E-Safety Policy

Contents

Owner and version control

Document Owners: Neil Gillard, Director of Finance and Operations, Sian Marsh, Director of Early Years and ITT and DSL.

This document must be approved annually by Senior Leadership Team and presented to the Board.

Policy approved by Simon Little MD

Signed 

Date 9th September 2021

Introduction

Best Practice Network recognises the benefits and opportunities that new technologies offer to teaching and learning. We encourage the use of technology in order to enhance skills and promote achievement. However, the accessible and global nature of the internet and the variety of technologies available mean that we are also aware of potential risks and challenges associated with such use.

Our approach is to implement safeguards within the Company and to support staff and learners to identify and manage risks independently. We believe this can be achieved through a combination of security measures, training and guidance and the implementation of our associated policies. In furtherance of our duty to safeguard learners and protect them from the risk posed by extremism and radicalisation, we will do all that we can to make our learners and staff stay safe online and to satisfy our wider duty of care.

This E-Safety policy should be read in conjunction with other relevant Company policies including Safeguarding Policy, IT Acceptable Use Policy, GDPR policy.

Scope

The purpose of this policy statement is to:

- Ensure the safety and wellbeing of learners is paramount when adults, young people and apprentices are using the internet, social media or mobile devices
- Provide staff and associates 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, associates, learners and anyone involved in Best Practice Network's activities.

This policy covers:

- Anyone logging into any network, service, website or portal associated with Best Practice Network
- Connecting a device via the BPN network
- Any electronic communication with a Best Practice Network Learner, member of Staff or associate

Responsibilities

We believe that no member of staff, associate or learner should ever experience abuse of any kind. Everyone should be able to use the internet for education and personal development, but safeguards need

to be in place to ensure they are kept safe at all times. The reporting responsibilities for e-safety follow the same lines of responsibility as the BPN Safeguarding and Child Protection responsibilities.

We will seek to keep staff, associates and learners safe by:

- Providing clear and specific directions to staff, associates and learners on how to behave online
- Supporting and encouraging everyone to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others
- Supporting and encouraging parents and carers of apprentices to do what they can to keep their children safe online
- Developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a young person
- Reviewing and updating the security of our information systems regularly
- Ensuring that usernames, logins, email accounts and passwords are used effectively
- Ensuring personal information about the adults and young people who are involved in our organisation is held securely and shared only as appropriate
- Ensuring that images of children, learners or young people 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 associates about online safety
- Examining and risk assessing any social media platforms and new technologies before they are used within the organisation

Staff and Associate Responsibilities:

- ensuring the safety of learners
- reporting any concerns or disclosures immediately to a Designated Safeguarding Lead (DSL)
- to keep to the terms and conditions of the IT Acceptable Use Policy at all times
- attend staff training on e-safety and always display a model example to learners
- actively promote through embedded good e-safety practice
- always communicate with learners professionally and in line with BPN's Communications Policy.

Staff and associates must never offer assurance of confidentiality everything discussed must be reported.

Learner Responsibilities:

- Adhere to the terms and conditions of the IT Acceptable Use Policy at all times
- Follow appropriate e-safety guidance as part of their programme of study
- Inform a member of staff where they are worried or concerned an e-safety incident has taken place
- Involving them or another member of the company community
- Act safely and responsibly at all times when using the internet and/or mobile technologies

Designated Safeguarding Leads Responsibilities:

- Leading the Safeguarding Committee
- Calling e-safety meetings when required
- Ensuring delivery of staff development and training
- Recording incidents
- Reporting any developments and incidents to the Senior Management Team
- Liaising with the local authority and external agencies to promote e-safety within the Company

BPN IT Department Responsibilities:

- Ensure the Companies IT infrastructure is secure and meets best practice recommendations
- IT security incidents are recorded, investigated and resolved within reasonable a reasonable
- timescale
- report any e-safety concerns or disclosures immediately to a Designated Safeguarding
- Lead (DSL)

Monitoring

Best Practice Network will monitor, log and report on learners and staff use of IT systems and IT network usage as part of the Company's responsibility towards the 'safeguarding of young people and vulnerable adults' and Prevent duty for terrorist and extremist behaviour.

