MRG Services UK Limited

E-SAFETY POLICY 2018-19

Ref No:	PL73	Originator:	Angie Boyes
Section:	2 - HR	ISO Ref:	4.2.3.73
Date:	24/08/2018	Approved:	Paul Gray
Revision:	1.0	Page:	Page **1** of **25**

Contents:

1.0 Scope of the Policy

1.1 This policy applies to all members of MRG Services UK Limited (including staff, learners, volunteers, parents/carers, visitors, community users) who have access to and are users of MRG Services UK Limited's IT systems, both in and out of MRG Services UK Limited.

1.2 MRG Services UK Limited empowers its members of staff to impose disciplinary penalties for inappropriate behaviour, such as incidents of cyber bullying or other e-safety incidents covered by this policy, which may take place outside of the provider, but is linked to membership of the provider.

1.3 MRG Services UK Limited will deal with such incidents within this policy and associated behaviour and anti- bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of college.

2.0 Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within MRG Services UK Limited.

2.1 Board of Directors:

The Board of 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 Board receiving regular information about e-safety incidents and monitoring reports. A member of the Board has taken on the role of E-Safety Lead. The role of the E-Safety Lead will include:

- regular meetings with the Safeguarding Manager
- reporting to the Board

2.2 E-Safety Committee:

The E-Safety Committee's role will include:

- regular monitoring of e-safety incident logs
- regular monitoring of filtering/change control logs
- reviewing the policy on an annual basis

2.3 Senior Leaders:

- Senior Leaders have a duty of care for ensuring the safety (including e-safety) of members of the provider community, though the day to day responsibility for e-safety will be delegated to the Safeguarding Manager.
- All members of the Senior Leadership Team 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. (see flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant HR disciplinary procedures).

- The E-Safety Lead is responsible for ensuring that the Safeguarding Manager and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Directors will receive regular monitoring reports from the Safeguarding Manager at monthly Senior Leadership Team Meetings.

2.4 Safeguarding Manager:

- leads on e-safety issues with IT Manager
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the e-safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority/relevant body
- receives reports of e-safety incidents and creates a log of incidents to inform future e- safety developments
- reports regularly to Senior Leadership Team

2.5 IT Manager:

The IT Manager is responsible for ensuring:

- that the company's technical infrastructure is secure and is not open to misuse or malicious attack.
- that the company meets required e-safety technical requirements and any relevant body E-Safety Policy/Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- 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 the E-Safety Lead and Safeguarding Manager for investigation/action/sanction.
- that monitoring software/systems are implemented and updated as agreed in company policies.

2.6 Teaching and Support Staff:

Teaching 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 Agreement.

- they report any suspected misuse or problem to the Safeguarding Manager for investigation/action/sanction.
- all digital communications with learners/parents/carers/employers and other agencies 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 agreements.
- 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 company 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

2.7 Safeguarding Team:

The Safeguarding Team should be trained in e-safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

2.8 Learners:

- are responsible for using the provider digital technology systems in accordance with the Learner Acceptable Use Agreement.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of their learning and realise that the provider's E-Safety Policy covers their actions out of learning, if related to their membership of the provider.

2.9 Parents/Carers:

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The provider will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website/VLE and information about national/local e-safety campaigns/literature.

3.0 Policy Statements

3.1 Education – 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 the provider's e-safety provision. Children and young people need the help and support of the provider to recognise and avoid e-safety risks and build their resilience.

3.1.1 E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The information given 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 Student Services meetings and tutorial/pastoral activities.
- Learners should be taught in all lessons 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 both within and outside college
- 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.
- It is accepted that from time to time, for good educational reasons, learners may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

3.2 Education – parents/carers:

Parents/carers play an essential role in the education of children and young people and in the monitoring/regulation of their on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

3.2.1 The provider will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site, VLE
- Parents/Carers evenings/sessions
- High profile events/campaigns e.g. Safer Internet Day

3.3 Education & Training – Staff/Volunteers:

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the provider e-safety policy and Acceptable Use Agreements.
- The E-Safety Committee will receive regular updates through attendance at external training events/other relevant organisations and by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training days.
- Managers will provide advice/guidance/training to individuals as required.

