



# The GTA E-Safety Policy

This policy applies to all members of GTA (including staff, apprentices, volunteers, parents/carers, and visitors) who access the GTA.

Document Ref	CP3.2
Version	1.4
Issue Date	08/03/2024
Reviewed Date	08/03/2024
Next Review Date	01/03/2024

Signature:

Approved By:

J. Mace

Position:

CEO

Date:

08/03/2024

## Contents Page

1.0 Schedule for Development/Monitoring/Review.....	Page 4
2.0 Objective.....	Page 4
3.0 Roles and Responsibilities.....	Page 4
3.1 Chief Executive.....	Page 4
3.2 CEO and Senior Leaders.....	Page 4
3.3 E-Safety Co-ordinator/Designated Senior Person.....	Page 5
3.4 ICT Support.....	Page 5
3.5 Teaching and Support Staff.....	Page 5
3.6 Safeguarding Designated Person.....	Page 6
3.7 Learners.....	Page 6
3.8 Parents/Carers.....	Page 6
3.9 Education – Learners.....	Page 6
3.10 Education – parents/carers.....	Page 7
3.11 Education & Training – Staff.....	Page 7
3.12 Training – Safeguarding.....	Page 7
4.0 Technical – infrastructure/equipment, filtering and monitoring.....	Page 8
4.1 Bring Your Own Device (BYOD) (GTA Staff).....	Page 8
4.2 Use of digital and video images.....	Page 9
5.0 Data Protection.....	Page 9
6.0 Communications.....	Page 9
7.0 Social Media - Protecting Professional Identity.....	Page 10
8.0 Staff User Access Summary.....	Page 10
9.0 Staff Inappropriate Use.....	Page 10
10.0 Apprentice User Access Summary.....	Page 11
11.0 Apprentice Inappropriate Use.....	Page 11
12.0 Reportable Incidents.....	Page 11

APPENDIX 1 - Secure transfer of data and access out of the GTA.....Page 13

APPENDIX 2 - ACCEPTABLE USE AGREEMENT (Staff).....Page 14

APPENDIX 3 – ACCEPTABLE USE AGREEMENT (Learner).....Page 17

## **1.0 Schedule for Development/Monitoring/Review**

The E-Safety Policy will be reviewed 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.

The Doncaster, Rotherham & District Group Training Association Ltd (GTA) 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
- Learners
- Parents/carers
- Staff

## **2.0 Objectives**

This policy applies to all members of the GTA (including staff, learners, volunteers, parents/carers, and visitors) who have access to and are users of the GTA ICT systems, both in and out of the GTA. This policy has been put in place to primarily protect anyone who has access to or is affected by the GTA ICT system/s and or network.

The Education and Inspections Act 2006 empowers senior management, to such extent as is reasonable, to regulate the behaviour of learners when they are off the GTA site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place outside of the GTA, but is linked to membership of the GTA. The 2011 Education Act increased these powers regarding the searching for and of electronic devices and the deletion of data. The GTA 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 takes place out of the GTA.

## **3.0 Roles and Responsibilities**

The following section outlines the e-safety roles and responsibilities of individuals and groups within the GTA.

### **3.1 Chief Executive**

The Chief Executive has the overall responsibility for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Chief Executive receiving regular information about e-safety incidents and monitoring reports. A member of the GTA staff has taken on the role of E-Safety Co-ordinator. The role of the E-Safety Co-ordinator / Chief Executive can include:

- Meetings between E-Safety Co-ordinator/Designated Senior Person
- Monitoring of e-safety incident logs
- Monitoring of filtering/change control logs
- Reports to Directors and trustees

### **3.2 Chief Executive, Senior Leaders and Safeguarding**

- The Chief Executive has an overall duty of care for ensuring the safety (including e-safety) of members of the GTA, though the day-to-day responsibility for e-safety will be delegated to the e-safety Co-ordinator/Designated Senior Person. The Chief Executive and (at least) another member of the Senior Leadership Team is aware of the procedures to be followed in the event of a serious e-safety allegation being

made against a member of staff (see dealing with e-safety incidents – included in this policy section – “Responding to incidents of misuse”).

