ONLINE SAFETY POLICY

INTRODUCTION

The use of technology has become an established and integral part of learning through the use of online resources, online delivery and remote working. Learners and staff have access to technology and resources that have a significant and positive impact on learning. Young people need to develop good skills in using technology to maximise its use as a learning tool and prepare themselves for future employment and careers. Technology is established as a supportive tool in good teaching and learning however, it has also established itself as significant component of many safeguarding issues.

The purpose of this policy statement is to:

- Ensure the safety and wellbeing is paramount when staff and learners are using the internet, social media or mobile devices.
- Provide staff, learners and volunteers, with the overarching principles that guide our approach to online safety.
- Ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

We believe that:

- Our learners and staff should never experience abuse of any kind.
- Our learners and staff should be able to use the internet for education and personal development, but safeguarding procedures need to be in place to ensure they are kept safe at all times.

We recognise that:

- The online world provides everyone with many opportunities; however, it can also present risks and challenges.
- We have a duty to ensure that all young people and adults involved in our organisation are protected from potential harm online.
- We have a responsibility to help keep learners safe online, whether or not they are using JTM's network and devices.
- Working in partnership with learners, their parents, carers and other agencies is essential in promoting their welfare and in helping learners be responsible in their approach to online safety .
- Regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, we all have the right to equal protection from all types of harm or abuse.

POLICY SCOPE

This policy is a living document, subject to full annual review but also amended where necessary during the year in response to developments within JTM, emerging themes or trends within the wider community or any changes in national guidance.

This policy applies to all staff, learners and other stakeholders of JTM who have access to our digital technology, networks and systems, whether on-site or remotely, or who use technology in their role and should be read alongside the IT Policy (QP_034) and Online

ONLINE SAFETY POLICY

Code of Conduct and Acceptable Use of Technology Policy (QP_208)
The policy aims to:

- Set out expectations for online behaviour, attitudes and activities and use of digital technology (including when devices are offline) for all JTM staff and learners.
- Help all to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the organisation regardless of device or platform.
- Facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare all learners for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Help JTM staff working with learners to understand their roles and responsibilities, to work safely and responsibly with technology and the online world for the protection and benefit of themselves and that of the learners, minimising misplaced or malicious allegations and to better understand their own standards and practice.
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns with reference to other policies such as Behaviour Policy or Anti-Bullying Policy.

We will seek to keep staff and learners safe by:

- Appointing an Online Safety Coordinator . This is Tom Sumnall, contact details in appendix 1.
- Providing clear and specific directions to staff and volunteers on how to behave online through our Online Code of Conduct and Acceptable Policy Use for staff and learners.
- Online safety and expectations when using technology for teaching and learning is discussed at induction and included in Learners Induction Handbook.
- Through our teaching and learning, provide learners with the support, encouragement and information to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others.
- Where appropriate supporting and encouraging parents and carers to do what they can to keep their children safe online.
- The use of acceptable use agreements for use by staff.
- Developing clear and robust safeguarding procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by a staff member or learner.
- Reviewing and updating the security of our information systems regularly through our third-party IT support ICU Group.
- Ensuring that usernames, logins, email accounts and passwords are used effectively.
- Ensuring personal information about the learners who are involved in our organisation is held securely and shared only as appropriate.
- Ensuring that images of learners are used only after their written permission has been obtained, and only for the purpose for which consent has been given.
- Ensuring parental consent is in place for participating in online learning for under 18-year-old learners.
- Providing supervision, support and training for staff and volunteers about online safety.

ONLINE SAFETY POLICY

If online abuse occurs, we will respond to it by:

- By taking all reasonable precautions to ensure online safety but recognises that incidents can occur both within the work/training environment and outside, and that those incidents can continue to impact on learners within the work/training environment . All members of JTM staff are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through our safeguarding procedures and where necessary liaise with employers
- Concerns will be handled in the same way as any other safeguarding concern following established and robust safeguarding procedures for responding to abuse (including online abuse).
- Providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying or cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation.
- Making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account.
- Reviewing at regular intervals any support plan developed to address online abuse, in order to ensure that any problems have been resolved in the long term.
- Any concern/allegation about staff misuse is referred to the DSL and General Manager unless the concern is about these individuals in which case the concern will be referred to the Apprenticeship and Training Manager Claire Fairhurst. Safeguarding procedures for dealing with an allegation against a staff member will be followed, advice and support will be sought form the LADO (Local Authority's Designated Officer) if appropriate.
- If appropriate parents/carers of online-safety incidents involving their child will be notified and Children Social Care/ Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law (particular procedures are in place for sexting and up skirting; see section below**.**

How will this policy be communicated?

