supajam®

Online Safety

August 2024

(Next review date August 2025)

Contents

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. Aims

SupaJam aims to:

- Have robust processes in place to ensure the online safety of students, staff and volunteers

- Identify and support groups of students that are potentially at greater risk of harm online than others

- Deliver an effective approach to online safety, which empowers us to protect and educate the whole college community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')

- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism

Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

• Teaching online safety in schools

• Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff

• Relationships and sex education – remove if not applicable, see section 4]

• Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on student's electronic devices where they believe there is a 'good reason' to do so.

3. Roles and responsibilities

3.1 The Director of Safeguarding

The Director of Safeguarding has overall responsibility for monitoring this policy and holding the SupaJam College Leaders to account for its implementation.

The Director of Safeguarding will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The Director of Safeguarding will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The Director of Safeguarding will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor any CPOMS reports regarding online safety concerns.

The Director of Safeguarding will ensure students are taught how to keep themselves and others safe, including keeping safe online.

The Director of Safeguarding must ensure SupaJam has appropriate filtering and monitoring systems in place on college devices and networks, and will regularly review their effectiveness. The DoS will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the college in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;

- Reviewing filtering and monitoring provisions at least annually;

- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;

- Having effective monitoring strategies in place that meet their safeguarding needs.

The Director of Safeguarding will;

- Ensure they have read and understand this policy

- Agree and adhere to the terms on acceptable use of SupaJam's ICT systems and the internet (appendix 3)

- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures

- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The College Leader

The College Leader is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the College.

3.3 The Designated Safeguarding Lead (DSL)

Details of SupaJam's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in the College, in particular:

• Supporting the Director of Safeguarding in ensuring that staff understand this policy and that it is being implemented consistently throughout the college.

• Working with the Director of Safeguarding to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly

• Taking the lead on understanding the filtering and monitoring systems and processes in place on college devices and college networks

• Working with the ICT contractor and Firewall provider to make sure the appropriate systems and processes are in place

• Working with the Director of Safeguarding, ICT contractor and other staff, as necessary, to address any online safety issues or incidents

• Managing all online safety issues and incidents in line with SupaJam's child protection and safeguarding policy

• Ensuring that any online safety incidents are logged on CPOMS (see appendix 5) and dealt with appropriately in line with this policy

• Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with SupaJam's promoting positive behaviour policy

• Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)

• Liaising with other agencies and/or external services if necessary

• Providing regular reports on online safety in SupaJam to the Director of Safeguarding

• Working with the Director of Safeguarding to undertake annual risk assessments that consider and reflect the risks students face

• Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The ICT Contractor (Acuit)

The ICT contractor is responsible for:

• Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and college networks, which are reviewed and updated at least annually to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

• Ensuring that the college ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly

- Conducting a full security check and monitoring SupaJam's ICT systems on a half termly basis unless a concern is raised beforehand

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with SupaJam's promoting positive behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy

- Implementing this policy consistently

- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that students follow SupaJam's terms on acceptable use (appendices 1 and 2)

- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by emailing the base's DSL or Director of Safeguarding

- Following the correct procedures by emailing a request (including the justification for the request) to the Director of Safeguarding for approval with at least 48 hours notice f they need to bypass the filtering and monitoring systems for educational purposes

- Working with the DSL to ensure that any online safety incidents are logged on CPOMS (see appendix 5) and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with SupaJam's promoting positive behaviour policy

- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the director of safeguarding of any concerns or queries regarding this policy

- Ensure their child has read, understood and agreed to the terms on acceptable use of SupaJam's ICT systems and internet (appendices 1 and 2)

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre

- Hot topics – Childnet

- Parent resource sheet – Childnet

3.7 Visitors and members of the community

Visitors and members of the community who use the college's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating students about online safety

Pupils will be taught about online safety as part of SupaJam's SMSC and additional curriculum:

All students will be taught to:

- That people sometimes behave differently online, including by pretending to be someone they are not

- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous

- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them

- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met

- How information and data is shared and used online

- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)

- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy

- Recognise inappropriate content, contact and conduct, and know how to report concerns

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online

- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online

- Not to provide material to others that they would not want shared further and not to share personal material that is sent to them

- What to do and where to get support to report material or manage issues online

- The impact of viewing harmful content

- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others, and negatively affect how they behave towards sexual partners

- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail

- How information and data is generated, collected, shared and used online

- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours

- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents/carers about online safety

SupaJam will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents/carers.

SupaJam will let parents/carers know:

- What systems SupaJam uses to filter and monitor online use

- What students are being asked to do online, including the sites they will be asked to access and who from SupaJam (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff, College Leaders or the SLT.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the anti-bullying policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

SupaJam will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyber-bullying with their class groups and the DSLs will include in their safeguarding induction with students at the start of the year.

All staff receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training (see section 11 for more detail).

SupaJam also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, SupaJam will follow the processes set out in the promoting positive behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, SupaJam will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The College Leader, and any member of staff authorised to do so by the Director of Safeguarding, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

• Poses a risk to staff or students, and/or

• Is evidence in relation to an offence

• Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

1. Make an assessment of how urgent the search is, and consider the risk to other students and staff. If the search is not urgent, they will seek advice from DSL or Director of Safeguarding.

