Policy Number: 555
E-SAFETY, INTERNET AND ACCEPTABLE USE

Table of Contents

1. Policy Aims

This online safety policy has been written by Phoenix involving employees, students and parents/carers, with specialist advice and input as required.

It takes into account the DfE statutory guidance "*Keeping Children Safe in Education*" 2020, the South West Adults Safeguarding Board, Children's Multi Agency Safeguarding Hub (MASH) and Local Authority Designated Officer (LADO) procedures.

The purpose of online safety policy is to:

- Safeguard/protect all members within our services (individual employees and the individuals we support) online.
- Identify approaches to educate regarding online safety throughout the organisation.
- Enable all employees to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns.

Phoenix recognises that the issues classified within online safety are considerable, and that these can be broadly categorised into three areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful material
- **Contact:** being subjected to harmful online interaction with other users
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm

2. Policy Scope

Phoenix recognises that online safety is an essential part of safeguarding and acknowledges the organisations duty to ensure that both those we support and our employees are protected from potential harm online.

The company also acknowledges that the internet and associated access devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life and that those we support should be empowered to build resilience and to develop strategies to manage and respond to the risk/s online.

This policy applies to all employees including but not limited to; governing bodies, managers, teachers, Support Workers, LSAs, bank workers, volunteers. Acceptable usage of IT statement for employees forms part of the GRP527 Code of Conduct policy which all employees should sign during induction.

This policy applies to people we support (inclusive of Young People, Service Users and Learners) in our services. **Appendix 1 of this policy provides an acceptable usage agreement for the individuals we support.**

2.1 Links with other policies and practices

This policy links with several other policies including:

Company

- Colleague Code of Conduct (GRP 527)
- Data Protection (GRP 528)
- Social Media (GRP 536)
- Mobile Phones including Photography and Video (GRP 553)
- Bring Your Own Device (GRP 557)

Oakwood College

- Positive Reinforcing and Behaviour Management (OCC2)
- Safeguarding/Learner Protection (OCC4)
- Counter bullying policies (OCC10)
- Confidentiality (OCC12)

Acorn/Academy

- Counter bullying policies (OCC10)
- Whole School Child Protection & Safeguarding (22)

3. Monitoring and Review

The policy will be revised following any national or local policy requirements, safeguarding protection concerns or any changes to the technical IT infrastructure. Phoenix will ensure regularly monitored internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.

To ensure oversight of online safety, the site Principal/Head Teacher/Registered Manager and Designated Safeguarding Lead/s will be informed of online safety concerns as appropriate.

4. Roles and Responsibilities

Designated Safeguarding Leads are identified in the Group Organisational Chart (accessible to all employees on the "U" drive). All members of staff have important roles and responsibilities to play with regards to online safety.

4.1 The leadership and management team will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a Code of Conduct, which includes acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place.
- Work with IT technical staff to monitor the safety/security of company systems/networks.
- Ensure that online safety is embedded within a progressive curriculum in our educational establishments, which enables all Learners to develop an age-appropriate understanding of online safety.
- Support the Designated Safeguarding Lead by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the Company community to access regarding online safety concerns, including internal, and external support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology whilst auditing and evaluating online safety practice to identify strengths and areas for improvement.
- Ensure all equipment and data is correctly archived when not in use and/or when employee/person we support leaves the organisation

4.2 The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other employees or other agencies, as appropriate.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this to the various services provided by the Company, as appropriate.
- Ensure all employees receive regular, up-to-date and appropriate online safety training.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as *Safer Internet Day*.
- Maintain records of online safety concerns, as well as actions taken, as part of the individual services safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the company response (e.g. policies and procedures).
- Report online safety concerns, as appropriate, to the management teams and Governing body.

4.3 It is the responsibility of all employees to:

- Contribute to the development of online safety policies.
- Read and adhere to all the relevant policies including the online safety policy.
- Take responsibility for the security of IT systems in the manner which used and data accessed.
- Model good practice when using technology and maintain a professional level of conduct in the use of technology, both on and off site.
- Embed online safety education in curriculum delivery (as appropriate).
- Have an awareness of a range of online safety issues and how they may be experienced by the vulnerable individuals in their care.
- Identify online safety concerns and take appropriate action by following the Company's safeguarding policies and procedures.
- Know when and how to escalate online safety issues.
- Take personal responsibility for professional development in this area.
- On leaving the Company handover IT equipment (laptop, phones, chargers, DVDs/CD media) and undertake a data handover

4.4 It is the responsibility of employees managing the technical environment to:

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies/procedures.
- Implement appropriate security measures (including password protection and encryption) to ensure that the Company's IT infrastructure is secure and not open to misuse or malicious attack.
- Ensure that the company's filtering software is applied and updated on a regular basis.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL and leadership team in accordance with the Company's safeguarding procedures.
- Ensure all company equipment on employee termination is returned to IT and checked, cleansed and suitable audit for re-use as applicable.