This policy can only impact upon practice if it is a (regularly updated) living document. Therefore, it is accessible to and understood by all stakeholders. It is communicated in the following ways:

- Posted on the organisation's website.
- Included in induction of staff and learners.
- Integral to safeguarding updates and training for all staff.
- Clearly reflected in the Online Code of Conduct and Acceptable Use Policies for staff and learners which are issued to all learners and staff at induction and updated/reviewed annually.

What are the main online safety risks today?

Online-safety risks are traditionally categorised as one of the 3 Cs: Content, Contact or Conduct (identified by Professor Tanya Byron's 2008 report "Safer children in a digital world"). These three areas remain a helpful way to understand the risks and potential response, whether technological or educational. They do not stand in isolation, however, and it is important to understand the interplay between all three.

Many of these new risks are mentioned in KCSIE 2022, e.g. extra-familial harms where children are at risk of abuse or exploitation to multiple harms in situations outside their

ONLINE SAFETY POLICY

families including sexual exploitation, criminal exploitation, serious youth violence, up skirting and sticky design.
In past and potential future remote learning and lockdowns, there is a greater risk for grooming and exploitation (CSE, CCE and radicalisation) as more time is spent at home and on devices. There is a real risk that some learners may have missed opportunities to disclose such abuse during the lockdowns or periods of absence.

Sexting – sharing nudes and semi-nudes
refer to the updated UK Council for Internet Safety (UKCIS) guidance on sexting - now referred to as Sharing nudes and semi-nudes: https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-peopleadvice for education settings to avoid unnecessary criminalisation of children.

NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.
There is a one-page overview called Sharing nudes and semi-nudes: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/947546/Sharing_nudes_and_semi_nudes_how_to_respond_to_an_incident_Summary_V2.pdf how to respond to an incident for all staff to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of an incident, and it is vital that the correct steps are taken.

Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.
The DSL will in turn use the full guidance document, Sharing nudes and semi-nudes – https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/947545/UKCIS_sharing_nudes_and_semi_nudes_advice_for_education_settings_V2.pdf advice for educational settings to decide next steps and whether other agencies need to be

Up skirting:

- It is important that everyone understands that up skirting (taking a photo of someone under their clothing, not necessarily a skirt) is now a criminal offence.

Bullying :

- Online bullying should be treated like any other form of bullying and the bullying policy should be followed for online bullying, which may also be referred to as cyberbullying, including issues arising from banter.

Sexual violence and harassment:

DfE guidance on sexual violence and harassment is referenced in Keeping Children Safe in Education (2022) and also a document in its own right. All staff must read Part one of this document as a minimum: paragraphs 51-57 cover the immediate response to a report and confidentiality which is highly relevant for all staff; the case studies section provides a helpful overview of some of the issues which may arise. Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance. Staff must work to foster a zero-tolerance culture. The guidance stresses that education settings must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as ‘low level’ are treated

ONLINE SAFETY POLICY

seriously and not allowed to perpetuate. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language

Related policies and procedures

This policy statement should be read alongside our organisational policies and procedures, including:

- Safeguarding and Prevent Policy and Procedure (QP_014)
- Emergency Planning and Covid-19 Response Policy (QP_115A)
- Induction Handbook (QD_020)
- Password and Security Policy (QD_034)
- Bullying and Harassment Policy (QP_015)
- Learner Behaviour Policy (QP_117)
- IT Policy (QP_034)
- Online Code of Conduct and Acceptable Use of Technology Policy (QP_208)
- Retention of Records Policy (QP_041)

APPENDIX 1

KEY CONTACT INFORMATION:

Safeguarding Team:

Role	Name	Email	Phone
Designated Safeguarding Lead	Gina Stephens	Gina.stephens@jarvis-eu.com	07867260276
Deputy Designated Safeguarding Lead and Online Safety and Prevent Co-ordinator	Tom Sumnall	tom.sumnall@jarvis-eu.com	07741743618
Deputy Designated Safeguarding Lead and Pastoral Support Co-ordinator	Janine Ridley	janine.ridley@jarvis-eu.com	07771672491
Additional staff who are DSL trained if the Safeguarding Team are unavailable			
General Manager	Sarah McCarthy	sarah.mccarthy@jarvis-eu.com	07764203649
Apprenticeship & Training Manager	Claire Fairhurst	claire.fairhurst@jarvis-eu.com	07775950929