The JGA Group
Online Safety Policy (incorporating Virtual Communication Protocols)

Introduction

JGA recognises the benefits and opportunities which new technologies offer to teaching and learning. Our approach is to implement safeguards within the Organisation, and to support staff and learners to identify and manage risks.

In line with our duty to safeguard learners and the Every Child Matters agenda, we will do all that we can to make our learners and staff stay safe online and to satisfy our wider duty of care. This Online Safety policy should be read in conjunction with our Safeguarding and Prevent, Bullying and Harassment, Equality, Diversity & Inclusion, Whistleblowing, Data Security, Digital Media and Computer Misuse policies.

Legislation

The Online Harms White Paper, published in April 2019, set out the Government's intention to introduce a new regulatory framework to improve protections for users online. As a result, The Online Safety Act 2023 (legislation.gov.uk) came into force in October 2023 and imposes legal requirements on:

a. Providers of internet services which allow users to encounter content generated, uploaded or shared by other users, i.e. user-generated content ("user-to-user services");
b. Providers of search engines which enable users to search multiple websites and databases ("search services"); and
c. Providers of internet services on which provider pornographic content is published or displayed.
d. The legislation requires providers of regulated user-to-user and search services to:

    i. assess the risks of harm to those users present on the service;
    ii. take steps to mitigate and manage the risks of harm to individuals arising from illegal content and activity, and (for services likely to be accessed by children) content and activity that is harmful to children. Providers will also need to assess the risk of their services being used for the commission or facilitation of a priority offence and to design and operate their services to mitigate this risk;
    iii. put in place systems and processes which allow users and affected persons to report specified types of content and activity to the service provider;
    iv. establish a transparent and easy to use complaints procedure which allows for complaints of specified types to be made;
    v. have particular regard to the importance of protecting users' legal rights to freedom of expression and protecting users from a breach of a legal right to privacy when implementing safety policies and procedures
    vi. put in place systems and processes designed to ensure that detected but unreported CSEA content is reported to the National Crime Agency (NCA).

Definition of Online Safety

The term Online Safety is defined for the purposes of this document as the process of limiting the risks to children, young people and vulnerable Adults when using Internet, Digital and Mobile Technologies (IDMTs) through a combined approach to policies and procedures, infrastructures and education, including training, underpinned by standards and moderation.

Online Safety risks can be summarised under the following three headings.

Content

- Exposure to age-inappropriate material (including sexting)
- Exposure to inaccurate or misleading information
- Exposure to socially unacceptable material, such as that inciting violence, hate, extremism or intolerance
- Exposure to illegal material, such as images of child abuse
- Illegal Downloading of copyrighted materials e.g. music and films

Contact

- Cyber predators - Grooming using communication technologies, potentially leading to sexual assault or child prostitution
- Radicalisation the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups.
- Cyber bullying via websites, mobile phones or other forms of communication device. Emotional abuse that could include blackmail.
- PPI - posting personally identifiable information) - individuals not understanding social boundaries which could put them at risk
- Phishing - cyber security professionals using emails to try to encourage individuals to click on links or other attachments. They may pose as a legitimate company or a relative. They may use 'Smishing' which is sending similar links by email.
- Accidentally downloading Malware to perform harmful actions on a computer

Commerce

- Exposure of minors to inappropriate commercial advertising
- Exposure to online gambling services
- Commercial and financial scams

Scope

The policy applies to all persons who have access to Organisation IT systems, both on premises and remote access. The Online Safety Policy applies to all use of the internet and electronic communication devices such as e-mail, mobile phones, social networking sites, and any other systems that use the internet for connection and providing of information.

Aims

The aims are to:

- ensure safeguards on organisation IT-based systems are strong and reliable
- ensure user behaviour is safe and appropriate
- assure that the storage and use of images and personal information on organisation IT- based systems is secure and meets all legal requirements
- educate Staff and learners in Online Safety and be proactive in alerting them of current risks
- ensure any incidents which threaten Online Safety are managed appropriately

Outcomes

Security

Organisation networks are safe and secure, with appropriate and up-to-date security measures and software in place.

Risk assessment

When making use of new technologies and online platforms, staff are to assess the potential risks that they and their learners could be exposed to.