4.5 It is the responsibility of those we support (at a level that is appropriate to their individual age, ability and vulnerabilities) to:

- Engage in age appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to Acceptable Use Statement (see Appendix 1).
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

4.6 It is the responsibility of parents and (non-Phoenix) carers to:

- Read the Acceptable Use Statement and encourage their children to adhere to it.
- Support the college/school in their online safety approaches by discussing online safety issues with their children and reinforce appropriate, safe online behaviour at home.
- Role model safe and appropriate use of technology and social media.
- Identify change in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the college/school, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

5. Education and Engagement Approaches

5.1 Education and engagement with leaners

Our educational establishments will establish and embed a progressive online safety curriculum throughout the whole college/school, to raise awareness and promote safe and responsible internet use amongst Leaners by:

- Ensuring education regarding safe and responsible IT use is in the curriculum.
- Reinforcing online safety messages whenever technology or the internet is in use.
- Educating Learners in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
- Teaching Learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Our educational establishments will support learners to read and understand in a way which suits their age and ability by:

- Displaying acceptable use posters in all rooms with internet access.
- Informing learners that network and internet use will be monitored for safety and security purposes.
- Rewarding positive use of technology by Learners.
- Seeking student voice when writing and developing college/school online safety policies and practices, including curriculum development and implementation.
- Using support, such as external visitors, where appropriate, to complement and support the college/school internal online safety education.

5.1.1 Vulnerable Learners

Phoenix is aware that some Learners are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to; Children in Care, Learners with Special Educational Needs and Disabilities (SEND) or mental health needs or Learners experiencing trauma.

Phoenix will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable Learners and will seek input from specialist staff as appropriate, including the DSL, ICT Tutor and external agencies where appropriate.

5.2 Training and engagement with employees

The Company will:

- Provide and discuss the online safety policy with all employees as part of induction.
- Provide up-to-date and appropriate online safety training for all employees. This will cover the potential risks posed to vulnerable individuals (e.g. *Content, Contact* and *Conduct*) as well as our professional practice expectations.
- Make employees aware that company systems are monitored and activity can be traced to individual users; employees will be reminded to behave professionally and in accordance with Company policies including the Code of Conduct when accessing company systems and devices.
- Make employees aware that their online conduct outside of work, including personal use of social media, could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which employees should use, according to the age and ability of those in their care.
- Ensure all employees are aware of the procedures to follow regarding online safety concerns affecting those they support and colleagues.

6. Reducing Online Risks

Phoenix recognise that the internet is a constantly changing environment with new 'apps', devices, websites and material emerging at a rapid pace. We will:

- Regularly review the methods used to identify, assess and minimise online risks.
- Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in our college or school is permitted.
- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
- Acknowledge that due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via a company device.
- Ensure all are made aware of the Company's expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments or media which could cause harm, distress or offence to others. This is clearly outlined in education and training approaches.

7. Safer Use of Technology

7.1 Classroom Use

Phoenix uses a wide range of technology. This includes access to:

- Computers, laptops, tablets and other digital devices
- Internet (which may include search engines and educational websites)
- Email
- Games consoles or educational based technologies
- Digital cameras, web cams and video cameras

All company owned devices will be used in accordance with the company's Code of Conduct or Acceptable Use Statement (see Appendix 1) and with appropriate safety and security measures in place.

Employees will always evaluate websites, tools and apps fully before use in the classroom.

Our colleges/schools will use age appropriate search tools, following an informed risk assessment, to identify which tool best suits the needs of our community.

The colleges/schools will ensure that the use of internet-derived materials, by employees and students, complies with copyright law and acknowledge the source of information.

Supervision of Learners will be appropriate to their age and ability.

In order to reduce the risk of unauthorised access or loss of information, Phoenix strives for a clear desk policy as follows:

- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
- Care must be taken to not leave confidential material on printers or photocopiers.
- All business-related printed matter must be disposed of using confidential waste bins or shredded.

- College day students - Students will be appropriately supervised when using technology, according to their ability and understanding.
- Students in residential provision - The college will balance student's ability to take part in age appropriate peer activities online, with the need to detect and prevent abuse, bullying or unsafe practice.

7.2 Managing Internet Access

The company will maintain a record of users who are granted access to the company's devices and systems. All employees will read and sign the Code of Conduct and those individuals we support will sign The Acceptable Use Statement (see Appendix 1) before being given access to any company computer system, IT resources or internet.

