SupaJam Online Safety Policy

August 2023

(Next review date August 2024)

Safeguarding Statement

SupaJam is a post 16 specialist provider, specialising in Music, Maths, English and Life Skills. All staff, volunteers and partners are committed to safeguarding the welfare of every person within SupaJam. Our mission is to help young people to engage and achieve within a safe and inclusive environment.

1. Principles

1.1 - All students at SupaJam Education in Music and Media (The College) have access to a range of new technologies for communicating and collaborating. It is essential that all students are safe and the same principles should apply to the 'virtual' or digital world as would be applied to The College's physical buildings.

1.2 - E-Safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

1.3 - Online technologies provide many different platforms for positive engagement, including Social Media but also provides opportunities for various levels of harm. Online technologies should be safe to use and the college will have protocols in place to respond to any incident where harm is, or may be caused, using online technologies.

2. Purpose of this policy

2.1 - SupaJam's Online Safety Policy;

- Sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- Allocates responsibilities for the delivery of the policy
- Is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- Establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the college and how they should use this understanding to help safeguard learners in the digital world
- Describes how SupaJam will help prepare learners to be safe and responsible users of online technologies
- Establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- Is supplemented by a series of related acceptable use agreements
- Is made available to staff at induction and through normal communication channels such as the Google Drive, Email, links to guidance and a policy reading list that supports the overarching safeguarding at SupaJam.
- Is published on SupaJam's website.

3. Responsibilities

Senior Leaders

3.1 - Senior Leaders have a duty of care for ensuring the safety (including online safety) of members of the SupaJam community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety may be delegated to the DSLs.

3.2 - The Director of Safeguarding is aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. This process is outlined in SupaJam's Online Incident Response Plan.

3.3 - Senior Leaders are responsible for ensuring that the Online Safety Lead, technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.

3.4 - The Director of Safeguarding is responsible for;

- Procuring filtering and monitoring systems
- Documenting decisions on what is blocked or allowed and why
- Reviewing the effectiveness of online provision and its safety
- Overseeing reports
- Making sure staff understand their roles, are appropriately trained and follow processes, policies and procedures
- Act on reports or concerns

Designated Safeguard Leads

3.5 - The Designated Safeguarding Leads will:

- Take the lead with online safety for their base.
- Take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns
- Have a role in establishing and reviewing SupaJam's online safety policies/documents alongside the Director of Safeguarding.
- Promote an awareness of and commitment to online safety education / awareness raising across SupaJam and beyond.
- Liaise with the Vocational Co-ordinators to ensure that the online safety curriculum is planned, mapped, embedded and evaluated.
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents.
- Receive reports of online safety incidents and create a log of such incidents to inform future online safety developments.
- Oversee and act on filtering and monitoring reports
- Oversee and manage safeguarding concerns

- Carry out checks on filtering and monitoring systems
- Provide (or identify sources of) training and advice for staff/parents/carers/learners
- Meet regularly with the Director of Safeguarding and the IT Team to discuss current issues, review (anonymised) incidents and if possible, filtering and monitoring logs
- Report regularly to the Director of Safeguarding

Teaching and support staff (including volunteers)

3.6 - SupaJam teaching staff are responsible for ensuring that:

- They have an awareness of current online safety matters/trends and of the current SupaJam Online Safety Policy and practices
- They understand that online safety is a core part of safeguarding
- They have read, understood, and signed the staff acceptable use agreement (AUA)
- They immediately report any suspected misuse or problem to the DSL for investigation/action, in line with SupaJam's safeguarding procedures.
- All digital communications with learners and parents/carers will be completed with professionalism at all times and only carried out using official college systems such as email, main line phones, work mobile devices or Google Chat.
- Online safety issues are embedded in all aspects of the curriculum and other activities
- Learners understand and follow the Online Safety Policy and acceptable use policy, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other college activities (where allowed) and implement current policies regarding these devices
- IWhere internet use in lessons is pre-planned, learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies.
- Have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- They model safe, responsible, and professional online behaviours in their own use of technology, including out of college and in their use of social media.

IT and Filtering System Provider (Blaucomm)

3.7 - SupaJam uses the company Blaucomm to provide some of its technology services. It is SupaJam's responsibility to ensure that Blaucomm puts in place all of the online safety measures that SupaJam's obligations and responsibilities require. It is also important that the provider follows and implements SupaJam's Online Safety Policy and procedures.