- The Chief Executive /Senior Leadership Team are responsible for ensuring that the e-safety Coordinator/Designated Senior Person 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 Chief Executive/Senior Leadership Team will ensure that there is a system in place to allow for monitoring and support of those in the GTA who carry out the internal e-safety monitoring role. This is to provide a safety net and support to those colleagues who take on important monitoring roles.

### **3.3 E-Safety Co-ordinator/Designated Senior Person**

- Leads on e-safety issues
- Takes day-to-day responsibility for e-safety issues and has a leading role in establishing and reviewing the GTA e-safety policies/documents
- Ensures that all staff is aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provide training and advice for staff.
- Liaises with the GTA technical staff.
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- Meets regularly with the e-safety Co-ordinator to discuss current issues, review incident logs and filtering/change control logs.
- Reports regularly to the Senior Leadership Team.

### **3.4 ICT Support**

The Centre Operations Manager is responsible for ensuring:

- The GTA’s technical infrastructure is secure and is not open to misuse or malicious attack.
- The GTA meets required e-safety technical requirements and any Local Authority/other relevant body E-Safety Policy/Guidance that may apply.
- Those users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- They keep up to date with e-safety technical information 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 Chief Executive/E-Safety Coordinator/Designated Senior Leader for investigation/action/sanction.
- That monitoring software/systems are implemented and updated as agreed in the GTA policies.

### **3.5 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 GTA 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 Chief Executive /E-Safety co-ordinator/Designated Senior Person for investigation/action/sanction.
- All digital communications with learners/parents/carers should be on a professional level and only carried out using official GTA systems.
- E-safety is embedded in all aspects of teaching sessions 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 teaching sessions and other GTA activities (where allowed) and implement current policies regarding these devices.
- In teaching sessions 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.

### **3.6 Safeguarding Designated Person**

The Safeguarding Designated Person and Safeguarding Deputy should be trained in e-safety issues and be aware of the potential for serious safeguarding issues to arise from:

- Sharing of personal data.
- Access to illegal/inappropriate materials.
- Inappropriate on-line contact.
- Potential or actual incidents of grooming.
- Cyber-bullying.

### **3.7 Learners**

- Are responsible for using GTA 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 the GTA's digital technologies and realise that the GTA's E-Safety Policy covers their actions out of the GTA, if related to their enrolment at the GTA.

### **3.8 Parents/Carers**

Parents/carers play a crucial role in ensuring that their apprentices understand the need to use the internet/mobile devices in an appropriate way. Parents and carers are encouraged to support the GTA in promoting good e-safety practices and to follow guidelines on the appropriate use of:

- Digital and video images taken at GTA events.
- Their apprentice's personal devices in the GTA (where this is allowed)

### **3.9 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 GTA's e-safety provision. Apprentices and young people need the help and support of the GTA 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:

- A planned e-safety curriculum should be provided as part of the Apprenticeship or program journey.
- Key e-safety messages should be reinforced as part of a planned programme of tutorial/pastoral activities.
- Learners should be taught in all teaching sessions to be critically aware of the materials/content they access online 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 the GTA.
- Staff should act as good role models in their use of digital technologies the internet and mobile devices.
- In teaching sessions 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, and 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.

### **3.10 Education – parents/carers**

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

### **3.11 Education & Training – Staff**

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 GTA's e-safety policy and Acceptable Use Agreements.
- The E-Safety Coordinator/Designated Senior Person (or other nominated person) will receive 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.
- The E-Safety Co-ordinator will provide advice/guidance/training to individuals as required.

### **3.12 Training –Safeguarding**

Safeguarding staff and at least one member from the Board of Directors should take part in e-safety training and or awareness sessions.