The following chart defines Student/Leaner access criteria in Schools

		Acceptable	**Acceptable at certain times**	**Acceptable for nominated users**	**Unacceptable**	**Unacceptable and illegal**
Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on material remarks proposal or comments that relate to;	Child sexual abuse images. The making, production or distribution of indecent images of children. Contrary to the protection of Children Act 1978					X
	Grooming incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003					X
	Possession of extreme pornographic image (grossly offensive, disgusting or otherwise of an absence character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in the UK – to stir up religious hatred (or hatred on the grounds of sexual orientation contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	Threatening behaviour, including promotion of physical violence or				X	

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	mental harm					
	Any other information which maybe offensive to colleagues or breaches the integrity of the ethos of the school/site or brings the service into disrepute.				X	
Using school systems to run a private business					X	
Using systems, applications, website or other mechanisms that bypass the filtering or other safeguards employed by the school/service					X	
Infringing copyright					X	
Revealing or publicising confidential or propriety information (e.g. financial/personal information, databases, computer/network access codes and passwords)					X	
Creating or propagating computer viruses o other harmful files					X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet					X	
On-line gaming (educational)		X				
On-line gaming (non-educational)				X		
On-line gambling						X
On-line shopping commerce					X	
File sharing				X		
Use of Social media					X	
Use of messaging Apps					X	
Use of broadcasting (e.g. You Tube)				X		

7.3 Filtering and Monitoring

The company deploys monitoring software to ensure those we support are not able to access unsuitable sites.

7.3.1 Decision Making

Phoenix operational management and leaders have ensured that our IT system has age and ability appropriate filtering and monitoring in place, to limit vulnerable individuals access and exposure to online risks. The operational management and leaders are aware of the need to prevent “over blocking”, as that may unreasonably restrict what those we support can be taught, with regards to online activities and safeguarding.

The Company's decision regarding filtering and monitoring has been informed by a risk assessment, taking into account our individual services specific needs and circumstances.

Changes to the filtering and monitoring approach will be risk assessed by staff with operational and technical experience and, where appropriate, with consent from the leadership team. The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate. All employees are aware that they cannot rely on filtering and monitoring alone to safeguard Learners; effective classroom management and regular education about safe and responsible use is essential.

7.3.2 Filtering

The company uses broadband connectivity through a WAN network.

The company uses C*ensornet* which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.

Filtering breaches

The company has a clear procedure for reporting filtering breaches;

- If individuals discover unsuitable sites, they will be required to turn off the screen and report to a member of staff immediately.
- The employee will report the concern (including the URL of the site if possible) to the DSL and IT technical staff.
- The breach will be recorded and escalated as appropriate.
- Parents/carers will be informed of filtering breaches involving their child (if appropriate).
- Any material that the college believes is illegal will be reported immediately to the appropriate agencies.

7.3.4 Monitoring

The Company will appropriately monitor internet use on all company owned or provided internet enabled devices. All users are informed that use of company systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

All data that is created and stored on Phoenix IT infrastructure is the property of Phoenix and there is no official provision for individual data privacy.

IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. Phoenix has the right to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.

Any monitoring will be carried out in accordance with audited, controlled internal processes, the UK Data Protection Act 1998, the Regulation of Investigatory Powers Act 2000, Computer Misuse Act 1990 and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000.

7.4 Managing Personal Data Online

Personal data will be recorded, processed, transferred and made available online in accordance with the Data Protection Act 199, Data Protection Bill September 2017 and compliant with General Data Protection Regulation (GDPR) (EU), May 2018.

7.5 Security and Management of Information Systems

The Company takes steps to ensure the security of our information systems, including:

- Virus protection being updated regularly.
- Provision of facilities for encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via secure remote access systems.
- Not using portable media without specific permission.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments.
- Regularly checking files held on the Company network.
- The appropriate use of user logins and passwords to access the Company network.
- All users are expected to log off or lock their screens/devices if systems are unattended.

7.5.1 Password policy

All employees have their own unique username and private passwords to access company systems; employees are responsible for keeping their password private.

From the point of starting the Company will ensure all those we support are provided (where required) with their own unique username and private passwords to access systems; those individuals are responsible for keeping their password private.

All users are required to:

- Use strong passwords for access into our system.
- Allow anyone else to use their user/service ID and password on any Phoenix IT system.
- Leave their user account/s logged in whilst unattended.
- Use someone else's user/service ID and password to access Phoenix 's IT systems.
- Leave their password unprotected (for example writing it down).
- Attempt to access data that they are not authorised to view or process.
- Exceed the limit of their authorisation or specific business need in interrogating the system or specific data.

Access to the Phoenix's IT systems are controlled by the use of user or service IDs and passwords. All user IDs and passwords are to be uniquely assigned to named individuals or a particular service and consequently, individuals are accountable for their interaction with the IT system.

7.6 Managing the Safety of the Company Website

The Company will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright. Employee or personal information related to those we support will not be published on our website; the contact details on the website will be the Head office/College/School address, email and telephone number as appropriate. The administrator account for the Company's website will be secured with an appropriately strong password and changes can only be made via the IT department.

The education services will post appropriate information about safeguarding, including online safety, on the college/school website for stakeholder engagement.

7.7 Publishing Images and Videos Online

The Company will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to): The BOYD, Data Protection, Code of Conduct, Social Media and Use of personal devices and mobile phones.

7.8 Managing Email

Access to company email systems will always take place in accordance with data protection legislation and in line with other company policies, including: Confidentiality and Employee Code of Conduct.

Spam or junk emails are blocked.

Any electronic communication which contains sensitive or personal information should only be sent using secure and encrypted email.