3.8 - The technology service (Blaucomm) provides uses the monitoring system Sophos to manage and monitor online activity. Blaucomm, in partnership with SupaJam, is responsible for ensuring that:

- They are aware of and follow SupaJam's Online Safety Policy and Internet Safety Policy to carry out their work effectively
- SupaJam's technical infrastructure is secure and is not open to misuse or malicious attack
- SupaJam meets (as a minimum) the required online safety technical requirements as identified by the local authority or other relevant body
- There is clear, safe, and managed control of user access to networks and devices
- They keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- The use of technology is regularly and effectively monitored in order that any misuse/ attempted misuse can be reported to the Director of Safeguarding for investigation and action
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
- Monitoring software/systems are implemented and regularly updated as agreed in SupaJam policies

Students

3.9 - Students are responsible for;

- Using SupaJam's digital technology systems in accordance with the student acceptable use agreement and Online Safety Policy (this should include personal devices – where allowed
-)Understanding the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Knowing what to do if they or someone they know feels vulnerable when using online technology.
- Understanding the importance of adopting good online safety practice when using digital technologies outside of SupaJam.

Parents/Carers

3.10 - Parents and carers will be encouraged to support SupaJam by:

- Reinforcing the online safety messages provided to learners in college
- Promoting acceptable use of their child's personal devices in college (where this is allowed)

Community users/Visitors

3.11 - Community users who access SupaJam's systems/website/learning platform as part of the wider college provision will be expected to sign or agree to a community user AUA before being provided with access to SupaJam's systems.

3.12 - SupaJam encourages the engagement of agencies/members of the community who can provide valuable contributions to the online safety provision and actively seeks to share its knowledge and good practice with other schools and the community.

4. Acceptable Use

4.1 - The Online Safety Policy and acceptable use agreements define acceptable use at the college. The acceptable use agreements will be communicated/re-enforced through:

- Student Code of Conduct
- Staff induction and handbook
- Posters/notices around where technology is used
- Communication with parents/carers
- Education sessions
- SupaJam's website
- Peer support.

4.2 - For full information please refer to SupaJam's Acceptable Use Policy.

5. Using Communication Technologies

5.1 - SupaJam considers the following as good practice:

- When communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by SupaJam
- Any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. Personal e- mail addresses, text messaging or social media must not be used for these communications under any circumstances.
- Staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of SupaJam and its community and not use it in any way which may bring disrepute to the individual or the organisation.
- Staff will immediately report to the DSL the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Students will be encouraged to follow the same guidance.
- Relevant policies and permissions should be followed when posting information online e.g., the college website and social media. Only SupaJam e-mail addresses should be used to identify members of staff and learners.

6 - Responding to and Reporting on Online Harm, Including Sexual Abuse & Harassment and Malicious Incidents

6.1 - In 2021, Ofsted's "Review of Sexual Abuse in Schools and Colleges" highlighted the need for schools to understand that reporting systems do not always respond to the needs of learners. While the report looked specifically at harmful sexual behaviours, it was noted that schools may wish to address these issues more generally in reviewing their reporting systems.

6.2 - The Ofsted review recommended that:

"School and college leaders should create a culture where sexual harassment and online sexual abuse are not tolerated, and where they identify issues and intervene early to better protect children and young people. In order to do this, they should assume that sexual harassment and online sexual abuse are happening in their setting, even when there are no specific reports, and put in place a whole-school approach to address them." (https://www.gov.uk/government/publications/review-of-sexual-abuse-in-schools-and-colleges/review-of-sexual-abuse-in-schools-and-colleges)

6.3 - In order to safeguard all learners, SupaJam will;

- Promote a culture of openness to the discussions of online safety, including abuse and manage incidents robustly
- Ensure that there are clear reporting routes which are understood and followed by all members of the SupaJam community which are consistent with SupaJam's safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- Maintain routine record-keeping and analysis of sexual harassment and sexual violence, including online, to identify patterns and intervene early to prevent abuse
- Take all reasonable precautions to ensure online safety for all college users but recognises that incidents may occur inside and outside of the college (with impact on SupaJam) which will need intervention.
- Ensure all members of the SupaJam community will be made aware of the need to report online safety issues/incidents and promote a transparent but supportive approach to these situations
- Deal with reports as soon as is practicably possible once they are received
- Provide the Designated Safeguarding Leads and other responsible staff with appropriate skills and training to deal with online safety risks.
- Manage and/or escalate any incident which may involve illegal activity or have the potential for causing serious harm using SupaJam's Online Incident Response Plan (see flowchart and user actions chart in the appendix)
- Have an appropriate process in place to report any issues. All concerns regarding students will be reported to the DSL; all concerns regarding staff will be reported to the Director of Safeguarding, unless the concern involves the Director of Safeguarding in which case the complaint is referred to the CEOs by the DSL and possibly the local authority.