#### **4.0 Technical – infrastructure/equipment, filtering, and monitoring**

The GTA will be responsible for ensuring that the 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. The GTA technical systems will be managed in ways that ensure that the GTA meets recommended technical requirements

There will be reviews and audits of the safety and security of the GTA's technical systems:

- Staff will have defined access rights to the GTA's 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 GTA has provided enhanced/differentiated user-level filtering (AVG).
- The GTA technical staff regularly monitors and records the activity of users on the GTA's 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.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. visitors) onto the GTA systems.
- An agreed policy is in place regarding the extent of personal use that users are allowed on the GTA devices that may be used out of the GTA.
- Users are not permitted to download and or install applications (including executable or similar types) onto a GTA device or whilst using GTA systems, without agreement from the Centre Manager and or Chief Executive.

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 GTA 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.

#### **4.1 Bring Your Own Device (BYOD) (GTA Staff)**

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led users to bring their own technologies to provide greater freedom of choice and usability. However, there are a number of e-safety considerations for BYOD. The use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing, and monitoring.

- The GTA has a set of clear expectations and responsibilities for all users.
- The GTA adheres to the Data Protection Act principles.
- All users are provided with and accept the Acceptable Use Agreement.
- Where possible these devices will be covered by the GTA's normal filtering systems while being used on the premises.
- All users should use a password to keep data safe.
- Any device loss, theft, or change of ownership of the device should be reported.



## 4.2 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 GTA 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 apprentice at GTA 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 is allowed to take digital/video images to support educational aims, but must follow the GTA's policies concerning the sharing, distribution, and publication of those images. Those images should only be taken on the GTA 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 the GTA 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.
- Learners' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers (under 18 years) will be obtained before photographs of learners are published on the GTA website.
- Learner's work can only be published with the permission of the learner, parents, or carers.

## 5.0 Data Protection

Personal data will be recorded, processed, transferred, and made available according to the Data Protection Act 1998, 2018 and the GTA's Data guidelines.

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.

## 6.0 Communications

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

- The official GTA 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 GTA 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, chat, VLE etc) must be professional in tone and content.
- 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 the learner/ website and only official email addresses should be used to identify members of staff.

## **7.0 Social Media - Protecting Professional Identity**

All Training Providers have a duty of care to provide a safe learning environment for learners and staff. Training Providers 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 GTA liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

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

- Training to include acceptable use; of social media risks; checking of settings; data protection; and reporting issues.
- Clear reporting guidance, including responsibilities, procedures, and sanctions.
- Risk assessment, including legal risk.

The GTA staff should ensure that:

- No reference should be made in social media to learners, parents/carers or GTA staff unless authorisation for the use of their identity has been given.
- They do not engage in online discussions on personal matters relating to members of the GTA community.
- Personal opinions should not be attributed to the GTA.
- Security settings on personal social media profiles are regularly checked to minimise the risk of loss of personal information.

## **8.0 Staff User Access Summary**

Staff members have access to the network so that they can obtain 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 and return to the GTA, to keep under file with a signed copy returned to the member of staff.

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 apprentices and young people so that an example of good practice can be established.

## **9.0 Staff 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 Chief Executive/Senior Designated Person immediately and then the Managing Allegations Procedure, Safeguarding and Apprentice Protection Policy must be followed to deal with any misconduct and all appropriate authorities contacted if required.

## **10.0 Apprentice User Access Summary**

Acceptable Use Agreement details how apprentices and young people are expected to use the internet and other technologies within the GTA, including downloading or printing of any materials. The agreement is there for apprentices 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 person, or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate search for inappropriate materials and the consequences of doing so.

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

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

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 /an education setting or other establishment.

