Joseph Leckie Academy

Online Safety Policy

Approved by JLA Trust Board:	01/2023
Last reviewed on:	01/2023
Next review due by:	01/2024

1. Policy Aims

1.1 This Online Safety Policy takes into account the DfE statutory guidance 'Keeping Children Safe in Education, 'Working Together to Safeguard Children' and the relevant Local Authority Safeguarding Children's Partnership Safeguarding procedures.

1.2 The purpose of this Online Safety Policy is to:

- Safeguard and protect all members of the Joseph Leckie Academy community online.
- Identify approaches to educate and raise awareness of online safety throughout the Academy.
- Enable all staff to work safely and responsibly, including the delivery of remote learning to role model positive behaviour online and to manage professional standards and practice when using technology.

1.3 Identify clear procedures to use when responding to online safety concerns. This Academy identifies that the issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:

1. **Content:** being exposed to illegal, inappropriate or harmful material.
2. **Contact:** being subjected to harmful online interaction with other users.
3. **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.
4. **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams' (KCSIE).

2. Policy Scope

2.1 Joseph Leckie Academy believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all student and staff are protected from potential online harm:

- Joseph Leckie Academy identifies that the internet and associated devices, such as computers, tablets, mobile phones and game consoles, are an important part of everyday life.
- Joseph Leckie Academy believes that students should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- This policy applies to all staff including the Trust Board, Senior Leadership Team (SLT), teachers, support staff, external contractors, visitors who access the IT network, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy) as well as students, parents/carers.
- This policy applies to all access to the internet and use of technology, including personal devices, or where students, staff or other individuals have been provided with devices for use off-site, such as a work laptop, tablet or mobile phone.

2.2 This policy links with several other policies including but not limited to:

- Anti-bullying policy
- ICT Acceptable Use Policy
- Behaviour and Relationships Policy
- Child Protection and Safeguarding Policy
- Relationships and Sex Education (RSE) Policy
- Data Protection policy
- ICT Security Policy
- Social Media Policy

3. Monitoring and Review

3.1 Technology evolves and changes rapidly. Joseph Leckie Academy will review this policy at least annually. The policy will also be revised following any national or local policy requirements; any child protection concerns or any changes to the technical infrastructure.

3.2 We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.

3.3 To ensure they have oversight of online safety, the Principal will be informed of online safety concerns, as appropriate.

3.4 Any issues identified via monitoring will be incorporated into our action planning.

4. Roles and Responsibilities

4.1 Joseph Leckie Academy recognises that all members of the community have important roles and responsibilities to play concerning online safety.

4.2 **Designated Safeguarding Lead (DSL)**. The DSL has lead responsibility for online safety and is supported by ICT Technicians. Whilst activities of the designated safeguarding lead may be delegated to an appropriately trained deputy, overall the ultimate lead responsibility for safeguarding and child protection, including online safety remains with the DSL.

The DSL will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Work alongside deputy DSLs to ensure online safety is recognised as part of the settings safeguarding responsibilities and that a coordinated approach is implemented.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant and up-to-date knowledge required to keep students safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that students with SEN and disabilities (SEND) face online.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents/carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the settings safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate, to the Senior Leadership Team and Trust Board.

- Work with the Senior Leadership Team to review and update online safety policies regularly (at least annually)
- Meet regularly with the Trustee with lead responsibility for safeguarding and online safety.
- The DSL should focus on what good online behaviour should look like.

4.3 **Senior Leadership Team (SLT).** The Senior Leadership Team will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies which cover acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks.
- Ensure that online safety is embedded within a progressive curriculum, which enables all students to develop an age-appropriate understanding of online safety.
- Support the DSL and any deputies by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure parents/carers are directed to online safety advice and information
- Provide information on the Academy website for parents/carers and the community
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal and external support.
- Audit and evaluate online safety practices to identify strengths and areas for improvement.

4.4 **IT and Technical Staff.** It is the responsibility of IT, and technical staff, to:

- Take personal responsibility for professional development in this area.
- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures as directed by the DSL and leadership team to ensure that the settings IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that our filtering policy is applied and updated regularly; responsibility for its implementation is shared with the leadership team.
- Ensure that our monitoring systems are applied and updated regularly; responsibility for its implementation is shared with the leadership team
- Ensure appropriate access and technical support is given to the DSL (and/or deputy) to our filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required.