2. Explain to the student why they are being searched, how the search will happen, and give them the opportunity to ask questions about it

3. Seek the student's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

1. Cause harm, and/or

2. Undermine the safe environment of the school or disrupt teaching, and/or

3. Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

• They reasonably suspect that its continued existence is likely to cause harm to any person, and/or

• The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

• **Not** view the image

• Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

• The DfE's latest guidance on searching, screening and confiscation

• UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

• Our Promoting Positive Behaviour Policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, students and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

SupaJam recognises that AI has many uses to help students learn, but may also have the potential to bully. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

SupaJam will treat any use of AI to bully students in line with our Anti-bullying and Promoting Positive Behaviour Policies.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the SupaJam.

7. Acceptable use of the internet in college

All students, parents/carers, staff, and volunteers are expected to sign an agreement regarding the acceptable use of the SupaJam's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to SupaJam's terms on acceptable use if relevant.

Use of SupaJam's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by students, staff, volunteers and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. Students using mobile devices in college

Students may bring mobile devices into college, but are not permitted to use them during:

• Lessons

• Activities organised by the college unless agreed with the teacher or activity lead.

Any use of mobile devices in college by students must be in line with the acceptable use agreement (see appendices 1 and 2) and SupaJam's 'expectations' as outlined in the Promoting Positive Behaviour Policy.

Any breach of the acceptable use agreement by a student may trigger further action in line with the school behaviour policy, which may result in the confiscation of their device where appropriate to do so.

9. Staff using work devices outside of SupaJam

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)

- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device

- Making sure the device locks if left inactive for a period of time

- Not sharing the device among family or friends

- Installing anti-virus and anti-spyware software

- Keeping operating systems up to date by always installing the latest update

- Staff members must not use the device in any way that would violate SupaJam's terms of acceptable use, as set out in appendix 3.

- Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from Peter Davey at *Acuit.*

10. How SupaJam will respond to issues of misuse

Where a student misuses SupaJam's ICT systems or internet, we will follow the procedures set out in our policies on Promoting Positive Behaviour Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses SupaJam's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures and staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

SupaJam will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails and staff meetings).

By way of this training, all staff will be made aware that:

Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse

Children can abuse their peers online through:

o Abusive, threatening, harassing and misogynistic messages

o Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups

o Sharing of abusive images and pornography, to those who don't want to receive such content

Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

• Develop better awareness to assist in spotting the signs and symptoms of online abuse

• Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks

• Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputy DSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5 and will

This policy will be reviewed every year by the Director of Safeguarding. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks students face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

Child protection and safeguarding policy

Promoting positive Behaviour policy

Staff disciplinary procedures

Data protection policy

Complaints procedure

ICT and internet acceptable use policy

Appendix 1: Student acceptable use agreement

ACCEPTABLE USE OF SUPAJAM'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STUDENTS AND PARENTS/CARERS
Name of student:

I will read and follow the rules in the acceptable use agreement policy.

When I use the SupaJam's ICT systems (like computers) and get onto the internet in school I will:

· Always use the college's ICT systems and the internet responsibly and for educational purposes only

· Keep my usernames and passwords safe and not share these with others

· Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer

· Tell a teacher or any member of staff (or sensible adult) immediately if I find or view any material that might upset, distress or harm me or others

· Always log off or shut down a computer when I've finished working on it

I will not:

· Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity

· Open any attachments in emails, or follow any links in emails, without first checking with a teacher

· Use any inappropriate language when communicating online, including in emails

· Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate

· Log in to the college's network using someone else's details

· Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision (applies to those under the age of 16 years)

If I bring a personal mobile phone or other personal electronic device into college:

· I will not use it during lessons unless I have permission by my teacher

· I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

• I will not plug in any device into the college computers or systems

I have read and understood this agreement.

Signed (student):	Date:

Appendix 2: acceptable use agreement (staff, advisory board members, volunteers and visitors)

ACCEPTABLE USE OF THE SUPAJAM'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, ADVISORY BOARD, VOLUNTEERS AND VISITORS

Name of staff member/advisory/volunteer/visitor:

When using the SupaJam's ICT systems and accessing the internet in college, or outside college on a work device (if applicable), I will not:

· Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)

· Use them in any way that could harm the college's reputation

· Access social networking sites or chat rooms

· Use any improper language when communicating online, including in emails or other messaging services

· Install any unauthorised software, or connect unauthorised hardware or devices to the college's network

· Share my password with others or log in to the college's network using someone else's details

· Take photographs of students without checking with teachers first

· Share confidential information about the college, its students or staff, or other members of the community

· Access, modify or share data I'm not authorised to access, modify or share

· Promote private businesses, unless that business is directly related to the college

• I will only use the college's ICT systems and access the internet in college, or outside college on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

• I agree that the college will monitor the websites I visit and my use of the college's ICT facilities and systems.

• I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

• I will let the designated safeguarding lead (DSL) and ICT manager know if a students informs me they have found any material that might upset, distress or harm them or others, and will also do so if I encounter any such material.

• I will always use the college's ICT systems and internet responsibly, and ensure that students in my care do so too.

Signed (staff member/advisor/volunteer/visitor):	**Date:**

Appendix 3: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT

Name of staff member/volunteer:	Date:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in college?	
Are you aware of the ways students can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with SupaJam's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the SupaJam's acceptable use agreement for students?	
Are you familiar with the filtering and monitoring systems on the SupaJam's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing SupaJam's ICT systems?	
Are you familiar with SupaJam's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	