3.4 Training – Board:

Directors should take part in e-safety training/awareness sessions, with particular importance for those who are involved in technology/e-safety/health and safety/safeguarding. This may be offered in several ways:

- Participation in college training/information sessions for staff.

3.5 Technical – infrastructure/equipment, filtering and monitoring:

The provider IT department will be responsible for ensuring that the provider infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- Provider technical systems will be managed in ways that ensure that the provider meets recommended technical requirements

- There will be regular reviews and audits of the safety and security of college technical systems
- All users will have clearly defined access rights to college systems and devices.
- All users will be provided with a username and secure password. Users are responsible for the security of their username and password.
- The provider has provided enhanced/differentiated user-level filtering
- IT staff regularly monitor and record the activity of users on the provider systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual/potential incident/security breach to the relevant person, as agreed.
- Users are not permitted to download and/or install applications (including executable or similar types) on to a college device or whilst using the providers systems, without agreement from the IT department.
- Users may use the following types of removable media for the purposes detailed:
    - CD/DVD – Playing original video material, original music and viewing data written to the media that is owned by the user (who has copyright ownership). The use of software written to writable versions of this media is strictly prohibited.
    - USB Media (memory sticks) – this type of media can be used on college devices for transferring personal work, this being data created by the user. The use of applications on this type of media is strictly prohibited.
    - Other types of media that may exist may only be used for the movement of personal data where the user owns the copyright.

3.6 Bring Your Own Device (BYOD) PL53:

The policy applies to any hardware and related software that is not organisationally owned or supplied but could be used to access organisational resources. That is, devices users have acquired for personal use but also wish to use in the provider's network environment.

3.6.1 Guidelines for Use of Wireless Internet

- Users must understand that the use of a personal device in the provider, is for work use only and at the provider's discretion.
- Users should have permission from the IT Manager to use a personal device within the provider.
- Access to the provider network by Wi-Fi using personal devices is prohibited unless permission has been provided by the provider IT Manager.
- Use of personal devices in the provider must support college activities.
- Users must power off and put away personal devices if directed to do so by management.
- Users must ensure that their personal device does not disrupt the learning/work of others. For example, audio should be muted unless directed otherwise by Management.
- Users are responsible for the use of their personal device on the provider premises.

- Users should practice caution when allowing others to access their personal device.

3.6.2 Further information is available from PL53 Bring Your Own Device Policy

3.7 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, parents/carers and learners need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying 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. The provider 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 e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at college events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other learners in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow college policies concerning the sharing, distribution and publication of those images. Those images should only be taken on college equipment, the personal equipment of staff should not be used for such purposes. Refer to FM02 (Learner Image Consent Form)
- 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 the provider into disrepute.
- 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.
- Learners' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Learners' work can only be published with the permission of the learner /and parents or carers for learners under the age of 18.

3.8 Data Protection:

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and the providers' Data Protection Policy.

3.8.1 Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.
- See Policy PL10

3.9 Communications:

A wide range of rapidly developing communications technologies has the potential to enhance learning. When using communication technologies, the provider considers the following as good practice:

- The official provider email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the provider 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 or parents/carers (email, VLE, letters etc) must be professional in tone and content.

3.10 Social Media - Protecting Professional Identity:

All education providers have a duty of care to provide a safe learning environment for learners and staff. The Provider could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the company liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The provider provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners, staff and the provider through limiting access to personal information:

- No reference should be made in social media to learners, parents/carers or college staff.
- They do not engage in online discussion on personal matters relating to members of the provider community.
- Personal opinions should not be attributed to the provider or local authority.

3.11 Appropriate and Inappropriate Use by Staff or Adults:

Staff members have access to the network so that they can obtain age appropriate resources for their classes and create folders for saving and managing resources.
They have a password to access a filtered internet service and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in.
All staff should receive a copy of the E-Safety Policy and a copy of the Acceptable Use Agreement, which they need to sign, return to the provider, to keep under file with a signed copy returned to the member of staff.

The Acceptable Use Agreement will be displayed on the staff noticeboards as a reminder that staff members need to safeguard against potential allegations and a copy of this policy is provided to all staff for home use.