4.5 **All Academy Staff.** It is the responsibility of all members of staff to:

- Contribute to the development of the eSafety Policy.
- Read and adhere to the eSafety Policy and ICT Acceptable Use Policy.
- Take responsibility for the security of setting systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off-site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.

- Identify online safety concerns and take appropriate action by following the settings safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.
- Identify students who are involved in cybercrime or those students who are at risk of becoming involved in cybercrime and make a safeguarding concern referral.

4.6 **Students**. It is the responsibility of students to:

- Engage in age-appropriate online safety education opportunities.
- Adhere to the acceptable use policies.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

4.7 **Parents/Carers.** It is the responsibility of parents/carers to:

- Encourage conformity to the ICT Acceptable Use Policy and encourage their children to adhere to them.
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the ICT Acceptable Use Policy.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Take responsibility for their awareness concerning the risks and opportunities posed by new and emerging technologies.

5. Education and Engagement Approaches

5.1 The Academy will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst students by:

- Ensuring education regarding safe and responsible use precedes internet access.
- Including online safety in Personal Development Programme (PDP), Relationships and Sex Education (RSE) and ICT/computing programmes of study.
- Reinforcing online safety messages whenever technology or the internet is in use.
- Educating students in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.

5.2 Teaching students to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. The Academy will support students to read and understand the acceptable use policies by:

- Displaying acceptable use posters in all rooms with internet access.
- Informing students that network and internet use will be monitored for safety and security purposes and following legislation.
- Using the support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

6. Vulnerable Students

6.1 Joseph Leckie Academy recognises that some students are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.

6.2 Joseph Leckie Academy will ensure that differentiated and ability-appropriate online safety education, access and support are provided to vulnerable students.

7. Training

7.1 Training and engagement with staff we will:

- Provide and discuss the eSafety policy and procedures with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff (including Trustees) where relevant to their role regularly, with at least annual updates. This will be delivered as part of the Academy's safeguarding and child protection training. There will also be regular updates through briefings and the weekly bulletin as needed.
- This will cover the potential risks posed to students (Content, Contact, Conduct and Commerce) as well as our professional practice expectations.
- Recognise the expertise of staff by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.
- Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the students.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting students, colleagues or other members of the community.

8. Awareness and Engagement with Parents/Carers

8.1 Joseph Leckie Academy recognises that parents/carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.

- We build a partnership approach to online safety with parents/carers by:
- Providing information and guidance on online safety in a variety of formats. This includes offering specific online safety awareness training and highlighting online safety at other events such as parent consultation evenings, and transition events
- Drawing their attention to the eSafety policy and expectations in newsletters, letters, our prospectus and on our website.
- Requiring them to read our ICT Acceptable Use Policy and discuss the implications with their children.

9. Reducing Online Risks

9.1 Joseph Leckie Academy recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. We will:

- Regularly review the methods used to identify, assess and minimise online risks.
- Examine emerging technologies for an educational benefit before use in the setting is permitted, as part of any Online Safety/Digital Strategy
- Ensure that appropriate filtering and monitoring are in place and take all reasonable precautions to ensure that users can only access appropriate material.
- All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in our acceptable use policies and highlighted through a variety of education and training approaches.
- Due to the global and connected nature of the internet, it is not possible to guarantee 100% that unsuitable material cannot be accessed via our computers, online systems or digital devices.

10. Safer Use of Technology

10.1 Use of Technology On Site. Joseph Leckie Academy uses a wide range of technology. This includes access to:

- Laptops and PCs
- Internet which may include search engines and educational websites
- Office 365 (including Outlook, Calendar, OneDrive, etc…) and other cloud-based platforms

10.2 The Academy will ensure:

- All setting-owned devices will be used following our acceptable use policies and with appropriate safety and security measures in place.
- All laptops are managed using Smoothwall Device Management, which allows the Academy to monitor activity, control access to the internet, locate the device and reset security features
- Smoothwall Monitor/Filter provides an active agent to provide onsite/offsite filtering, monitoring and (if activated) timed policies, both in and out of the Academy.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The Academy will use age-appropriate search tools to meet the needs of our community.
- We will ensure that the use of internet-derived materials, by staff and students complies with copyright law and acknowledge the source of information.
- Supervision of students will be appropriate to their age and ability. students will be appropriately supervised both in person and remotely when using technology, according to their ability and understanding

10.3 Managing Internet Access.

- We will maintain a record of users who are granted access to our devices and systems
- All staff, students and visitors will read and agree to an ICT Acceptable Use Policy before being given access to our computer system, IT resources or internet. This may appear periodically as a pop-up screen on devices.