Behaviour

- It is strictly forbidden to download or transmit any material which might reasonably be considered obscene, abusive, sexist, racist, defamatory, related to violent extremism or terrorism or which is intended to annoy, harass, or intimidate another person. This also applies to use of social media systems accessed from Organisation systems.
- All users of technology adhere to the standards of behaviour set out in the JGA Data Security and Digital Media and Computer Misuse Policies. All users of IT adhere to Organisation guidelines when using email, mobile phones, social networking sites, chat rooms, video conferencing and web cameras, etc.
- Any abuse of IT systems and any issues of bullying or harassment (cyber bullying) are dealt with seriously, in line with staff and learner disciplinary procedures.
- Any conduct considered illegal is reported to the police. Staff must take responsibility for moderating any content posted online.
- Staff should be aware of cyber bullying, grooming law and child protection issues and forward any concerns to the Designated Safeguarding Lead.
- Staff should keep personal and professional lives separate online; staff should not have students as ‘friends’ on social media sites that share personal information.
- Staff should be wary of divulging personal details online and are advised to look into privacy settings on sites to control what information is publicly accessible.

- Staff should recognise that they are legally liable for anything they post online. Staff are expected to adhere to the organisation's Equality, Diversity & Inclusion policy at all times and not post derogatory, offensive or prejudiced comments online.
- Staff should not bully or abuse colleagues/learners online. Staff entering into a debate with a learner online should ensure that their comments reflect a professional approach.
- Staff should not post any comments online that may bring the organisation into disrepute or that may damage the organisation's reputation.
- Staff wishing to debate and comment on professional issues using personal sites, should be aware that this may be seen as a reflection of organisation views, even with a disclaimer, and should consider their postings carefully.
- Staff should not use their organisation e-mail address to join sites for personal reasons or make their organisation e-mail address their primary contact method.
- Staff should be aware that any reports of them undertaking inappropriate online activity that links them to the Organisation will be investigated and may result in disciplinary action.

Use of images and video

The use of images or photographs is encouraged in teaching and learning, e.g. recording progress via case studies (before and after treatments), providing there is no breach of copyright or other rights of another person. Staff and learners are trained in the risks of downloading, posting and sharing images, and particularly in the risks involved in posting personal images onto social networking sites, for example. JGA staff provide information to learners on the appropriate use of images, and on how to keep their personal information safe. Advice and approval from a senior manager is sought in specified circumstances or if there is any doubt about the publication of any material.

Personal information

Processing of personal information is done in compliance with the JGA Data Security Policy and Procedure. Personal information is kept safe and secure and is not passed on to anyone else without the express permission of the individual. No personal information is posted to the Organisation website/intranets without the permission of a senior manager. Staff keep learners' personal information safe and secure at all times. When using an online platform, all personal information is password protected. No personal information of individuals is taken offsite unless the member of staff has the permission of their line/contract manager. Every user of IT facilities logs off on completion of any activity. Organisation mobile devices that store sensitive information are encrypted and password protected.

Personal data no longer required is securely deleted. Where an Awarding Organisation is conducting online examinations/assessments, their specific requirements are followed at all times.

Education and Training

Staff and learners are supported through training and education to develop the skills to be able to identify risks independently and manage them effectively. Learner inductions and tutorials contain sessions on Online Safety. Learners are guided in Online Safety across the curriculum and opportunities are taken to reinforce e- safety messages.

Learners are encouraged to embrace ICT equipment during lessons and they will sometimes use JGA laptops or tablets or their own phones to research. Tutors will actively monitor use of equipment at these times to ensure learners are (a) doing the task that has been assigned and (b) they are not accessing any sites that have no relevance to their learning or others that may put them at risk.

JGA will ensure that its ICT equipment has appropriate Malware and Anti-Virus software so that data storage risks are minimalised. Laptops and tablets are checked annually for servicing and updating any necessary software. JGA holds both Cyber Essentials and Cyber Essentials Plus accreditations which are inspected and renewed annually.

Incidents and Response

A clear and effective incident reporting procedure is maintained and communicated to learners and staff. Reports of Online Safety incidents are acted upon immediately to prevent, as far as reasonably possible, any harm or further harm occurring. Action following the report of an incident might include disciplinary action, sanctions, reports to external agencies (e.g. the police), review of internal procedures and safeguards, tutor support for affected learners, etc.

Where an Online Safety incident is reported to JGA the matter, we will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring. If a learner wishes to report an incident, they can do so to their tutor/coach or Learner Progress Adviser, the Designated Safeguarding Officer, or Director of Quality and Performance (SMT Safeguarding Lead). Where a member of staff wishes to report an incident, they should contact their line/contract manager as soon as possible.