Company email addresses and other official contact details must not be used for setting up personal social media accounts.

Users of Company IT systems must immediately tell the DSL and IT team if they receive offensive communication. Excessive social email use can interfere with teaching and learning in education environments and will be restricted; access to external personal email accounts may be blocked if this interferes with the receipt of education in schools and colleges.

7.8.1 Employees

The use of personal email addresses by employees for any official company business is not permitted. All employees are provided with a bespoke company email address, to use for all official communication. Employees are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between other employees, those we support and/or stakeholders (e.g. parents).

Individuals must not;

- Use the internet or email for the purposes of harassment or abuse.
- Use profanity, obscenities, or derogatory remarks in communications.
- Access, download, send or receive any data (including images), which is offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.
- Use the internet or email to make personal gains or conduct a personal business.
- Use the internet or email to gamble.
- Use the internet to ascertain extremist or terrorist views/activity
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Place any information on the Internet that relates to Phoenix, alter any information about it, or express any opinion about Phoenix, unless they are specifically authorised to do this.
- Send unprotected sensitive or confidential information externally.
- Forward Phoenix business mail to personal (non-Phoenix) email accounts (for example a personal Hotmail account).
- Make official commitments through the internet or email on behalf of Phoenix unless authorised to do so.
- Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.
- Infringe any copyright, database rights, trademarks or other intellectual property.
- Download any software from the internet without prior approval of the IT Department.
- Connect Phoenix devices to the internet using non-standard connections.
- Intentionally interfere with the normal operation of the Internet or computer operation.
- Process large amounts of data causing a sustained high volume of network traffic.
- Use the internet or email to investigate violence or bomb making activity
- Undertake any form of criminal activity

7.8.2 Learners

Learners will use Phoenix provided email accounts for educational purposes (if required). Learners will sign an Accessible Use Statement (Appendix 1) and will receive education regarding safe and appropriate email etiquette before access is permitted.

7.9 Educational use of Webcams

Phoenix recognises that the use of webcams can be a challenging activity but brings a wide range of learning benefits.

7.9.1 Content

When recording a videoconference lesson, it should be made clear to all parties at the start of the conference and written permission will be obtained from all participants; the reason for the recording must be given and recorded material will be stored securely. If third party materials are included, the company will check that recording is permitted to avoid infringing the third

party intellectual property rights. The company will establish dialogue with other conference participants before taking part in a videoconference.

7.10 Management of Applications (apps) used to Record Learner's Progress

The college (for example) uses APPs and TAPs to track students' progress and share appropriate information with parents and carers. The Headteacher/Principal is ultimately responsible for the security of any data or images held of Learners.

In order to safeguard Learner's data:

- Only Company issued devices will be used for apps that record and store Learner's personal details, attainment or photographs.
- Company devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
- All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
- Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

8. Social Media

8.1 Expectations

The expectations' regarding safe and responsible use of social media applies to all members of the Phoenix community. The term social media may include (but is not limited to): blogs; wikis; social networking sites; Facebook; Twitter; Instagram; forums; bulletin boards; video/photo sharing sites; chatrooms and instant messenger. All employees are expected to engage in social media in a positive, safe and responsible manner, at all times.

All members of the Phoenix community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others or in any way addresses the nature of the Company.

The use of social media during college/school/working hours for personal use **is not** permitted. Inappropriate or excessive use of social media during college/work hours or whilst using college devices may result in disciplinary and/or removal of internet facilities. Concerns regarding the online conduct of any employee on social media, should be reported to the DSL and will be managed in accordance with company policies.

8.2 Employee Personal Use of Social Media

The safe and responsible use of social networking, social media will be discussed with all employees as part of their induction and will be revisited and communicated via regular

employee training opportunities. Safe and professional behaviour will be outlined for all employees as part of the Code of Conduct.

Reputation

All employees are advised that their online conduct on social media can have an impact on their role and reputation within the Company. Disciplinary action may be taken if they are found to bring the company into disrepute, or if something is felt to have undermined confidence in their professional abilities. Employees are encouraged not to identify themselves as employees of Phoenix on their personal social networking accounts. This is to prevent information on these sites from being linked with the company and also to safeguard the privacy of other employees.

All employees are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with company policies and the wider professional and legal framework. Information and content that employees have access to as part of their employment, including photos and personal information about students and their family members or colleagues will not be shared or discussed on social media sites.

Employees will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role in the Company.

Communicating with students and parents and carers

All employees must NOT communicate with or add as 'friends' any current or past individuals we have supported or their family members via any personal social media site. Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead.

If ongoing contact with individuals is required once they have left our support, employees will be expected to use existing alumni networks or official communication tools/social media accounts.

Any communication from individuals we have previously supported or their families received on personal social media accounts will be reported to the respective Designated Safeguarding Lead.

8.3 Students' Personal Use of Social Media

Safe and appropriate use of social media will be taught to students as part of an embedded and progressive education approach, via age appropriate sites and resources. Any concerns regarding students' use of social media, both at home and at college/school, will be dealt with in accordance with existing company policies. Concerns will also be raised with parents/carers as appropriate.