6.4 - Where there is suspected illegal activity, the device or devices involved may be removed from use as possible evidence for any investigation (e.g. Police investigation). Where there is no suspected illegal activity, devices may be checked using the following procedures:

- One or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.

- Conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the Police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
- Ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form.
- Once this has been completed and fully investigated the SLT will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Disciplinary Procedures
    - Involvement by local authority
    - Police involvement and/or action
- It is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively.
- There are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- Incidents should be logged by email to the Director of Safeguarding or CEOs (whichever is appropriate according to the above).
- Relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; Police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- Those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant).
- Learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
    - the safeguarding team for consideration of updates to policies or education programmes and to review how effectively the report was dealt with
    - staff, through regular briefings
    - learners, through all college updates/lessons
    - parents/carers, through newsletters, SupaJam social media, website only

SupaJam will make the flowchart below available in appendix A to staff to support the decision-making process for dealing with online safety incidents.

7. Supporting Learners to Understand the Risks

7.1 - While regulation and technical solutions are particularly important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety is therefore an essential part of SupaJam's online safety provision. Learners need the help and support to recognise and avoid online safety risks and develop their resilience.

7.2 - Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum via SMSC lessons for all students at all levels as well as any national or local initiatives (e.g. Anti-Bullying Week).
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes.
- Learner needs and progress are addressed through effective planning and assessment by their RSL Teacher
- The programme will be accessible to learners at different abilities such as those with additional learning needs or those with English as an additional language.
- Learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside of college
- Staff should act as good role models at all times in their use of digital technologies the internet and mobile devices
- Where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit, challenging those which are unconsidered inappropriate or unsafe and reported to the DSL
- In lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- It is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be done with the base specific DSL and/or the Director of Safeguarding and will need to be auditable, with clear reasons for the need
- The online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes. Staff should take measures to keep abreast of local and national developments as well as receive frequent training.

7.3 - Any conversation by any member of staff with a young person which outlines the need to report any incident involving online behaviours will be done so in a supportive and non-judgmental way, providing the young person with learning opportunities.

8. Monitoring and Filtering

8.1 - SupaJam and Blaucomm work in partnership to manage the monitoring and filtering systems within the organisation to keep learners, staff and the wider community safe and are regularly. Filtering and monitoring policies are agreed by the SLT and are reviewed and updated in response to changes in technology and patterns of online safety incidents/ behaviours. Any material which is considered to be illegal, unethical, discriminative or inappropriate may be blocked using the monitoring and filtering system.

8.2 - SupaJam manages access to content across its systems for all users and has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different groups of users including staff and learners).

8.3 -SupaJam monitors all network use across all its devices and services and an appropriate monitoring strategy for all users has been agreed where users are aware that the network is monitored. This includes in-class physical monitoring on computer use as well as digital monitoring. The Director of Safeguarding is responsible for managing the monitoring strategy and processes and where possible, Blaucomm will regularly monitor and record the activity of users on the college technical systems and report issues to the Director of Safeguarding.

8.4 -There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention. Management of serious safeguarding alerts is consistent with safeguarding policy and practice. Filtering reports are regularly reviewed and alert the Director of Safeguarding to breaches of the filtering policy, which are then acted upon.

8.5 - Any attempt, or successful endeavour by any staff or student to access illegal websites or content, including child sexual abuse imagery or terrorist related activity, or dissemination of illegal material such as sharing nude pictures illegally, will be acted upon immediately, including a referral to relevant services and/or Police.

8.6 - By actively employing the Internet Watch Foundation Child Abuse Images and Content (CAIC) list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office, monitoring and filtering content lists are regularly updated.

8.7 - SupaJam will ensure that there are established and effective routes for users to report inappropriate content as well as a clear process to deal with requests for filtering changes.

8.8 - Where personal mobile devices have internet access through SupaJam's network, content is managed in ways that are consistent with policy and practice. Access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with SupaJam's policy and practice.

8.9 - If necessary, SupaJam will seek advice from, and report issues to the South West Grid for Learning (SWGfL) Reporting Harmful Content site.

9. Training and Raising Awareness

9.1 - All staff and volunteers at SupaJam will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.

