Learner Computer and Digital Use Policy

As well as opportunities, new technologies have brought new challenges and risks. The internet can be used to spread terrorist material; it can be a tool for abuse and bullying; and it can be used to undermine civil discourse, objective news and intellectual property. Increasingly sophisticated use of data can create powerful insights from our behaviour online, which can be deployed in ways that influence the decisions we make or target the services and resources we receive.

Government are leading the way to tackling these challenges. The starting point is that we will have the same rights and expect the same behaviour online as we do offline. We will take action to ensure that the internet and new technologies are not only safe and secure, but also that they are developed and used responsibly and ethically, with users' interests at their heart.

https://www.gov.uk/government/publications/digital-charter/digital-charter
https://www.gov.uk/government/consultations/online-harms-white-paper/public-feedback/onlineharms-white-paper-initial-consultation-response

This policy is provided to each employee and learner on joining and when significant updates occur. Accepting employment at Rotunda or registering on one of Rotunda Training Programmes indicates acceptance of the terms of this policy the detail of which will be covered during the induction process.

This policy applies to the use of all fixed/mobile electronic technologies and associated software, including personal equipment used on Rotunda premises or venues, that employees or learners have access to for personal and programme use that might pose e-safety risks during a time spent on Rotunda premises or venues, affecting the welfare of other employees or learners or where the culture or reputation of Rotunda are put at risk.

All employees and learners are responsible for their own good behaviour on Rotunda premises or venues. Employees are also subject to a separate additional policy which forms part of their contract of employment.

This policy is linked to the Rotunda Safeguarding Policy which is available to all employees, learners and employers.

E-SAFETY – ROTUNDA RESPONSIBILITIES

The internet is used in Rotunda to raise educational standards, to promote learner achievement, to support the professional work of staff and to enhance the school's management functions. Technology is advancing rapidly and is now a huge part of everyday life, education and business. We want to equip our learners with all the necessary ICT skills that they will need in order to enable them to progress confidently in their educational careers and onward towards their working environments when they leave education.

Some of the benefits of using ICT and the internet in education are:

For learners:

- unlimited access to worldwide educational resources and institutions such as art galleries, museums and libraries.
- an enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally.
- self-evaluation; feedback and assessment; updates on current affairs as they happen.
- access to learning whenever and wherever convenient.
- freedom to be creative.
- freedom to explore the world and its cultures from within a classroom.
- social inclusion, in class and online.
- access to case studies, videos and interactive media to enhance understanding.
- individualised access to learning.

For staff:

- Support and develop online learning.
- professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies.
- immediate professional and personal support through networks and associations.
- improved access to technical support.
- ability to provide immediate feedback to learners and parents.
- class management, attendance records, assessment and assignment tracking.

Rotunda Online-Safety Coordinator is the Safeguarding Lead and has day-to-day responsibility for E-Safety issues and has a leading role in establishing and reviewing Rotunda E-Safety policies and 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 advice for staff, as required and advises young people on E-safety and how to stay safe.
- liaises with the Local Authority where applicable for incidents that are defined as Safeguarding concerns and appropriate referrals made
- receives reports of E-Safety incidents and creates a log of incidents to inform future developments (following Rotunda Safeguarding reporting procedures and Complaints/ Disciplinary Policies)
- reports regularly to the Senior Leadership Team comprising of CEO.

It is the responsibility of the CEO to ensure the DSL receives appropriate training on Safety issues and be aware of the potential serious safeguarding/ child protection issues to arise from:

- The sharing of personal data
- Access to illegal/ inappropriate materials
- Inappropriate online contact with adults/ strangers
- Potential or actual incidents of grooming
- Cyber-bullying
- Sexting and the sending of inappropriate images including self-images

Rotunda is committed to safeguarding the welfare of all and recognises that an effective e-safety strategy is paramount to this. Our responsibilities include:

- Focusing on e-safety in all areas of work and the curriculum and reinforcing key e-safety messages as part of training, assessment and support activities
- Minimising the risks associated with using the internet and how to protect all from potential risks
- Being critically aware of content accessible online and guided to how to validate accuracy of information
- Recognising suspicious, extremist or bullying behaviour
- Understanding the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect
- Having an awareness of the consequences of negative online behaviour
- How to report cyberbullying and / or incidents that make anyone feel uncomfortable or under threat and how Rotunda will deal with those who behave badly

- Ensuring that employees act as good role models in their use of technologies, the internet and mobile electronic devices
- Providing sufficient e-safety training to employees and learners to protect employees, learners and themselves from online risks and to deal appropriately with e-safety incidents when they occur

For parents (learners under 18 and those identified as vulnerable):
Communication between Rotunda and parents/carers may be through e-mail and telephone messages. This form of contact can often be considered to be more effective, reliable and economic. Text messages and letters will also inform parent/carers of details relating to attendance, behaviour and other appropriate matters. It is paramount that parents (or carer) understand the safeguarding responsibilities of Rotunda and the permissions they require to ensure safety and compliance.