An attempt to interfere or avoid the monitoring or logging of any IT systems will be referred to the Companies disciplinary process.

Where requested this information will be securely shared with appropriate local authorities and external support agencies.

Cyber Security

Best Practice Network IT systems and the Company's Information Security Management System is certified to meet the following Information Security and Cyber Security standards:

- Cyber Essentials Scheme

These standards are regularly reviewed by independent experts providing staff, learners & stakeholders reassurance that Best Practice Network IT systems cyber security follow the highest levels of best practice.

Any breach of the Computer Misuse Act 1990 including all forms of hacking or acquiring / accessing someone else's digital identity is a criminal offence and will be referred to the company's disciplinary procedure and sent to the police for investigation.

Training

Learners:

Learners will be provided with e-safety guidance by their facilitators or tutors and have access to e-safety information. Tutorial planning will include appropriate and relevant e- safety guidance for learners. Tutorial and the programme will also ensure learners consider their digital footprint in both a personal and professional context.

Issues associated with E-safety apply across the curriculum and learners should receive guidance on what precautions and safeguards are appropriate when making use of the internet and mobile technologies. Learners should also know what to do and who to talk to where they have concerns about inappropriate content, either where that material is directed to them, or where it is discovered as part of a random search.

Within taught sessions, learners will be encouraged to question the validity and reliability of materials researched, viewed or downloaded. They will also be encouraged to respect the copyright of other parties and to cite references properly.

Staff

Staff will receive an introductory session for digital learning/working systems and environments within the induction period. This introductory session will signpost the E-Safety Policy and provide an overview for academic staff. Formal agreement to the expectations and terms will be managed by the Human Resources department. Each member of staff must record the date of the training attended on their CPD calendar.

Any new or temporary users will also be asked to sign the company Staff IT Policy.

Behaviour

Use of any Best Practice Network IT equipment and systems is conditional to the Company Policies including the IT Acceptable Use Policy & the Anti-Bullying Harassment Policy and Procedure.

Communications by staff and learners should be always courteous and respectful whether offline or online. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the Anti-Bullying and Harassment Policy.

Cyber Bullying

Cyber bullying is a form of bullying. As it takes place online, it is not confined to company buildings or company hours. Cyber bullies can communicate their messages to a wide audience with speed and often remain anonymous or unidentifiable.

Cyber bullying includes bullying via:

- Text message and messaging apps e.g. sending unwelcome texts or messages that are threatening or cause discomfort
- Picture/video-clips e.g. using mobile device cameras to bully someone, with images usually sent to other people or websites
- Phone call e.g. silent calls or abusive messages. The bully often disguises their number
- Email e.g. emailing upsetting messages, often using a different name for anonymity or using someone else's name to pin the blame on them
- Chat room e.g. sending upsetting responses to people when they are in a web-based chat room
- Instant Messaging (IM) e.g. sending unpleasant messages in real-time conversations on the internet
- Websites e.g. insulting blogs, personal websites, social networking sites and online personal polling sites

Where conduct is found to be unacceptable, the Company will deal with the matter internally and refer to relevant policies, for example, the Disciplinary and Dismissal Policy. Where conduct is considered illegal, the company will report the matter to the police.

Safeguarding and Prevent

All staff and associates should beware of the Companies responsibility of the Prevent Duty and Safeguarding of young people and adults at risk.

The following guidance must be adhered by all staff and associates communicating online:

- Don’t post any personal views, beliefs or opinions

  challenge any personal views, beliefs or opinions posted by learners
- Staff must post with counter arguments to any personal view, beliefs or opinions posted by
- learners which undermines British Values

- Any post considered to isolate or put a young person or vulnerable adult at risk should be referred to a Safeguarding Officer for further investigation
- Any post considered to promote extreme views should be referred to a Safeguarding Officer for
- further investigation

Online Communication

Online communication must:

- Be concise
- Be engaging and use appropriate language
- Use decent-quality images whenever possible
- Use British English, correct spelling and grammar
- Follow the appropriate style and brand guidelines

Appropriate use of online communication.

