1st Floor
Bishops House
Artemis Drive
Tachbrook Park
Warwick
CV34 6UD UK

Phone: +44 (0) 1926 333680
Email: info@widgit.com

www.widgit.com

Safeguarding Policy

1. Policy Purpose

Safeguarding means protecting peoples' health, wellbeing and human rights, and enabling them to live free from harm, abuse and neglect. The purpose of this policy is to provide an environment where all can work safely; The company will take every reasonable precaution to minimise risk whilst working at our own premises with staff and others associated with Widgit such as, contractors, stakeholders, partners, customers and/or visitors. This policy will also cover social media and e-safety.

2. Policy Statement

Widgit believes that everyone we come into contact with, regardless of age, gender identity, disability, sexual orientation or ethnic origin has the right to be protected from all forms of harm, abuse, neglect and exploitation. We will not tolerate abuse and exploitation by staff or associates.

It is the responsibility of all staff at Widgit to raise any concerns you have or any concerns which are reported to you according to this policy.

3. Roles and Responsibilities

Widgit has a duty of care to provide a safe environment for all staff and its associates by:

- Ensuring that everyone understands their safeguarding accountabilities and responsibilities.
- Contributing to the creation and maintenance of a safe environment.
- Promoting safe practice and challenging poor or unsafe practice.
- Identifying where there are concerns and taking appropriate action to address them.

Widgit commits to addressing safeguarding throughout its work, and will take responsibilities for:

- Prevention
- Reporting
- Response

Prevention

Widgit as a company will:

- Make this policy available to all staff and publicly, provide appropriate means for staff to become familiar with, and know their responsibilities within this policy.
- Work in a way that protects people from any risk of harm that may arise from their coming into contact with Widgit. This includes the way in which information about individuals who work with us or use our services is gathered and communicated.
- Record and store information professionally and securely.
- Provide a safe physical environment for staff and its associates, by applying health and safety measures in accordance with the law and regulatory guidance.
- Review this policy annually.

Widgit staff and associated persons are obliged to:

- Contribute to creating and maintaining an environment that prevents safeguarding violations and promotes the implementation of the Safeguarding Policy.
- Value, listen to and respect all people whom they come into contact with.
- Report any concerns or suspicions regarding safeguarding violations by staff or associated persons to the appropriate person.

Additionally, staff and all others associated with Widgit must not:

- Sexually abuse or exploit anyone.
- Subject anyone to physical, emotional or psychological abuse or neglect.
- Use language, make suggestions or offer advice which is inappropriate or sexually proactive.
- Exchange money, employment, goods or services for sexual activity.

Reporting

The company will establish safe, appropriate and accessible means of reporting safeguarding concerns for staff.

Staff – Staff members who have a complaint or concern relating to safeguarding should report it immediately to their line manager. If the staff member does not feel comfortable reporting to their line manager (for example, if that person is implicated in the concern) they must report to any other appropriate senior member of staff.

People other than staff – Any other associated person who has a complaint or concern relating to safeguarding should contact Widgit by email in the first instance at confidential@widgit.com or by phone on 01926 333680, where you will be directed to the appropriate senior member of staff.

Response

Widgit will follow up safeguarding reports and concerns in a timely manner.

Widgit will apply appropriate disciplinary measures to staff found in breach of policy. Where staff or associated persons have caused harm to a person, regardless of whether or not a formal internal response is initiated (such as an internal investigation), the company will offer appropriate support to that person.

4. Written Records

The relevant person will retain a copy of the report; any notes, memoranda or correspondence dealing with the matter; and any other relevant material. Copies of reports, notes etc. should be kept secure at all times. The member of staff who has cause for concern should make a full record as soon as possible. The record should include the nature of the allegation and any other relevant information including:

- Date, time and place where the safeguarding concern occurred.
- Names of others present.
- Name of the complainant and, where different, the name of the person who has allegedly been abused; nature of the alleged abuse.
- Description of any injuries/incidents observed; and the account which has been given of the allegation.

5. Guidelines for Staff

This procedure must be followed whenever any member of staff hears an allegation from a vulnerable person that abuse has, or may have, occurred or where there is a significant concern that there may be such abuse.

