martin

Signed by: 

Shay Moran, Senior Vice President

Date: 13 October 2021

GP Strategies Training Limited

e-Safety Policy

1. Aim

General Physics UK Ltd and its Group Companies (hereunder referred to as "The Company") recognise the benefits and opportunities which new technologies offer to teaching and learning. Our aim is to protect our learners, implement safeguards within the Company, and to support staff and learners to identify and manage risks. We aim to achieve this through a combination of security measures, training, guidance and implementation of our associated policies. In support of our wider duty of care to safeguard learners we aim to ensure our learners and staff are equipped with the knowledge and resources to enable them to stay 'e-Safe'.

2. Definition of e-Safety

The term e-Safety is defined for the purposes of this policy as the process of limiting the risk to children, young people and adults at risk when using internet, digital and mobile technologies (IDMTs) through a combined approach to policies and procedures, infrastructures and education, including training underpinned by standards and inspection. e-Safety risks can be summarised under the following three headings.

2.1 Content

- Exposure to inaccurate or misleading information;
- Exposure to socially unacceptable material, such as that inciting violence, hate, extremism, intolerance and radicalisation aligned to our Prevent Duty;
- Exposure to illegal materials such as images of child abuse;
- Illegal downloading of copyright materials e.g. music and films; and
- Exposure to age-inappropriate material.

2.2 Contact

- Grooming using communication technologies, potentially leading to sexual assault and/or child prostitution, or radicalisation; and
- Cyberbullying via websites, social media, mobile phones or other forms of communication devices.

2.3 Commerce

- Exposure of minors to inappropriate commercial advertising;
- Exposure to online gambling services;
- Commercial and financial scams; and
- Identity theft.

3. Scope

This policy applies to all members of staff and learners who have access to the Company IT systems, both on the premises and remotely. Any user of the Company IT systems must adhere to e-Safety rules and the GP-UK-A-02 Electronic Communications Policy. The e-Safety policy applies to all use of the internet, electronic communication devices such as e-mail, mobile phones, games consoles, social networking sites and any other systems that use the internet for connection and providing information.

4. Statement of Intent

- To ensure safeguard on IT-based systems are strong and reliable;
- To ensure the use of IT is safe and appropriate;
- To ensure that the storage and use of images and personal information on Company IT-based systems is secure and meets all legal requirements;

- To educate staff and learners in e-Safety; and
- To ensure any incidents which threaten e-Safety are managed appropriately.

5. Purpose

- To protect the safety and wellbeing of children and young people when adults, young people using the internet, social media or mobile devices;
- To provide staff and volunteers with the overarching principles that guide their approach to online safety;
- To protect GPSTL and their staff from allegations of inappropriate or profligate use;
- To ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices;
- To protect the privacy of staff, learners and other personal information held on the IT system;
- To ensure the integrity of GPSTL's data and the intellectual property rights of the software;
- To ensure the privacy of electronic communications to and from our staff;
- To protect all systems 'stakeholders' from malicious attack, including viruses, offensive and pornographic materials;

The policy statement applies to all staff, volunteers, and young people and anyone involved in GPSTL's activities.

5.1 We will also seek to keep children and young people safe by:

- appointing a DSL responsible for coordinating online safety
- making the DSLs responsible for maintaining a central register of reported referrals supported by chronology records;
- providing clear and specific directions to staff and volunteers on how to behave online through our code of behaviour;
- providing supervision, support and training for staff and volunteers about online safety;
- making certain the Skills Coaches review learner on-line behaviour after each one-to-one session;
- supporting and encouraging the young people using our service to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others;
- developing an online safety agreement for use with young people;
- developing 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;
- 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;
- examining and risk assessing any social media platforms and new technologies before they are used within the organisation.

5.2 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 (including prejudice-based and discriminatory bullying), emotional abuse, sharing of nude and semi-nude images, sexual abuse and exploitation (sexual, criminal or otherwise);
- 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 annually, in order to ensure that any problems have been resolved in the long term.

6. Outcomes

6.1 Security

Company networks are safe and secure with appropriate and up-to-date security measures and software in place.

6.2 Risk Assessment

When making use of new technologies and online platforms, risk assessments are carried out.

6.3 Behaviour

All users of technology adhere to the standards of behaviour set out in this policy and the GP-UK-A-02 Electronic Communications Policy.

Any conduct considered illegal is reported to the police and any abuse of IT systems and any issues of bullying or harassment (cyber-bullying) are dealt with seriously, in line with staff and learner disciplinary procedures.

6.4 Use of Images and Video

The use of images or photographs is encouraged in teaching and learning providing that there is no breach of copyright or other rights of another person, or government legislation.

Staff and learners are trained in the risks of downloading, posting and sharing images and specifically the risk involved in posting personal images onto social networking sites.

Staff provide information to learners of the appropriate use of images and on how to keep their personal information safe.

Advice and approval from a senior manager is sought in specified circumstances or if there is any doubt about the publication of any materials.

6.5 Personal Information

Processing of personal information is carried out in compliance with the Data Protection Act as outlined within the GP-UK-A-03 Data Protection and the GP-UK-A-04 Disclosure Policies.

6.6 Education and Training

Staff and learners are supported through training and education so they can independently develop their skills to identify risk and manage them effectively.

Learning curriculums contain sessions on e-safety and opportunities are taken to reinforce e-Safety messages.

7. Incidents and Response

A clear and effective incident reporting procedure is maintained and communicated to learners and staff. Reports of e-Safety incidents are acted upon by the local/lead safeguarding contacts immediately to prevent, as far as reasonable possible, any harm or further harm occurring.

On identification of any breach of the policy a safeguarding incident form shall be completed and sent to the DSL. Action following the report of an incident might include disciplinary action, sanctions, reports to external agencies, review of internal procedures and safeguarding and tutor or learner support.

Learner web histories are monitored on a daily basis to ensure site visit remain fit for purpose.

GPSTL's web filtering system provides a high level of security by blacking malware, phishing and botnet sites. This protection is applied to all laptops regardless of the network they are connects to and includes home networks and public Wi-Fi.

8. Responsibilities

Whilst is it expected that all staff of the Company will accept personal responsibility for practical application of the policy, lead responsibility for its implementation will rest with the Senior Vice President, the Vice President, Senior Management Team and Lead and Local Nominated Persons responsible for Learner Safeguarding.

9. Policy Access, Monitoring and Review

The policy will be published on the intranet under e-safety and will be reviewed annually or sooner should there be a change in legislation or where an e-Safety incident has been recorded.

10. Referenced Procedures and Documentation

GPSTL-100-OP-26-SF-01 e-Safety incident reporting form
GP-100-OP-18 Safeguarding & Prevent Policy
GP-UK-A-03 Data Protection Policy
GP-UK-06 Grievance Policy
GP-UK-P-07 Discrimination and Anti-harassment Policy
GP-UK-HS-01 Health and Safety Policy
GP-UK-HS-02 General Arrangements for Policy Implementation
GP-100-OP-08 Learner Reviews
GP-UK-A-02 Electronic Communications Use Policy

NSPCC/02 Helpline 0808 800 5002
http://www.o2.co.uk/help/nspcc/child-protection
Child Exploitation and Online Protection Centre (CEOP)
http://www.ceop.police.uk
Childnet - http://www.childnet.com
The UK Safer Internet Centre - http://www.saferinternet.org.uk