- The training will be an integral part of the school's annual safeguarding and data protection training for all staff

- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand SupaJam's Online Safety Policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours.
- The Director of Safeguarding and Designated Safeguarding Leads (or other nominated person) will receive regular updates through attendance at external training events, (e.g. UKSIC / SWGfL / MAT / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/Bitesize training/CPD Days.
- The Designated Safeguarding Leads will provide advice/guidance/training to individuals as required.

9.2 - Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/ regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

9.3 - SupaJam will seek to provide information and awareness to parents and carers through:

- Regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes.
- The learners – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by learners leading sessions at parent/carer evenings.
- Letters, newsletters and website updates with reference to the relevant web sites/ publications, e.g. SWGfL; www.saferinternet.org.uk/, www.childnet.com/parents-and-carers (see Appendix for further links/resources).

10. Technology

10.1 - SupaJam is responsible for ensuring that the infrastructure/network is as safe and secure as is reasonably possible and that polices and procedures approved within this policy are implemented. SupaJam should ensure that all staff are made aware of the polices and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

10.2 - SupaJam's technical systems will be overseen by the Operations Manager and Director of Safeguarding and managed in ways that ensure that it meets the recommended technical requirements:

- There will be regular reviews and audits of the safety and security of SupaJam's technical systems
- Servers, wireless systems and cabling are securely located and physical access restricted
- There are rigorous and verified back-up routines, including the keeping of network separated (air-gapped) copies off-site or in the cloud.
- All users (adults and learners) have responsibility for the security of their username and

password and must not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security

- All of SupaJam's networks and systems will be protected by secure passwords. Passwords must not be shared with anyone. All users will be provided with a username and password by the Operations Manager who will keep an up-to-date record of users and their usernames

- A two factor authentication process is in place for all staff users.

- Passwords should be long and complex enough to not be easily guessed.

- Records of learner usernames and passwords for learners are kept in an electronic format securely.

- The CEOs are responsible for ensuring that all software purchased and used by SupaJam is adequately licenced and that the latest software updates (patches) are applied.

- Appropriate security measures are in place (include the how from Louis/Blaucomm) to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the SupaJam's systems and data. These are tested regularly. Infrastructure and individual workstations are protected by up-to-date endpoint (anti-virus) software.

- An agreed policy is in place for the provision of temporary access of 'guests', (e.g., trainee teachers, supply teachers, visitors) onto the SupaJam systems either through the 'visitor' login profile or setting them up with temporary access, depending on the nature of their work (for example, they are only working for one day or a short period of time)

- An agreed policy is in place regarding the extent of personal use that users (staff / learners / community users) and their family members are allowed on SupaJam devices that may be used out of college - this is listed in the acceptable use agreement

- An agreed policy is in place that allows staff to/forbids staff from downloading executable files and installing programmes on SupaJam devices

- An agreed policy is in place regarding the use of removable media (e.g, memory sticks/ CDs/DVDs) by users on SupaJam devices.

- Systems are in place that prevent the unauthorised sharing of personal data unless safely encrypted or otherwise secured.

11. Social Media and electronic messages (including email)

11.1 - Social media (e.g. Facebook, Twitter, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However, some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube have social media elements to them.

11.2 - SupaJam recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and learners are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation.

11.3 - SupaJam does produce material for social media platforms including Instagram and LinkedIn. All content must be professional, courteous, non-discriminative and in line with the college’s values at all time.

11.4 - Social media posts should not include any specific information, including identifiable information relating to any student unless there is explicit reasons and consent to do so (full details can be found in the college’s Data Protection policy)

11.5 - Any peer to peer incident which identifies online bullying, harassment or abuse through social media platforms not directly linked to the college accounts or systems (i.e they are happening outside of SupaJam) will be investigated the same way through SupaJam’s safeguarding policies and processes.