## **11.0 Apprentice Inappropriate Use**

Should an apprentice or young person be found to misuse the online facilities whilst at the GTA, the following consequences could occur:

- Any apprentice or young person found to be misusing the internet by not following the Acceptable Use Agreement may have a letter sent home to parents/carers (if under 18 years of age) and to their employer explaining the reason for suspending the apprentice or young person's use for a particular lesson or activity.
- Further misuse of the agreement may result in further sanctions which could include not being allowed to access the internet for a period.
- If an apprentice or young person accidentally accesses inappropriate materials the apprentice should report this to an adult immediately and take appropriate action to hide the screen or close the window so that an adult can take the appropriate action. Where an apprentice or young person 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](http://www.thinkuknow.co.uk)) to make a report and seek further advice. The issue of an apprentice or young person deliberately misusing online technologies should also be addressed by the establishment.

Apprentices should be taught and encouraged to consider the implications of misusing the internet and posting inappropriate materials to websites, for example, as this may have legal implications.

## 12.0 Reportable Incidents

It is hoped that all members of the GTA community will be responsible users of digital technologies, who understand and follow the GTA 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, accusations should be reported to the Chief Executive or Safeguarding Lead or Deputy if the Lead is not available who investigated an alleged misuse.

The following action will be taken into consideration when investigating:

- Isolate the computer or device in question as best you can. Any change to its state may hinder a later police investigation.
- 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.
- 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 apprentice 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 the content being reviewed includes images of abuse, then the monitoring should be halted and referred to the Police immediately. Other instances, but not limited to that could be reported to the Police are:

- Incidents of 'grooming' behaviour.
- The sending of obscene materials to an apprentice.
- Adult material which potentially breaches the Obscene Publications Act.
- Criminally racist material.
- Other criminal conduct, activity, or materials.

It is important that all the above steps are taken as they will provide an evidence trail for the GTA and possibly the police.

The completed investigation form/s will be retained by the GTA for evidence purposes.

## APPENDIX 1

Secure transfer of data and access out of the Doncaster GTA.

The GTA recognises that personal data may be accessed by users out of the GTA or transferred to other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from GTA 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 out of the GTA.
- 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 (Office 365 or 7-Zip).
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe.

## APPENDIX 2

### DONCASTER GTA ICT ACCEPTABLE USE AGREEMENT (GTA STAFF)

New technologies have become integral to the lives of apprentices and young people today, both within the GTA and in their lives outside the GTA. The internet and other digital information and communications technologies are powerful tools, which open new opportunities for everyone. 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 always have an entitlement to safe internet access.

This Acceptable Use Policy is intended to ensure:

- Staff will be responsible users and stay safe while using the internet and other communications technologies for educational, personal, and recreational use.
- The GTA ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Staff is protected from potential risk in their use of ICT in their everyday work.
- The GTA will try to ensure that staff will have good access to ICT to enhance their work, and to enhance learning opportunities for learners learning and will, in return, expect staff to agree to be responsible users.

This policy applies to any device in the GTA. It applies across the whole network and includes Wi-Fi, and mobile hotspots. The GTA can carry out secure content inspections (SSL inspection). This means that when you access a site that uses techniques to secure the information between the website and yourself, the GTA can read the information and remove inappropriate content or prevent access to the material.

Excluded from this inspection are sites that contain sensitive financial information, including banks and payment systems.

Your activity on the internet is closely monitored by the GTA, whether on a GTA device or using your own device through the GTA Wi-Fi network.

The GTA email system is provided for educational and work purposes, where required the GTA could access your GTA email for safeguarding purposes.

#### ***Acceptable Use Policy Agreement***

I understand that I must use the GTA 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 apprentices or young people in my care in the safe use of ICT and embed e-safety in my work.

For my professional and personal safety:

- I understand that the GTA 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 the GTA ICT systems (e.g. laptops, email, VLE company-issued mobiles & tablets etc) out of the GTA, and to the transfer of personal data (digital or paper-based) out of the GTA.
- I understand that the GTA ICT 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 GTA.
- 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 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 the GTA 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 the GTA's 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 GTA website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in the GTA in accordance with GTA's policies
- I will only communicate with learners and parents/carers using official GTA systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.