When accessing the Learning Platform from home, the same Acceptable Use Agreement will apply. The acceptable use should be similar for staff to that of the children and young people so that an example of good practice can be established

3.12 In the Event of Inappropriate Use

If a member of staff is believed to misuse the internet or learning platform in an abusive or illegal manner, a report must be made to the HR Manager immediately and then the Disciplinary Procedure and the Safeguarding Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

3.13 Appropriate and Inappropriate Use by Children or Young People:

Acceptable Use Agreements detail how children and young people are expected to use the internet and other technologies within college, including downloading or printing of any materials. The agreements are there for children and young people to understand what is expected of their behaviour and attitude when using the internet. This will enable them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another child, or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

3.13.1 The Provider should encourage parents/carers to support the agreement with their child or young person. This can be shown by signing the Acceptable Use Agreements together so that it is clear to the provider/education setting or other establishment that the agreement is accepted by the child or young person with the support of the parent/carer. This is also intended to provide support and information to parents/carers when children and young people may be using the Internet beyond college/education setting or another establishment.

3.13.2 The downloading of materials, for example, music files and photographs need to be appropriate and 'fit for purpose' based on research for work and be copyright free.

3.13.3 File-sharing via e-mail, weblogs or any other means online should be appropriate and be copyright free when using the learning platform in or beyond college/education setting or other establishment.

3.14 In the Event of Inappropriate Use

Should a child or young person be found to misuse the online facilities whilst at college, the following consequences should occur:

- Any child found to be misusing the internet by not following the Acceptable Use Agreement may have a letter sent home to parents/carers explaining the reason for suspending the child or young person's use for a particular lesson or activity.

- Further misuse of the agreement may result in further sanctions which could include a meeting with the Safeguarding Manager, learner and parent/carer to discuss next steps and/or a referral to a relevant external agency e.g. Under the Prevent Duty.

- If misuse is persistent, it could result in a learner's programme being immediately terminated.

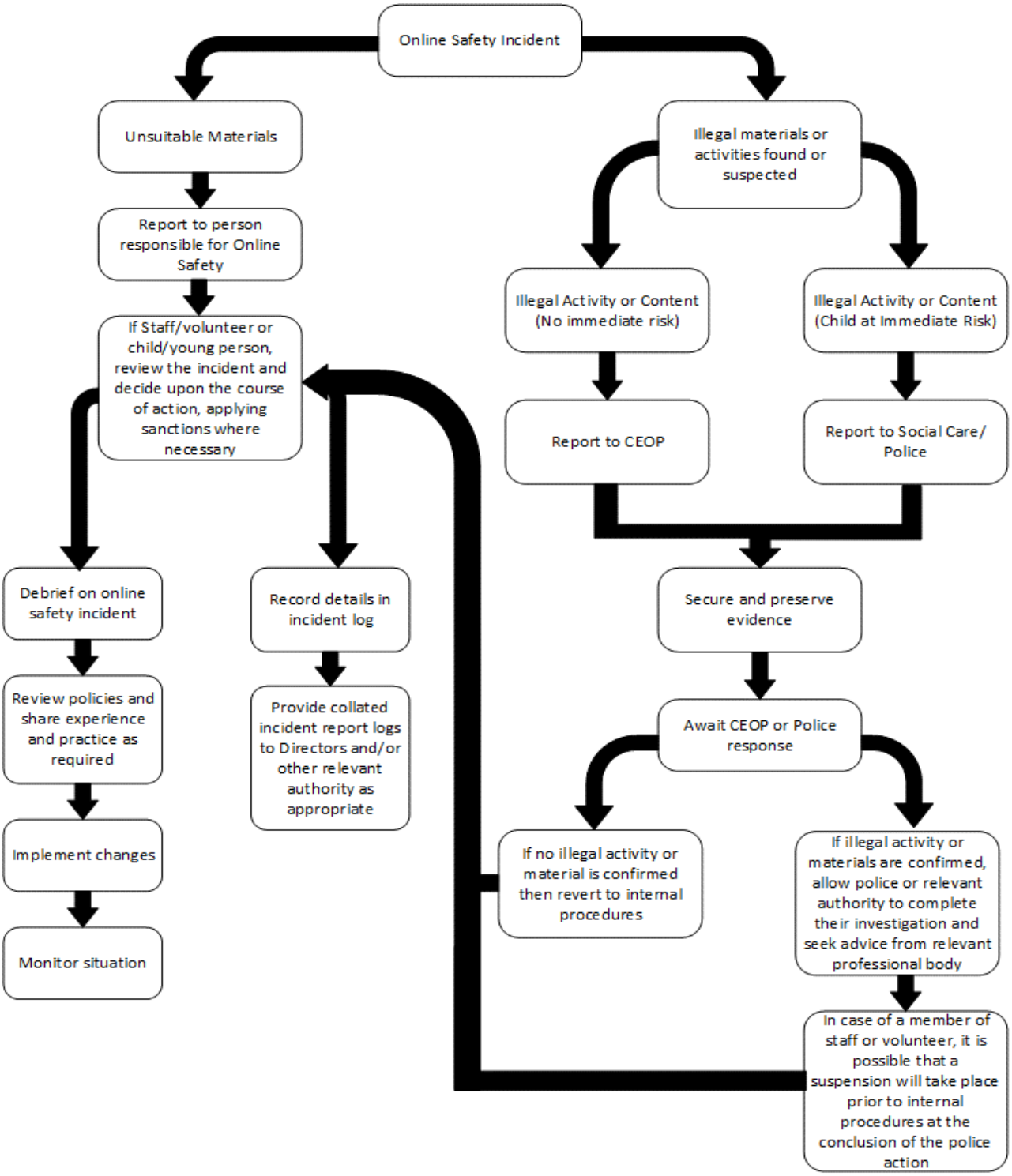
3.14.1 In the event that a learner **accidentally** accesses inappropriate materials the learner should report this to a member of staff immediately and take appropriate action to hide the screen or close the window, so that the staff member can take the appropriate action. Where a learner feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice.