Students will be advised:

- To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location. Examples would include name, address, mobile or telephone numbers, college/school attended, email addresses, full names of friends/family, specific interests and clubs.
- To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
- Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
- To use safe passwords.
- To use social media sites which are appropriate for their age and abilities.
- How to block and report unwanted communications and report concerns both within college/school and externally.

8.4 Official Use of Social Media

Phoenix official social media channels are; Twitter; Facebook; YouTube and Linked In. The official use of social media sites, by the Company, only takes place with clear educational or community engagement objectives. The official use of social media as a communication tool has been formally risk assessed and approved by the Company. Nominated individuals have access to account information and login details for the social media accounts.

Employee expectations

If nominated employees are participating in online social media activity as part of their capacity as an employee of the company, they will:

- Be professional at all times and aware that they are an ambassador for the company.
- Be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
- Always act within the legal frameworks they would adhere to within the workplace, including: libel, defamation, confidentiality, copyright, data protection and equalities laws.
- Ensure that they have appropriate written consent before posting images on the official social media channel.
- Not disclose information, make commitments or engage in activities on behalf of the company unless they are authorised to do so.
- Not engage with any direct or private messaging with current, or past individuals we have supported.
- Inform their line manager and the Designated Safeguarding Lead of any concerns, such as criticism, inappropriate content or contact from those we support.

9. Use of Personal Devices and Mobile Phones

Phoenix recognises that personal communication through mobile technologies is an accepted part of everyday life for students, staff and parents/carers, but technologies need to be used safely and appropriately within the company.

9.1 Expectations

All use of personal devices and mobile phones will take place in accordance with the law and other appropriate company policies, including, but not limited to: Anti-bullying, Behaviour and safeguarding protection. Electronic devices of any kind that are brought onto site are the responsibility of the user at all times.

All employees are advised to take steps to protect their mobile phones or devices from loss, theft or damage; the company accepts no responsibility for the loss, theft or damage of such items on company premises.

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- Equipment and media taken off-site must not be left unattended in public places and not left in line of sight of a potential theft.
- Laptops must be carried as hand luggage when travelling.
- Data should be protected against loss or compromise when working remotely
- Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN.

The sending of abusive or inappropriate messages via mobile phones is forbidden by any employee; any breaches will be dealt with as part of the Code of Conduct policy.

All employees are advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the company's Code of Conduct.

Individuals must not:

- Use Phoenix's telephones for conducting private business.
- Make hoax or threatening calls to internal or external destinations.
- Accept reverse charge calls from domestic or International operators, unless it is for business use and cannot be avoided.

9.2 Employee Use of Personal Devices/Mobile Phones

Employees will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant company policy and procedures, such as: Confidentiality, Safeguarding, Data Protection and Acceptable use.

Employees will be advised to:

- Keep mobile phones and personal devices in a safe and secure place.
- Keep mobile phones and personal devices switched off or switched to 'silent' mode.
- Ensure that Bluetooth or other forms of communication are hidden or disabled during lesson times.
- Not use personal devices during teaching periods, unless permission has been given by the Head Teacher/Principal, such as in emergency circumstances.
- Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.

Employees are not permitted to use their own personal phones or devices for contacting students or parents. Any pre-existing relationships, which could undermine this, will be discussed with the Designated Safeguarding Lead and or principal.

Employees will not use personal devices to take photos/videos of students.

If an employee is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

9.3 Students' Use of Personal Devices and Mobile Phones

Students will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences. If a student needs to contact his/her parents or carers they will be allowed to use a company phone.

Parents are advised to contact their child via appropriate means. Exceptions may be permitted on a case-by-case basis.

Mobile phones or personal devices will not be used by students during lessons or formal school/college time unless as part of an approved and directed curriculum based activity with consent from a member of staff.

Mobile phones and personal devices must not be taken into examinations. Students found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.

If a student breaches the company policy, the may be confiscated and will be held in a secure place for later collection. Company staff may confiscate a student's mobile phone or device if they believe it is being used to contravene the college's Behaviour or Bullying policy, or could contain youth produced sexual imagery (sexting).

Searches of mobile phone or personal devices will only be carried out in accordance with the college's policy. www.gov.uk/government/publications/searching-screening-and-confiscation)

Students' mobile phones or devices may be searched by a member of the leadership team, with the consent of the student or a parent/ carer. Mobile phones and devices that have been confiscated will be released to parents or carers If there is suspicion that material on a student's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

9.4 Visitors' Use of Personal Devices and Mobile Phones

Employees are expected to challenge visitors if they have concerns over their use of personal devices and will always inform the Designated Safeguarding Lead or Head Teacher/Registered Manager/Principal of any breaches of company policies.

10. Responding to On-line Safety Incidents and Concerns

All employees will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.

All employee must respect confidentiality and the need to follow the official Company procedures for reporting concerns.

