Development/Monitoring /Review of this Policy

This e-safety policy has been developed in consultation with the following stakeholders:

- Learners
- Staff
- Safeguarding Officers
- Board of Trustees

Schedule for Development / Monitoring / Review

The implementation of this e-safety policy will be monitored by the Operations Director

Monitoring will take place at regular intervals: Annually or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.

Should serious e-safety incidents take place, the following persons / external agencies should be informed:

- Managing Director
- Operations Director
- Safeguarding Designated Officers
- LA Safeguarding Officer
- Police (if applicable)

Appris will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys/questionnaires and feedback from learners

Scope of the Policy

This policy applies to all employees of Appris and learners who have access to and are users of the Appris ICT systems, both internally and remotely.

Appris will deal with misuse of resources within this policy and will, where known, inform employers and parents of incidents of inappropriate e-safety behaviour that take place.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within Appris:

Board of Trustees/Directors

Directors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Trustees receiving regular information about e-safety incidents and monitoring reports:

The Directors have a duty of care for ensuring the safety (including e-safety) of Appris staff and learners, through the day to day responsibility for e-safety will be delegated to the Managing Director.

The Managing Director and Operations Director should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

The Managing Director is responsible for ensuring that staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

The Managing Director will ensure that there is a system in place to allow for monitoring and support of those on site who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

External ICT provider

Appris has a managed ICT service provided by an outside contractor, it is the responsibility of Appris to ensure that the managed service provider carries out all the e-safety measures that would otherwise be the responsibility of Appris.

The external ICT provider is responsible for ensuring:

- that Appris' technical infrastructure is secure and is not open to misuse or malicious attack
- that users may only access the networks and devices through a properly enforced password protection policy.
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to a Director for investigation / action / sanction

Delivery and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to a Director for investigation / action / sanction
- all digital communications with learners should be on a professional level and only carried out using official systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- learners understand and follow the e-safety and acceptable use policies (see agreement form)
- learners have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned, learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Learners

Whilst regulation and technical solutions are very important, their use must be balanced by educating learners to take a responsible approach. The education of learners in e-safety is therefore an essential part of Appris' e-safety provision. Young people need the help and support of Appris to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- Key e-safety messages should be reinforced as part of a planned programme of learning
- Learners should be taught in all sessions to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.

- Learners should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Learners should be helped to understand the need for the Learner Acceptable Use Agreement and encouraged to adopt safe and responsible use.
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where learners are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

Staff
It is essential that all staff understand their responsibilities, as outlined in this policy, including:

- Existing staff are fully aware of the Appris e-safety policy and Acceptable Use Agreements at point of implementing the policy
- All new staff should ensure that they fully understand Appris e-safety policy and Acceptable Use Agreements at point of induction

Use of digital and video images
The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff and learners need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

It is common for employers to carry out internet searches for information about potential and existing employees. Appris will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Staff are allowed to take digital / video images to support educational aims. Those images should only be taken on Appris equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that learners are appropriately dressed and are not participating in activities that might bring the individuals or Appris into disrepute.
- Learners must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with good practice guidance on the use of such images.
- For learners under 18, written permission from parents or carers will be obtained before photographs of learners are published on Appris website

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Prevent Duty

The Counter-Terrorism and Security Bill, seeks to place a duty on specified authorities to 'have due regard, in the exercise of its functions, to the need to prevent people from being drawn into terrorism'. Preventing people becoming terrorists or supporting terrorism also requires challenge to extremist ideas where they are used to legitimise terrorism and are shared by terrorist groups. Appris are identified as a specified authority as they are in the Further Education sector.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how Appris currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

Communication Technology	**Staff & Other Adults**			**Training Centre Learners**			
	Allowed	**Allowed at certain times**	**Allowed for selected staff**	**Not allowed**	**Allowed**	**Allowed at certain times**	**Allowed with staff permission**
Mobile phones may be brought on site	✓				✓		
Use of mobile phones in lessons	✓			✓			
Use of mobile phones in social time	✓				✓		
Taking photos on mobile phones/ cameras			✓	✓			
Use of other mobile devices eg tablets, gaming devices			✓	✓			
Accessing personal email addresses	✓						✓
Use of messaging apps	✓					✓	
Use of social media	✓					✓	

When using communication technologies Appris considers the following as good practice:

- The 'info' email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff should therefore use only Appris email service to communicate with others.
- Users must immediately report, to the Operations Director – in accordance with Appris policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and learners must be professional in tone and content. These communications may only take place on official systems. Personal email addresses, text messaging or social media must not be used for these communications.

- Learners should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on Appris website and only official email addresses should be used to identify members of staff.