3.15 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 (see "In the Event of Inappropriate Use" above). See flow chart on the next page.

3.16 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, refer to the right-hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



3.17 Other Incidents

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

3.17.1 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.
    - Involvement by Local Authority or national/local organisation (as relevant).
    - 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.
        - 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.

3.17.2 It is important that all of the above steps are taken as they will provide an evidence trail for the provider 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.

APPENDIX 1

Secure transfer of data and access out of college

MRG Services UK Limited recognises that personal data may be accessed by users out of college or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the provider or authorised premises without permission and unless the media is encrypted, and password protected and is transported securely for storage in a secure location
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members)
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe.

APPENDIX 2

MRG Services UK Limited

ACCEPTABLE USE AGREEMENT (Staff/Volunteer) 2018

Acceptable Use Policy Agreement

1.0 GENERAL

1.1 New IT technologies have become integral to the lives of children and young people in today's society, both within work and in their lives outside education. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone.

1.2 These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

2.0 SCOPE

This Acceptable Use Policy is intended to ensure:

2.1 That staff will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

2.2 That MRG Services UK Limited systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

2.3 That staff are protected from potential risk in their use of technology in their everyday work.

2.4 The provider will try to ensure that staff will have good access to digital technology to enhance their work, to enhance learning opportunities for learners learning and will, in return expect staff to agree to be responsible users.

3.0 STAFF AGREEMENT

All members of staff must read and sign the agreement set out below: -

3.1 I understand that I must use MRG Services UK Limited systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that learners receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

4.0 PROFESSIONAL AND PERSONAL SAFETY

4.1 I understand that the provider will monitor my use of the provider digital technology and communications systems.

4.2 I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.), and to the transfer of personal data (digital or paper based).

4.3 Moving of IT and AV equipment on all sites without the express permission of the IT Manager is prohibited.

4.4 I understand that the provider digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the provider.

4.5 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.

4.6 I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

5.0 PROFESSIONALISM

I will be professional in my communications and actions when using College IT systems:

5.1 I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

5.2 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.

5.3 I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the provider 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. Where these images are published (e.g. on the provider website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.

5.4 I will only use social networking sites in accordance with the provider's policies.

5.5 I will only communicate with learners and parents using official College systems. Any such communication will be professional in tone and manner.