The company requires staff, parents, carers and students to work in partnership to resolve online safety issues. After any investigations are completed, the Company will debrief, identify lessons learnt and implement any policy or curriculum changes as required. If the company is unsure how to proceed with an incident or concern, the DSL will seek advice from the Education and Local Authority Safeguarding Team.

Where there is suspicion that illegal activity has taken place, the Company will contact the Education and Local Authority Safeguarding Team or the Police using 999 if there is immediate danger or risk of harm. If an incident or concern needs to be passed beyond the Company environment (for example if other local Colleges are involved or the public may be at risk), the Company will speak with the Police and/or the Local Authority Safeguarding Team first, to ensure that potential investigations are not compromised.

10.1 Concerns about Students Welfare

The DSL will be informed of any online safety incidents involving safeguarding or child protection concerns. The DSL will record these issues in line with the company's child protection policy. The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Adult Safeguarding Team, Children's Multi Agency Safeguarding Hub (MASH) and procedures.

The company will inform parents and carers of any incidents or concerns involving their child, as and when required. The company will inform all placing Local Authority commissioners and Social Workers, as and when required.

10.2 Employee Misuse

Any complaint about employee misuse will be referred to the DSL. Appropriate action will be taken in accordance with the Code of Conduct.

11. Procedures for Responding to Specific Online Incidents or Concerns

11.1 Youth Produced Sexual Imagery or "Sexting"

Phoenix recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; therefore all concerns will be reported to and dealt with by the Designated Safeguarding Lead. The company will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and KSCB guidance: "Responding to youth produced sexual imagery".

Phoenix will ensure that all employees are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods. The company will ensure that all employees are aware of sources of support regarding youth produced sexual imagery.

11.1.1 Dealing with 'Sexting'

If the company is made aware of an incident involving the creation or distribution of youth produced sexual imagery, the company will:

- Act in accordance with our Child protection and Safeguarding policies and the relevant Safeguarding Board's procedures.
- Immediately notify the Designated Safeguarding Lead.
- Store the device securely. If an indecent image has been taken or shared on the college network or devices, the company will take action to block access to all users and isolate the image.
- Carry out a risk assessment which considers any vulnerability of student(s) involved; including carrying out relevant checks with other agencies.
- Inform parents and carers, if appropriate, about the incident and how it is being managed.
- Inform student social workers and Local Authority placing commissioners, if appropriate, about the incident and how it is being managed.
- Make a referral to Specialist Children's Services and/or the Police, as appropriate.
- Provide the necessary safeguards and support for students, such as offering counselling or pastoral support.
- Implement appropriate sanctions in accordance with the college's Behaviour policy, but taking care not to further traumatise victims where possible.
- Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance. Images will only be deleted once the college has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
    - Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

- The company will take action regarding youth produced sexual imagery, regardless of whether the incident took place on/off college premises, using college or personal equipment.
  - The company will not:
    - View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so. In this case, the image will only be viewed by the Designated Safeguarding Lead and their justification for viewing the image will be clearly documented.
    - Send, share, save or make copies of content suspected to be an indecent image of children (i.e. youth produced sexual imagery).

11.2 Online Child Sexual Abuse and Exploitation

Phoenix will ensure that all employees are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns. Phoenix recognises online child sexual abuse as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the Designated Safeguarding Lead. The company will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate education for students, staff and parents/carers. The company will ensure that all employees are aware of the support available regarding online child sexual abuse, both locally and nationally.

11.2. 1 Dealing with Online Child Sexual Abuse and Exploitation

If the Company is aware of incident involving online sexual abuse of a vulnerable individual we will:

- Act in accordance with the appropriate Child Protection and Safeguarding policies and the relevant Safeguarding Board's procedures.
- Immediately notify the Designated Safeguarding Lead.
- Store any devices involved - securely.
- Immediately inform the police via 101 (or 999 if a vulnerable individual is at immediate risk)
- Carry out a risk assessment which considers any vulnerabilities of individuals involved (including carrying out relevant checks with other agencies).
- Inform parents/carers about the incident if appropriate and how it is being managed.
- Make a referral to Specialist Children's Services (if required/ appropriate).
- Provide the necessary safeguards and support for students, such as, offering counselling or pastoral support.
- Review the handling of any incidents to ensure that best practice is implemented; college leadership team will review and update any management procedures, where necessary.

The college will take action regarding online child sexual abuse, regardless of whether the incident took place on/off college premises, using college or personal equipment.

If the company is unclear whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through the Safeguarding Team and/or Police.

11.3 Indecent Images of Children (IIOC)

Phoenix will ensure that all employees are made aware of the possible consequences of accessing Indecent Images of Children (IIOC). The company will take action regarding IIOC on college equipment and/or personal equipment, even if access took place off site. If the company is unclear if a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through Devon Police and/or the Safeguarding Team.

If made aware of IIOC, the company will:

- Act in accordance with the company's child protection and safeguarding policy and the relevant Safeguarding Boards procedures.
- Immediately notify the Designated Safeguard Lead.
- Store any devices involved securely.