USE OF ROTUNDA NETWORK AND INTERNET
As normal practice employees and learners will be allowed to use Rotunda equipment, network or internet for testing, examination and assessment purposes under close supervision. In instances where use is authorised employees may review files and communications to ensure that users are using the system responsibly. For good practice the following are not permitted for employees or learners:

- Damaging, degrading or disrupting computers, computer systems or computer networks or performance
- Violating copyright laws
- Using others' passwords
- Trespassing in others' folders, work or files
- Intentionally wasting resources
- Any act which could result complaints to, or legal action against, Rotunda
- Using the Rotunda network for illegal activity
- Viewing, retrieving, downloading or sharing any material which in the reasonable opinion of the Chief Executive Officer is unsuitable.

The following are also not permitted on the Rotunda computers:

- Plagiarism - presenting documents compiled from Internet as own work
- Changing any of the computers' default settings, such as screensavers, backgrounds, folders, icons
- Installing any software without authorisation
- Circumvention of security or other provisions
- Malicious damage to or tampering with any system, network or changing of data
- Transmission, creation or possession of threatening, extremist, defamatory or obscene material

- Gaining unauthorised access to resources or websites using internal/external wireless modems.

EMPLOYEE AND LEARNER MOBILE ELECTRONIC DEVICE USE

"Mobile electronic device" includes but not limited to, laptops, tablet computers, iPods. Ipads, watches and mobile phones.

The use of mobile devices by employees is covered in the employee handbook and states "Please do not use your personal mobile phone while you are working other than if required by the Company as part of your job role."

Rotunda permits limited access to the wireless network by such devices, as set out in this section of the policy. This connection provides filtered access to the Internet using filtering and security software. The downloading of programs to these devices is the responsibility of the user and Rotunda cannot monitor or accept any responsibility for any programs that are installed or problems that an installation might cause. The downloading of programs to a personal laptop is also the responsibility of the user and Rotunda cannot monitor or accept any responsibility for any programs that are installed.

The following rules apply to all mobile electronic devices:

- Employees and learners may only connect their own devices to the internet via a mobile service while on Rotunda premises. In public venues they may be able to use the local access
- Under no circumstances should Rotunda computers, printers or other devices be detached from the network to make way for an employees or learner's own device.
- Employees and learners should ensure that their own devices are properly protected from viruses before communicating with Rotunda employee or other learners
- Rotunda does not accept any responsibility for the theft, loss of, or damage to, mobile electronic devices brought onto its premises or venues
- Employees and learners must not use mobile electronic devices in any manner which is inappropriate.

Mobile phone protocol

- Mobile phones will be switched off or on silent during all teaching or assessment sessions except with the permission of the tutor/assessor.

- Employees and learners may keep their mobile device about their person but should only use them outside classroom or assessment time unless with the permission of the tutor or trainer for that session.
- Learners may not bring mobile phones, Smart Watches or other wearables into examination rooms under any circumstances. If brought to the exam room, they must be handed in before and then collected after the examination.
- Employees and learners must not use mobile phones in any manner which is inappropriate. The taking and storing of indecent images and sexting are serious breaches of discipline and safeguarding
- Employees should only use mobile phones and other mobile electronic devices as a method of communication with learners with their permission. If there are reasonable grounds to believe that inappropriate communications have taken place, the CEO will require the relevant devices to be produced for examination and the usual disciplinary procedures will apply.

Camera, photograph and video protocol

- Using photographic material of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline.
- Employees and learners must allow the CEO to access images stored on mobile phones and/or cameras and must delete images if requested to do so. This would only be done if Rotunda had reason to believe that the image constitutes a breach of discipline.
- Posting of inappropriate photographic material which in the reasonable opinion of the CEO is offensive on websites such as YouTube, Facebook, Snapchat, Twitter, WhatsApp etc. is a serious breach of discipline and will be subject to disciplinary procedures whatever the source of the material
- Cameras and mobile electronic devices with a camera facility may be confiscated and searched in appropriate circumstances, if the CEO has reasonable grounds to believe that a learner's camera or mobile electronic device contains images, text messages or other material that may constitute evidence of criminal activity, she may hand the device to the Police for examination.
- On the instruction of the CEO employees and learners may be permanently banned from bringing a camera, mobile electronic device or laptop onto premises in future.

EMAIL

- On recruitment, all employees are provided with a Rotunda email account for business use only. Learners will provide their own email address.

- Learners must not use any personal web-based e-mail accounts such as Yahoo or Hotmail through the Rotunda network.