- We will carry out audit activity to help identify students trying to access sites to establish any vulnerabilities and offer advice, support and react accordingly Filtering and Monitoring Decision Making
- Joseph Leckie Academy Trustees have ensured that our setting has age and ability-appropriate filtering and monitoring in place, to limit students' exposure to online risks. The Trustees are aware of the need to prevent “over blocking”, as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding.
- Changes to the filtering and monitoring approach will be assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard students; effective classroom management and regular education about safe and responsible use is essential.

10.4 Filtering. Education broadband connectivity is currently provided through ?. We use Smoothwall, to block sites, including automated updates as well as manually added lists Smoothwall Monitor agent will identify attempts to access inappropriate sites and categorise them as pornography, violence, racial hatred, extremism, gaming and sites of an illegal nature.

10.4.1 If students discover unsuitable sites, they will be required to:

- Report the concern immediately to a relevant member of staff.
- The member of staff will report the concern (including the URL of the site if possible) to the DSL (or deputy) and/or technical staff.
- The breach will be recorded and escalated as appropriate.
- Parents/carers will be informed of filtering breaches involving their child.
- If it involves student laptops or Academy accounts, the ICT Technicians may be required to remote lock them/change account passwords to avoid any tampering with evidence
- Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the Police or CEOP

10.5 Monitoring

- We will appropriately monitor internet use on all settings owned or provided internet-enabled devices. This is achieved by the Smoothwall filtering system currently.
- If a concern is identified via monitoring approaches we will follow the procedure in our Child Protection and Safeguarding Policy. This will be reported directly to the Principal who will consider the Child Protection and Safeguarding Policy and involve the LADO, as appropriate.
- All users will be informed that the use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation. Managing Personal Data Online will be recorded, processed, transferred and made available online per UK Data Protection legislation.
- We take appropriate steps to ensure the security of our information systems, including:
- Virus protection is updated regularly on all Academy platforms.
- Encryption for all messages via the Academy email system
- Instructions sent to all staff for the encryption and sensible use of portable media storage.
- All portable media will be automatically checked by an anti-virus /malware scan before use.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments.

- Regularly checking files held on our network.
- The appropriate use of user logins and suitable passwords to access our network.
- All users are required to log off or lock their screens/devices if systems are unattended.

10.6 **Password Guidance.** In accordance with the ICT Acceptable Use Policy:

- All members of staff will have their unique usernames and private passwords to access our systems; members of staff are responsible for keeping their passwords private.
- All students are provided with their unique usernames and private passwords to access our systems; students are responsible for keeping their passwords private.

We require all users to:

- use strong passwords for access into our system – the longer and more unusual, the stronger it becomes. Using a combination of upper, and lower case, numbers and special characters is recommended and may be set as default on some systems.
- reset their password when prompted (usually after 90 days)
- always keep their password private; users must not share it with others or leave it where others can find it
- not log in as another user at any time unless they have permission from the Academy Leadership Team or as part of an investigation

10.7 **Managing the Safety of our Website.** We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).

- We will ensure that our website complies with guidelines for publications including accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff or student's personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number.
- The administrator account for our website will be secured with an appropriately strong password. We will post appropriate information about safeguarding, including online safety, on our website for members of the community, especially parents/carers
- Publishing Images and Videos Online
- We will ensure that all images and videos shared online are used following the associated policies, including (but not limited to) the Data Protection Policy, Copyright legislation, ICT Security Policy and the ICT Acceptable Use Policy.
- Managing Email
- Reference to the appropriate use of emails and Educational use of Videoconferencing and/or Webcams can be found within the ICT Acceptable Use Policy.

11. Social Media

11.1 Reference can be found within the ICT Acceptable Use Policy, in the Academy Staff Code of Conduct and Social Media Policy.

11.2 Students' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to students as part of an embedded and progressive education approach, via age-appropriate sites and resources.

- We are aware that many popular social media sites state that they are not for children under the age of 13, therefore we will not encourage the creation of accounts specifically for students under this age.
- Any concerns regarding students' use of social media will be dealt with under existing policies, including Anti-Bullying Policy and Behaviour and Relationships Policy.
- Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.