If made aware that a employee or a learner has been inadvertently exposed to indecent images of children whilst using the internet, the company will:

- Ensure that the Designated Safeguard Lead is informed.
- Ensure that any copies that exist of the image, for example in emails, are quarantined.
- Report concerns, as appropriate to parents and carers.

If made aware that indecent images of children have been found on the company devices, the company will:

- Ensure that the Designated Safeguard Lead is informed.
- Ensure that any copies that exist of the image, for example in emails, are quarantined.
- Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
- Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
- Report concerns, as appropriate to parents and carers.

If made aware that an employee is in possession of indecent images of children on Company devices, the Company will:

- Ensure that the Headteacher/Principal is informed.
- Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the Company's managing allegations policy.
- Quarantine any devices until police advice has been sought.

11.4 Cyberbullying

Cyberbullying, along with all other forms of bullying, will not be tolerated within Phoenix. Full details of how the company will respond to cyberbullying are set out in the Counter Bullying policy.

11.5 Online Hate

Online hate content, directed towards or posted by specific employees will not be tolerated at Phoenix and will be responded to in line with existing Company policies. All employees will be advised to report online hate in accordance with relevant Company policies and procedures.

If the company is unclear on how to respond, or whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice through the Safeguarding Team and/or the local Police.

11.6 Online Radicalisation and Extremism

The company will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in our services.

If the company is concerned that a child or parent/carer may be at risk of radicalisation online, the Designated Safeguarding Lead will be informed immediately and action will be taken in line with the safeguarding protection policy.

Prevent Training is available to employees.

12. Useful Links

Devon Support and Guidance

MASH
Worried about a child's safety?
If you are concerned about a child or young person in Devon and want to speak to someone contact our Multi-Agency Safeguarding Hub (MASH) on 0345 155 1071 or
email mashsecure@devon.gcsx.gov.uk and give as much information as you can.

If a child is at immediate risk contact the police on 999.

The following organisations can also offer advice and information if you are concerned about a child:

- Devon Children and Families Partnership
- NSPCC – Help and advice
- Childline
- REACH – is a specialist service in Devon which supports young people up to 17 years old, who either run away or who may be at risk of, or experiencing child sexual exploitation (CSE)

Peninsula Safeguarding Adults Boards:

- Cornwall & Isles of Scilly Safeguarding Adults Board
- Plymouth Safeguarding Adults Board
- Torbay Safeguarding Adults Board

Devon and Cornwall Police:

- www.devon-cornwall.police.uk or https://www.devon-cornwall.police.uk/advice/your-internet-safety/
- In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Devon Police via 101

National Links and Resources

- Action Fraud: www.actionfraud.police.uk
- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org

- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
  - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for colleges: www.360safe.org.uk
- Dignity in Care network: www.dignityincare.org.uk
- Victim Support: www.victimsupport.org.uk
- Devon Domestic Violence and Abuse: www.devon.gov.uk/index/childrenfamilies/domestic_violence.htm
- Child Exploitation and Online Protection centre - report concerns to CEOP via the "Click CEOP" button
- Virtual Global Taskforce - making the internet safer for children
- Think U Know - advice for parents, teachers and young people and teaching resources
- Internet Watch Foundation - report illegal content online
- Action Fraud - report consumer and online fraud
- Parent Port - Site for parents to report inappropriate content (on and offline)
- Childline - NSPCC Childline Service
- Revenge Porn Helpline (NB if under 18s are involved report to CEOP or Devon Police)
- Stop Online Abuse - Report online sexism, homophobia, biphobia and transphobia
- Parent Port - Report inappropriate content (on and offline)
- Professionals Online Safety Helpline for professionals who work with children and young people in the UK, specifically tackling online safety concerns: helpline@saferinternet.org.uk or 0844 381 4772

Charities and support services

- Anti-Bullying Alliance
- NSPCC Online Safety
- The Marie Collins Foundation - helping children abused online
- The Lucy Faithfull Foundation - Advice, self-help and educational programmes about online abuse (including peer on peer abuse)
- Digital Trust - Advice regarding online stalking and harassment
- The Samaritans: Supporting Colleges
- Papyrus - Prevention of young suicide
- Young Minds

General

- Safer Internet Day
- 360 safe self-review tool - interactive tool from the SWGfL to help colleges to review their online safety provision and to develop an action plan
- Ofcom - Ofcom frequently post research into online safety
- EU Kids Online - Research

- Research summaries via the online safety blog

Online safety resources from other Authorities or Grids

- South West Grid For Learning

UK Safer Internet Centre:

- Advice Centre: Teachers and college staff
- Advice Centre: Governors and Trustees
- Professional Reputation
- Professional Online Safety Helpline

Useful links for parents and carers

The following content will be helpful to share with parents and carers. They may contain helpful preventative resources, useful guides and leaflets for families as well as advice for dealing with specific issues and concerns.