The GTA has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the company:

- When I use my mobile devices (Tablets/laptops/mobile phones/USB devices etc) in the GTA, I will follow the rules set out in this agreement, in the same way as if I were using GTA equipment.
- I will also follow any additional rules set by the GTA about such use.
- I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.
- I will not use personal email addresses on the GTA 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 programs).
- I will ensure that my data is regularly backed up, in accordance with relevant GTA policies.
- I will not try to upload, download, or access any materials which are illegal (apprentice 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
- 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, nor will I try to alter computer settings unless this is allowed in the GTA policies.
- I will not disable or cause any damage to the GTA equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others as outlined in the GTA E-Safety Policy.

When using the internet in my professional capacity or for the GTA sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own 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 the GTA:

- I understand that this Acceptable Use Agreement applies not only to my work and use of GTA ICT equipment in GTA, but also applies to my use of the GTA ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the GTA.

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

STAFF ACCEPTABLE USE AGREEMENT

This form relates to the Acceptable Use Agreement (Staff), 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, you will not be granted access to the GTA ICT systems and network.

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

- I will use the GTA systems and devices (both in and out of the GTA).
- I will use my own devices in GTA (when allowed) e.g. mobile phones, USB devices, cameras etc.
- I will use my own equipment out of the GTA in a responsible and sensible manner.

Name of Staff (PRINT) .....

Signed .....

Date .....



## APPENDIX 3

### DONCASTER GTA ACCEPTABLE USE AGREEMENT (LEARNER)

Digital technologies have become integral to the lives of apprentices and young people, both within and outside the GTA. These technologies are powerful tools, which open new opportunities for everyone. These technologies can stimulate discussion, promote creativity, and stimulate awareness of context to promote effective learning. Everyone should have an entitlement to safe internet access.

This Acceptable Use Policy is intended to ensure:

- That apprentices and young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal, and recreational use.
- That the GTA systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The GTA will try to ensure that learners will have good access to digital technologies to enhance their learning and will, in return, expect the learners to agree to be responsible users.

This policy applies to any device in the GTA. It applies across the whole network and includes Wi-Fi. The GTA carries out secure content inspection (SSL inspection). This means that when you access a site that uses techniques to secure the information between the website and yourself, the GTA could read the information and remove inappropriate content or prevent access to the material.

Excluded from this inspection are sites that contain sensitive financial information, including banks and payment systems.

Your activity on the internet is closely monitored by the GTA, whether on a GTA device or using your own device through the GTA Wi-Fi.

The GTA email system is provided for educational and business purposes, where required the GTA can access your GTA email for safeguarding purposes.

#### **Acceptable Use Policy Agreement**

I understand that I must use the GTA 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 the GTA 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 online.
- I will not disclose or share personal information about myself or others when online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- If I arrange to meet people off-line that I have communicated with online, I will do so in a public place and take an adult with me if required.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.

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

- I understand the GTA 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 the GTA systems or devices for online gaming, online gambling, internet shopping, file sharing, or video broadcasting (e.g. 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 the GTA has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the GTA:

- I will only use my own personal devices (mobile phones/USB devices etc) in the GTA if I have permission. I understand that, if I do use my own devices in the GTA, I will follow the rules set out in this agreement, in the same way as if I was using GTA 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 programs 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 GTA 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 try to download copies (including music and videos)
- 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 GTA:

- I understand that the GTA also has the right to act against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of the GTA and where they involve my membership of the GTA (examples would be cyber-bullying, 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.

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 to the GTA systems and devices.

DONCASTER GTA

LEARNER ACCEPTABLE USE AGREEMENT

This form relates to the Acceptable Use Agreement (learner) 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, you will not be granted access to the GTA ICT systems and network.

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

- I will use the GTA systems and devices (both in and out of the GTA).
- I will use my own devices in GTA (when allowed) e.g. mobile phones, USB devices, cameras etc.
- I will use my own equipment out of the GTA in a sensible and responsible manner.

Name of Staff (PRINT) .....

Signed .....

Date .....