PERSONAL SAFETY

Learners are advised:

- Not to reveal their home address, image, or phone numbers, or those of other learners or of employees when on-line
- Not to arrange to meet someone that they have only met on the Internet or by email or in a chat room, unless they are certain of their own safety.
- To avoid sharing their account and password and keep their password private
- To report any unsolicited email, security problems, any unpleasant or inappropriate material, messages, or anything that makes them feel uncomfortable when on-line
- Take care in using social and blogging websites with great care being aware of the dangers that can be associated with posting pictures, text, opinions, videos and communications online
- To make themselves aware of the security settings available when using social and blogging websites to protect personal information that is published on-line.

USE OF SOCIAL NETWORKS

- The use of social networking sites such as Facebook, WhatsApp, Twitter, or similar previously listed sites is prohibited during the learning or working day
- Learners must not place photos taken during Rotunda activities on any social network space without explicit agreement from tutor or Education Programme Manager
- Learners are advised not to make contact or chat to anyone who is not known to them and only invite known friends to chat rooms or similar
- Only to accept friendship requests from people they know in real life
- 'Friend' requests must not be made to or by employees
- Learners must consider carefully how the images they share or comments they make may be used or viewed by others. Abusive or bullying language must never be used, nor should any other inappropriate language or comments be made
- Learners and employees must not make comments about Rotunda, employee members, other learners or any other person that could be considered as defamatory or which could bring the Rotunda into

disrepute. Behaviour of this kind will result in disciplinary action being taken in accordance with existing policies
- Inappropriate use of social networking sites may be reported to the site hosting it and inappropriate posts removed.

CYBER-BULLYING

Cyberbullying is the use of ICT, particularly mobile electronic devices and the Internet, deliberately to upset someone else. Any behaviour which seeks to intimidate or humiliate, and which is repeated, intentional, malicious, such as to cause distress, unhappiness or insecurity, is strictly forbidden. Use of electronic devices of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline.

Learners and employees should remember the following:

- Always respect others - be careful what you say online and what images you send
- Think before you send - whatever you send can be made public very quickly and could stay online forever
- Don't retaliate or reply online
- Save the evidence - learn how to keep records of offending messages, pictures or online conversations. Ask someone if you are unsure how to do this. This will help to show what is happening and can be used by Rotunda to investigate the matter
- Block the bully. Most social media websites and online or mobile services allow you block someone who is behaving badly
- Don't do nothing - if you see cyberbullying going on, support the victim and report the bullying
- If you think you, or another person, is being bullied, they should talk to a manager or employee or any trusted adult about it as soon as possible.

The website http://www.digizen.org/ also provides useful support and resources to individuals who may feel uncomfortable with their use of the Internet. Other useful resources include http://www.saferinternet.org.uk and http://www.thinkuknow.co.uk

SAFEGUARDING AND PREVENT

Rotunda recognises that it has a duty under Section 26 of the Counter-Terrorism and Security Act (2015) to have due regard to the need to prevent people from being drawn into terrorism and to promote and safeguard the welfare of children and vulnerable adults (Education Act, Working Together to Safeguard Children and KCSIE).

Managers are responsible for the well-being of the employees and learners and must ensure appropriate material only is accessible through its resources

and networks. Any employees who feels someone is showing an interest in extremist, abusive or inappropriate material should report this to the CEO or Safeguarding Lead in the first instance. Any employees who believes learners have access to inappropriate material should report this to the CEO or Designated Safeguarding Lead.

PROCEDURES

Employees and learners are responsible for their actions, conduct and behaviour on the internet in the same way that they are responsible during workshops and breaks. Use of technology should be safe, responsible and legal. Violations of the rules in this policy will be dealt with in accordance with Rotunda' procedures.

Bullying incidents involving the use of technology will be dealt with under Rotunda' Bullying and Harassment Policy and Disciplinary Procedures.
If there is a suggestion that a learner is at risk of abuse or significant harm, the matter will be dealt with under the Safeguarding Policy and Procedures.

SANCTIONS

Violations of the rules in this policy will result in a temporary or permanent ban from Rotunda activities and termination of employment. Any action taken will depend on the seriousness of the offence. When applicable, the Police or local authorities may be involved including those identified as Safeguarding Incidents which will be reported using our Safeguarding Policy and Incident Report form to the Designated Safeguarding Lead.

MONITORING AND REVIEW

All serious e-safety incidents will be logged. The CEO has responsibility for the implementation and annual review of this policy and will consider the record of e-safety incidents and new technologies with the Safeguarding Lead, where appropriate, to consider whether existing security and e-safety practices and procedures are adequate.

Rotunda Policy Review Record

Reviewed by:	**Approval date:**	**Review frequency:**	**Review date:**	**Signed:**
Maxine Ennis	09/04/2024	Annual	10/04/2025