Following any incident, the Organisation will review what has happened and decide upon the most appropriate and proportionate course of action. Sanctions may be put in place, external agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident. Serious incidents will be dealt with by senior management, in consultation with appropriate external agencies.

Responsibilities

Maintaining best practice in IT procedures and practices to manage any Online Safety risks effectively is paramount. The following are responsible for implementing it:

- The resident IT Consultant for championing good Online Safety practice in Organisation IT facilities and processes, and for providing technical expertise when issues are being investigated

- Designated Safeguarding Lead (DSL) for all Online Safety matters in relation to Organisation Learners
- Tutors/Coaches/Learner Progress Advisers for providing pastoral and practical support for learners dealing with issues related to Online Safety and for incorporating Online Safety into learner induction. Also for embedding Online Safety education and practice into the learner's programme.
- All Staff for implementing good Online Safety practice and safeguards consistent with this policy in their area of responsibility and staying alert to any risks, reporting any concerns promptly to the DSL.

Key Contacts:

Paula Wakelin, Designated Safeguarding Lead: paula.wakelin@jga-group.co.uk
Richard Brady, Deputy Designated Safeguarding Lead: richard.brady@jga-group.co.uk
Ray Green, resident IT Consultant: ray.green@jga-group.co.uk
Susan Prestridge, Operations Director: susan.prestridge@jga-group.co.uk
Lisa MacCormac, Director of Quality & Performance: lisa.maccormac@jga-group.co.uk

Annex A: Virtual Communications Protocols (p7)

Policy Issued	July 2024
Version No	V1
Last Review	N/A
Next Review	July 2025
Policy Owner	Lisa MacCormac, Director of Quality & Performance

Annex A: Virtual Communication Protocols

General Security Tips when using online platforms (Zoom, Teams, GoTo, Skype, etc)

1. If the platform allows, create a unique ID to provide added protection for large meetings, usually found under Meeting Options (certainly for Zoom)

2. Enable Require a Meeting Password and only send the password to those you have specifically invited to attend

3. Create a Waiting Room, where meeting attendees are let in (either all at once or one at a time) by the host at the specified time

4. For additional security, the Host can choose to limit screen sharing, either to themselves alone or to designated participants. This can be done in advance or during the meeting

5. Create an "invite only" meeting so that only those you have specifically invited can join, using the same email address to sign in that was used to invite them

6. If the platform allows, lock the meeting once all participants have joined

7. The Host can choose to remove participants from the call or put them on hold if they are disruptive. Equally, the Host can choose to disable their camera or place them on Mute

8. Disable the private chat function if there is a possibility that it could distract participants or provide a vehicle for inappropriate comments

Conducting Online Meetings

- Ensure that online meetings serve a specific purpose and that this is the most appropriate way to address it. If it's something that can be resolved by sending a quick email or in another, less time consuming way, don't make your team spend their time sitting through an unnecessary meeting. Similarly, only invite those who are essential to the conversation

- Make sure your meeting has an agenda, aim and objectives and that there are clear actions at the end of it. Stick to the topic and remember that the maximum period a person can concentrate for at any one time is 2 hours; ensure your meeting time is appropriately paced and factor in comfort breaks

- Attend on time and keep to time

- If a follow-up meeting is required, ensure that it is focused and is not just an opportunity to cover old ground. Again, make sure actions are closed or updated and that everybody is clear about them

- Speak clearly, ensure everybody can hear you and suggest that all attendees remain muted when not speaking to minimise unnecessary background noises

Conducting Online Training

- Observe the protocols for conducting online meetings above

- Unless there is a specific and agreed reason for not doing so, expect all participants to turn on their video screens. This is because it enables you to see if everybody is engaged and assess levels of learning but also provides an environment that learners are more used to working in and encourages greater interaction between them

- If any participant is unable to use their video screen, ensure you use targeted questioning and other assessment methods to monitor engagement and learning levels

- Consider the individual and collective needs of your audience and make sure any required adjustments are in place. For example, some people on the autism spectrum may struggle with video calling, as it can exacerbate sensory triggers such as loud noise and bright lights

- Take regular "temperature checks" to ensure that the environment and content of the training are appropriate. Get regular feedback from your learners and make adjustments as required. For example, a full day of online training on some topics may be too exhausting, even with scheduled breaks built in. It may be more appropriate to consider delivery over a longer period, for example two half-days, instead.