- Think U Know - Information from CEOP about online abuse and exploitation
- Internet Matters - Information from BT, Sky, Talk Talk and Virgin
    - Digital resilience toolkits
    - Leaflets
    - What the experts say
- Childnet - Information for parents and carers
    - Family agreements and conversation starters
    - Supporting Young People Online Leaflets
    - Keeping under fives safe online Leaflets
    - Music, TV, Film and the Internet Leaflets
    - Parents resource sheet
    - Screen time boundaries
- UK Safer Internet Centre parents advice
- The Parent Zone - guidance for parents and professionals working with families
- Parent Info - Excellent resource to include on college and setting websites
- NSPCC Online Safety - NSPCC Online Safety advice
    - O2 and NSPCC
    - Talking to your child -
- Barnardo's Follow me
- Barnardo's Be Safe guide for parents and children about sexual exploitation
- Parents Protect - Lucy Faithfull Foundation
- Get Safe Online
- Family Online Safety Institute (FOSI)
- Vodafone Digital Parenting
- EE Digital Living resources - for colleges and parents and carers
- NWG and UK Safer Internet Centre leaflet: Online: Onguard - A Guide to Becoming a Safer Parent Online -

Review Sites and Social Media Guides

- Net Aware - NSPCC reviews of 50+ popular apps and games
- Internet Matters - Safe set up guides (includes popular social media sites)
- Common Sense Media - American site which reviews websites, games etc with age suitability
- UK Safer Internet Centre
- Think U Know
- Webwise.ie
- Parents Guide to Games

Gaming and online video content

- Ask About Games - advice on computer gaming and parental controls
- Pegi - information about games rating
- Safer Internet Centre Gaming Resources
- NSPCC Online Games
- Parents Guide to Games
- Internet Matters - safe set up guides for gaming devices
- BBFC

Technical Tips and Parental Controls

- UK Safer Internet Centre: Parents guide to new technology - links and tips about popular device
- UK Safer Internet Centre: Parents guide to parental controls
- Internet Matters - Information from BT, Sky, Talk Talk and Virgin
- Internet Matters - Safe set up guides for devices and social media apps
- NSPCC Parental Controls
- Yahoo Safety Tips
- Google Safety Center - includes family safety
- How Computers Work
- NetLingo - common online acronyms and text speak e.g. LOL, POS
- Staying safe online: parental controls on broadband

APPENDIX 1 Acceptable Usage Agreement

Learner, Student Service User, Young Person IT Acceptable Use Agreement

1. I will only use computer systems in school/home, including the internet, e-mail, digital video, mobile technologies, etc. for school or legitimate purposes.

2. I will not harm or destroy equipment in school, this includes headphones and other ancillary devices.

3. I will never encourage others to send rude or abusive messages

4. I will not put viruses or anything harmful onto school computers.

5. If I discover an unsuitable site, r if something makes me uncomfortable, I will switch off the screen immediately and tell my Teacher, Support Worker or other responsible Individual.

6. I will not invite any Phoenix employee to become a friend on social networking or similar sites.

7. I will not download or install software.

8. I will only log on to the computer with my own user name and password.

9. I will not reveal my passwords to anyone, and I will change them regularly.

10. I will only use my designated e-mail address (if applicable) when given.

11. I will make sure that all digital communications with other students, teachers or others is responsible, appropriate, inoffensive and sensible. This includes both inside and outside of school/home and includes all electronic communication such as social networking, twitter, video broadcasting, texting etc.

12. If I feel bullied online then I know it is important to tell someone and not to suffer in silence. I also know there are websites and organisations I can get further help.

13. I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use. I will only use appropriate and polite language. I will not use language that might offend other people in any way. This includes language about race, culture, belief, gender or disability.

14. I will not deliberately browse, download, upload or forward material that could be considered offensive, extremist, terrorist or illegal.

15. I will not give out any personal information such as name, phone number, birthday, property address or email address. I will not arrange to meet someone unless this is part of an approved project.

Continued/…

16. I must seek permission before I take, store, and distribute images, audio or videos. These digital recordings must never be of an inappropriate or offensive nature. If asked to delete any digital recordings I will do some from all media.

17. I will ensure that my online activity will not cause my school, the Phoenix employees or others distress or bring Phoenix into disrepute.

18. I will support the Phoenix approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community

19. I will always respect the privacy and ownership of others' work on-line.

20. I will not attempt to bypass the internet filtering system.

21. I will respect Copyright not bring any illegal content, including pirated songs, movies, software, offensive material and will not share or distribute it further.

22. I understand that all my use of the Internet, content of emails and other related technologies can be monitored and logged, and content can be made available.

23. I will change my password if I think someone else knows it.

Additional Notes on the above/changes applicable to an individual person signing this form.

I understand that these rules are designed to keep me safe and that if they are not followed, consequences may be applied (including referral to the police).

Young Person, Learner, Student, Teacher or other staff member signature

We have discussed this document and the following agrees to follow the eSafety rules and to support the safe and responsible use of ICT.

Individual's Name : Printed block capitals

Signature :

Employee Name : Printed block capitals

Signature :

Date :