- Listen to what is said.
- Accept what you are told – you do not need to decide whether or not it is true.
- Listen without displaying shock or disbelief.
- Reassure the person reporting their concern.
- Do not promise confidentiality.
- Do not promise that "everything will be alright now" (it might not be).
- Respond to the person reporting but do not interrogate.
- Avoid leading questions but ask open ended ones.
- Clarify anything you do not understand.
- Explain what you will do next, i.e. inform a senior member of staff / appropriate person.
- Make notes as soon as possible – during the interview if you can.
- Use the person's own words – do not assume – ask, e.g. "Please tell me what xxxxx means".
- Include: time date place.
- Describe observable behaviour and appearance.
- Cross out mistakes – do not use correction fluid.
- Do not destroy your original notes – they may be needed later on and must be given to the senior member of staff / appropriate person.
- Consider what support is needed for the vulnerable person – you may need to give them a lot of your time or they may need to be referred for counselling.
- Ensure you are supported – such interviews can be extremely stressful and time consuming.
- Once reported to the senior member of staff / appropriate person, they will take responsibility for the matter and will take all of the necessary actions. However, if you have questions or need additional support, then ask.

6. Whistleblowing

It is important that people within Widgit have the confidence to come forward to speak or act if they are unhappy with anything. Whistleblowing occurs when a person raises a concern about dangerous or illegal activity, or any wrong- doing within their organisation. This includes concerns about safeguarding. There is also a requirement by Widgit to protect whistleblowers.

Please refer to our Whistleblowing Policy:

IT and Data Protection / Whistleblowing Policy.PDF

7. Social Media & E-safety

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

Staff and all associated persons are personally responsible for what they communicate on social media and other digital platforms, and when using Widgit's internet and equipment – both on behalf of Widgit and in a personal capacity.

- Widgit will not accept anyone behaving in a threatening, bullying or abusive way online – whether in a professional or personal capacity.
- Staff responsible for the creation of online content on Widgit accounts and platforms (e.g. Tweets and Facebook posts) should seek advice and sign-off from their line managers on sensitive content, or where they are concerned about the appropriateness of the content.
- For safeguarding reasons, people should not be tagged in online or social media posts.
- Where possible, staff should not make use of their personal social media accounts to carry out their work for Widgit-related projects, events or initiatives. If possible, a new account should be opened that enables the staff member to maintain boundaries between their personal and professional lives.
- Widgit staff and its associates should not have private conversations with under 18s through email, or through accounts on social media or online platforms.
- Widgit should provide guidelines on settings and privacy to people engaging in digital spaces for Widgit initiatives to protect them from harmful behaviour.
- Sharing online content of people involved in Widgit's work on social media should follow the guidelines on privacy, data protection, informed consent, safe programming and risk management.

8. Media Sharing

All photos, videos and media content captured must, prior to sharing internally and / or externally, have the prior consent of all individuals involved. When planning to capture a Widgit colleague or client, permission must be sought beforehand to avoid putting individuals on the spot; this includes the recording of Teams and Zoom calls, or any other video conferencing platform.

All media content, regardless of audience, must be reviewed completely before distribution. For example, if a full-length recording is to be shared, the individual circulating the content must watch the entire video beforehand for confidentiality / quality assurance purposes.

9. Privacy, Data Protection and Informed Consent (digital)

Widgit has a duty of care to protect the digital data and content of staff, associates and anyone else involved in Widgit's work, even when an informed decision is made to share this content.

Widgit must take every reasonable precaution to ensure that any digital data or content does not place people at risk or render them vulnerable to any form of harassment, abuse or exploitation.

Research which involves digital elements, such as online surveys or platforms, must be well thought through and appropriate for the context. Special considerations must be given to data protection concerns and mitigating risk to research participants.

Other related Widgit policies include:

- Data Protection
- Information Security

All information stored digitally and online by Widgit must be processed in accordance to these policies, which may reflect national or regional laws on which Data Protection policies are based, such as the General Data Protection Regulation (GDPR) in the European Union (2018).

10. Confidentiality

Staff and associated persons will maintain confidentiality at all stages of the process when dealing with safeguarding concerns. Information relating to the concern will be shared strictly on a need to know basis, and will be kept secure at all times. Information will only be shared in line with the General Data Protection Regulations (GDPR) and Data Protection. The following principals apply:

- Staff should never offer complete confidentiality. All staff need to understand how to share information legally and professionally.
- The Data Protection Act is not a barrier to sharing information but provides a framework to ensure that personal information about living persons is shared appropriately.

- Be open and honest with the person from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.
- Base your information sharing decisions on considerations of the safety and wellbeing of the person and others who may be affected by their actions.
- Ensure any information shared is accurate and up to date, is shared in a timely fashion, and is shared securely.
- Keep a record of your decision around whether or not to share information, what you have shared, with whom and for what purpose.

11. Policy Review

This policy will be reviewed **every 3 years**, or sooner if changes in legislation occur or new best practice evidence becomes available.

Document Control	
Version Number	v 1.1
Date Ratified	29 November 2021
Date Issued	11 July 2024
Next Review Date	11 July 2027