5.6 I will not engage in any on-line activity that may compromise my professional responsibilities.

6.0 SAFE ENVIRONMENT AND SYSTEMS

The provider have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the provider:

6.1 When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc), I will follow the rules set out in this agreement, in the same way as if I was using College equipment. I will also follow any additional rules set by the provider about such use. I will ensure that any such

devices are protected by up to date anti-virus software and are free from viruses.

6.2 I will not use personal email addresses on the provider IT systems.

6.3 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)

6.4 I will ensure that my data is regularly backed up, in accordance with relevant Provider policies.

6.5 I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist 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.

6.6 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.

6.7 I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in policies.

6.8 I will not disable or cause any damage to the Provider's equipment, or the equipment belonging to others.

6.9 I understand that data protection policy requires that any staff/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 Provider's policy to disclose such information to an appropriate authority.

6.10 I will immediately report any damage or faults involving equipment or software, however this may have happened.

7.0 USING THE INTERNET

When using the internet in my professional capacity or for the Provider's sanctioned personal use:

7.1 I will ensure that I have permission to use the original work of others in my own work.

7.2 Where work is protected by copyright, I will not download or distribute copies (including music and videos).

8.0 RESPONSIBILITIES

I understand that I am responsible for my actions in and out of the provider:

8.1 I understand that this Acceptable Use Policy applies not only to my work and use of the Provider's digital technology equipment whilst in learning, but also applies to my use of College systems and equipment off the

premises and my use of personal equipment on the premises or in situations related to my employment by the provider.

8.2 I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Directors or the Local Authority and in the event of illegal activities the involvement of the police.

9.0 DECLARATION

9.1 I have read and understand the above and agree to use the provider digital technology systems and my own devices (when carrying out communications related to the provider) within these guidelines.

Signature: _____

Name: _____

Date: _____

APPENDIX 3

MRG Services UK Limited

ACCEPTABLE USE AGREEMENT

(Learner)

2018

IT, including the internet, e-mail and mobile technologies, has become an important part of learning and a major part of people's personal lives. These technologies are powerful tools, which open up new opportunities for everyone. MRG Services UK Limited believe that young people should have an entitlement to safe internet access and expects all learners to be responsible when using any IT. For learner safety, your internet activity on college equipment is closely monitored and logs are kept of activity. These logs include who is accessing what material and for how long.

Acceptable Use Policy Agreement
I understand that I must use MRG Services UK Limited IT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I will make sure that all IT contact with other people is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be upsetting or not allowed at college. If I accidentally find anything like this, I will close the screen and tell a member of staff immediately.
- I will not give out my own details such as my name, phone number or home address.
- I will be responsible for my behaviour when using IT because I know that these rules are to keep me safe.
- I know that the provider may check my use of IT and monitor the Internet sites I have visited, and that my parent/carer will be contacted if a member of college staff is concerned about my e-safety.
- I will be aware of "stranger danger" when communicating online.
- If I arrange to meet people offline that I have communicated with online, I will do so in a public place and take someone responsible with me.
- I will not share images of anyone without their permission.

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

- I will only use IT in college for college purposes.
- I will only open e-mail attachments from people I know, or who my tutor has approved.
- I will not tell other people my IT passwords.
- I will only open/delete my own files.
- I will not bring software, CDs or IT equipment into college without permission.
- I will only use the Internet after being given permission from a tutor.
- 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 the provider systems or devices for online gaming, online gambling, internet shopping, file sharing or video broadcasting unless I have permission from a member of staff to do so.

I understand that I am responsible for my actions, both in and out of college:

- I understand that MRG Services UK Limited has the right to take action against me if I am involved in incidents of inappropriate behaviour, which are covered in this agreement, e.g. Cyber bulling.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted access to college systems and devices.

MRG Services UK Limited
ACCEPTABLE USE AGREEMENT
(Learner) 2018

This form relates to the Learner Acceptable Use Agreement, to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to the Provider IT systems.

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

- I use MRG Services UK Limited systems and devices.
- I use my own devices in MRG Services UK Limited (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc
- I use my own equipment out of MRG Services UK Limited in a way that is related to my learning e.g. communicating with other members of the provider, VLE, website etc.

Name of Learner (PRINT)	
Vocational Group	
Signed by Learner	
Signed by parent/carer (if under 18)	
Date	

(Please detach this page and hand it to Reception)