Use of Biometric Systems

It should be noted that no complete images of fingerprints / palms are stored and the original image cannot be reconstructed from the data. That is, it is not possible for example, to recreate a fingerprint or even the image of a fingerprint from what is in effect a string of numbers.

Social Media - Protecting Professional Identity

Appris ensures reasonable steps are in place to minimise risk of harm to learners, staff and Appris through limiting access to personal information and clear reporting guidance, including responsibilities, procedures and sanctions.

Staff should ensure that:

- They do not engage in online discussion on personal matters relating to learners
- Personal opinions should not be attributed to Appris
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Appris' use of social media for professional purposes will be checked regularly by the Directors to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video good practice.

Unsuitable / inappropriate activities

Some internet activity eg accessing child abuse images or distributing racist material is illegal and would obviously be banned from Appris and all other technical systems. Other activities eg cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate, either because of the age of the users or the nature of those activities.

Appris believes that the activities referred to in the following section would be inappropriate and that users, as defined below, should not engage in these activities when using Appris equipment or systems. Appris policy restricts usage as follows:

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978
- Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.
- Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008

- criminally racist or fundamentalist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) or acts of terrorism - contrary to the Public Order Act 1986 and the Counter-Terrorism and Security Bill.
- pornography
- promotion of any kind of discrimination
- threatening behaviour, including promotion of physical violence or mental harm
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of Appris or brings Appris into disrepute
- Using Appris systems to run a private business
- Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards deployed by Appris
- Infringing copyright
- Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Unfair usage (downloading / uploading large files that hinders others in their use of the internet)
- On-line gaming or gambling
- On-line shopping / commerce
- File sharing
- Use of social media
- Use of messaging apps
- Use of video broadcasting eg Youtube

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

Illegal Incidents
If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, this should be referred to a Director for responding to online safety incidents and report immediately to the police.

Other Incidents
It is hoped that all parties will be responsible users of digital technologies, who understand and follow the policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)

Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

- Internal response or discipline procedures
- Police involvement and/or action
- if content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - criminally racist or fundamentalist material
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for Appris and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

Actions & Sanctions

It is more likely that Appris will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that all parties are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal student behaviour or staff disciplinary procedures.

Acceptable Use Policy Agreement for Learners and Visitors

I understand that I must use the ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that Appris will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it (including online or via mobile devices).

I understand that everyone has equal rights to use technology as a resource and:

- I understand that Appris systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use Appris' systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that Appris has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of Appris:

- I will only use my own personal devices (mobile phones / USB devices etc) if I have permission. I understand that, if I do use my own devices in Appris, I will follow the rules set out in this agreement, in the same way as if I was using Appris' equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any device, nor will I try to alter computer settings.

- I will only use social media sites with permission and at the times that are allowed.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download copies.
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of the learning environment:

- I understand that Appris also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement (examples being cyber-bullying, accessing criminally racist or fundamentalist material, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to Appris network / internet and in the event of illegal activities involvement of the police.

I confirm that I have read and understand the above and agree to follow these guidelines when:

- I use Appris systems and devices
- I use my own devices in Appris (when allowed) eg mobile phones, USB devices, cameras etc

Name of Learner/Visitor:	
Signed:	
Date:	

Acceptable Use Policy Agreement for Staff

I understand that I must use the ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that learners receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that Appris will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of ICT systems (eg laptops, email, VLE etc) out of office and to the transfer of personal data.
- I understand that Appris ICT systems are primarily intended for work use and that I will only use the systems for personal or recreational use within the policies and rules set down by Appris.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using Appris ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with this policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so.
- I will only use chat and social networking sites in accordance with this policies.
- I will only communicate with learners and employers using official systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

Appris has the responsibility to provide safe and secure access to technologies and ensure the smooth running of Appris:

- I will not use personal email addresses on Appris ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist or fundamentalist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer.
- I will not disable or cause any damage to equipment, or the equipment belonging to others.

- I understand that data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by the policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that I am responsible for my actions in and out of Appris:
- I understand that this Acceptable Use Policy applies not only to my work but also applies to my use of ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by Appris.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include, where applicable referral to the Police in the event of illegal activities.

I have read and understand the above and agree to use Appris ICT systems (both in and out of work) and my own devices within these guidelines.

Name of Staff:	
Signed:	
Date:	

Record of reviewing devices / internet sites (responding to incidents of misuse)

Date:	
Reason for investigation:	

Details of first reviewing person

Name:	
Position	
Signature	

Details of second reviewing person

Name:	
Position	
Signature	

Name and location of computer used for review (for web sites)

Web site(s) address / device	Reason for concern

Conclusion and Action proposed or taken

Reporting Log

Date	Time	Incident	Action taken		Incident Reported by
			What?	By whom?	