real arts workshops

Search for our hash-tag to see our work:
#GivingPeopleACreativeVoice

Cyber Security Policy

We treat all company digital information as highly critical.

This includes (but not exhaustively): documents, photographs, emails, presentations, policies, schemes of work, plans, spreadsheets, resources, customer surveys, videos, quotations, designs, staff information, customer information, meeting notes, marketing and promotions, website, social media, contracts, consent forms, testimonials, newsletters, monitoring reports and social impact reports, financial reporting, branding, letters, invoices, blogs, insurances, DBS details.

It is therefore extremely important that this data is stored, safeguarded and protected on a regular basis.

- We use 2 x solid external hard drives and 2 different cloud based solutions (Google Drive and DropBox) to manage all this data.
- Only the owners of the company have access to this data and the company social media accounts.
- We have malware protection and anti-virus software (McAfee) installed in all our devices.
- All our devices are password protected.
- Our software is regularly updated.
- The staff area of our website is password protected.
- We regularly use ‘Report Spam’ on our emails.

In line with the National Cyber Security Centre Small Business Guide Actions, we will

- Identify and record essential data for regular backups
- Create password policy
- Sign up to threat alerts
- Switch on our Firewall

- Make sure Anti-virus software is running
- Ensure data is being backed up to a secondary back up (ie external drive AND the Cloud)
- Ensure all applications are up to date

September 2021