The appropriate use of communication applies to all devices and services, which might include:

- Computers, Laptops & Mobile devices (including phones and tablets)
- Game Consoles
- Email, Instant / Direct Messages & Chat rooms
- Social Media

All BPN Staff, associates and learners must:

- Not create, store, exchange, display, print or circulate any message or media which may cause offense to others
- Not post or circulate any message which may be considered harassment
- Not send messages at random or excessively, also referred to as "spamming"
- Not post any confidential information to any online platform

Staff must not use personal devices or accounts as a method of communicating with learners and must not give out their personal contact details.

Learner contact details must never be stored on a staff members' personal device(s), including computers, laptops, mobile phones, tables, personal cloud or personal storage devices.

If a post could be considered as representing or being associated to the Company in any way then:

- It is imperative to portray a balanced tone when raising politically sensitive issues
- When linking to websites not controlled by the Best Practice Network Group (such as to relevant news articles) it must be clear that the link is external

Only approved online messaging services can be used to communicate with the BPN network. All communication must be via a Company user account these include

- Email (using a company account)
- Microsoft Teams and Microsoft Office 365 collaboration (using a company account)
- iMessenger (using a Company device and account)
- SMS (using a Company device)

The use of any other communication application including but not limited to SnapChat & WhatsApp are not permitted to communicate with learners.

Social Media

Only employees who have been authorised to use social media accounts may create, maintain, or post on behalf of official Company Group accounts. The use of social media will only be approved where it is deemed to benefit learners and learning, is in the business interests of the Company, and meets safeguarding and PREVENT duties.

Best Practice Network has a number of official social media communications channels, which are part of the Company Group infrastructure. These take priority in externally published documents and materials.

In the event of an incident or emergency involving Best Practice Network no content should be posted to any social media channels except by the Marketing and Communications team who will manage PR centrally

Creating new social media accounts

New social media accounts that use an official logo or a Best Practice Network Group name must not be created unless approved through the social media approval process.

When an administrator leaves the Company Group, their access to BPN social media accounts must be revoked, and the account either handed over to another administrator or closed.

The Company will close down any “unofficial” social media sites using the Company’s logo, name or copyrighted materials, even if created by staff or learners.

Online privacy and personal information

Best Practice Network employees and associates must be aware of their social media presence, particularly when the social media account openly states that they work within the Company Group.

Members of staff are responsible for managing their own social media presence and ensuring that their privacy settings are correct. Staff members are responsible for ensuring that their privacy settings are appropriate for the type of content they share on social media.

Best Practice Network employees, associates and learners are expected to respect the Companies reputation when posting online. Any information which may be considered to be damaging the Companies reputation may result in disciplinary and/or legal action.

Use of the Companies Intellectual Property (IP) must be requested and approved by the Marketing department. Any use of IP without permission may result in disciplinary and/or legal action.

Employees and associates Best Practice Network must maintain professional boundaries at all times, particularly when accepting or inviting 'friend' connections on personal social media accounts.

Employees and associates must not passively or actively connect on social media with current or ex-learners who are under the age of 18 or who have a vulnerability, adults who they support, or any other persons deemed inappropriate by the Designated Safeguarding Leads.

When the social media account uses a passive connection, such as the 'follow' action on Twitter and Instagram, employees must not 'follow' learners under the age of 18.

Useful Links for further Information:

Child Exploitation & Online Protection Centre **http://www.ceop.police.uk/**

Internet Watch Foundation **https://www.iwf.org.uk/**

Get Safe Online **https://www.getsafeonline.org/**

Appendix 1 – Incident Management Process