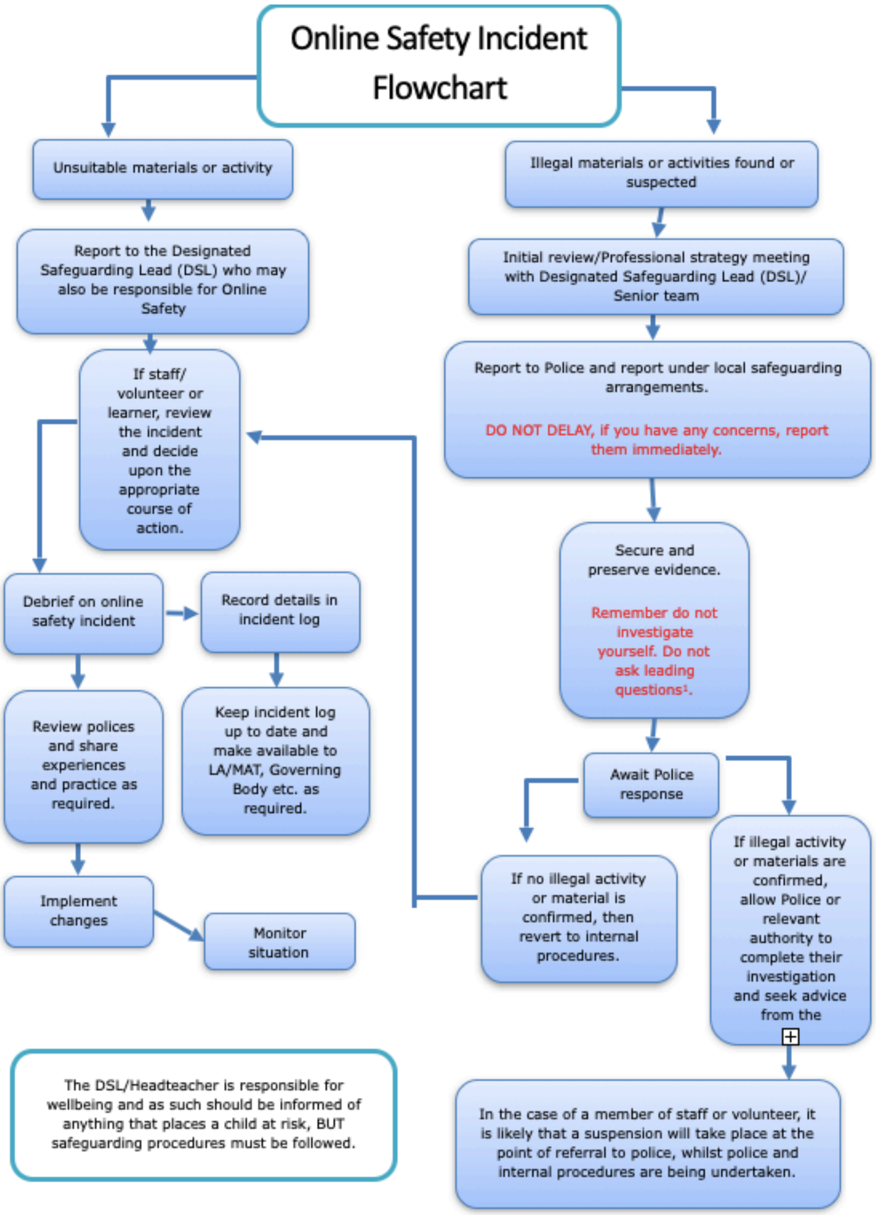
11.6 - Any incident, whether occurring within SupaJam or not which may suggest illegal or dangerous activity, including anything relating to radicalisation, terrorist ideologies or promoting ideologies contrary to the fundamental British Values, will be reported to the Police or other relevant service.

11.7 - Staff and students using SupaJam’s social media must ensure that the views expressed are in line with the values of the organisation, do not engage in online discussion on personal matters relating to members of the SupaJam community, do not offer personal opinions not attributed to SupaJam and are professional and respectful at all time.

11.8 - All email accounts set up under SupaJam require users to send professional, courteous and respectful messages at all times. Emails will not be used for any malicious purpose, or be used to forward or send any inappropriate or illegal material under any circumstance. All disclosures or known incidents will be investigated.

11.9 - Students must immediately tell a member of staff if they receive offensive email(s).

Appendix A



Online Safety Incident Flowchart

Unsuitable materials or activity

Report to the Designated Safeguarding Lead (DSL) who may also be responsible for Online Safety

If staff/ volunteer or learner, review the incident and decide upon the appropriate course of action.

Debrief on online safety incident

Record details in incident log

Review polices and share experiences and practice as required.

Keep incident log up to date and make available to LA/MAT, Governing Body etc. as required.

Implement changes

Monitor situation

Illegal materials or activities found or suspected

Initial review/Professional strategy meeting with Designated Safeguarding Lead (DSL)/ Senior team

Report to Police and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not ask leading questions[1].

Await Police response

If no illegal activity or material is confirmed, then revert to internal procedures.

If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

The DSL/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.