Students will be advised:

- To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
- To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
- Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
- Use safe passwords.
- To use social media sites which are appropriate for their age and abilities.
- How to block and report unwanted communications.
- How to report concerns both internally and externally.
- Official Use of Social Media

11.3 **Academy Social Media.** Joseph Leckie Academy has various official social media channels, including Twitter, Facebook, LinkedIn and Instagram.

- The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes. The official use of social media as a communication tool has been formally risk assessed and approved by the Principal
- Official social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
- Staff may be given approval by the Principal to run an official social media account and will be provided with additional guidance about conduct, transparency and accountability in representing the Academy.
- Staff responsible for social media will use Academy email addresses to manage any official social media channels.
- Official social media sites are suitably protected and linked to our website.
- All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Parents/carers and students will be informed of any official social media use, along with expectations for safe use and action is taken to safeguard the community.
- Parents/carers will be informed of any official social media use with students; written parental consent will be obtained, as required.

12. Use of Personal Devices and Mobile Phones

12.1 Reference is made within the ICT Acceptable Use Policy and the Staff Code of Conduct.

13. Responding to Online Safety Incidents and Concerns

13.1 All members of the Academy will be made aware of the reporting procedure for online safety concerns via My Concern, including breaches of filtering, youth-produced sexual imagery (sexting), cyberbullying and illegal content.

13.2 All members of the Academy must respect confidentiality and the need to follow the official procedures for reporting concerns. Students, parents/carers and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure. We require staff, parents/carers and students to work in partnership to resolve online safety issues.

13.3 After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required.

13.4 Where there is suspicion, that illegal activity has taken place, we will follow the local safeguarding procedures which will include Police using 101, or 999 if there is immediate danger or risk of harm. If an incident or concern needs to be passed beyond our community (for example if other local settings are involved or the public may be at risk), the DSL or Principal will speak with relevant agencies (e.g. call the Police) first to ensure that potential investigations are not compromised.

13.5 Concerns about Students' Welfare. The DSL (or deputy) will be informed of any online safety incidents involving safeguarding or child protection concerns:

- The DSL (or deputy) will record these issues via My Concern, in line with our Child Protection and Safeguarding Policy.
- The DSL (or deputy) will ensure that online safety concerns are escalated and reported to relevant agencies in line with procedures.
- We will inform parents/carers of online safety incidents or concerns involving their child, as and when required.

14. Procedures for Responding to Specific Online Incidents or Concerns

14.1 **Online Sexual Violence and Sexual Harassment between Children.** Joseph Leckie Academy recognises that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.

14.1.1 Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our Child Protection and Safeguarding Policy and Anti-Bullying Policy.

14.1.2 Joseph Leckie Academy recognises that the internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities. Joseph Leckie Academy also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

14.1.3 Joseph Leckie Academy will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and

ability appropriate educational methods as part of our PDP curriculum. We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.

14.1.4 We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment. If made aware of online sexual violence and sexual harassment, we will:

- Immediately notify the DSL (or deputy) and act following our child protection and anti-bullying policies.
- If the content is contained on student electronic devices, it will be managed in accordance with the DfE 'searching screening and confiscation' advice. Searching, screening and confiscation at school - GOV.UK
- Provide the necessary safeguards and support for all students involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
- Implement appropriate sanctions under our Behaviour and Relationships Policy.
- Inform parents/carers, if appropriate, about the incident and how it is being managed.
- If appropriate, make a referral to partner agencies, such as Social Care and/or the Police.
- If the concern involves children and young people in a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community. - If a criminal offence has been committed, the DSL (or deputy) will discuss this with the Police first to ensure that investigations are not compromised.
- Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate

14.2 Youth Produced Sexual Imagery (“Sexting”). Joseph Leckie Academy recognises youth-produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).

14.2.1 We will follow the advice as set out in the non-statutory UKCCIS guidance: ‘Sexting in schools and colleges: responding to incidents and safeguarding young people’ and KSCB guidance: “Responding to youth produced sexual imagery”.

14.2.2 Joseph Leckie Academy will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability-appropriate educational methods.

14.2.3 We will ensure that all members of the community are aware of sources of support regarding youth-produced sexual imagery.

14.2.4 We will respond to concerns regarding youth-produced sexual imagery, regardless of whether the incident took place on-site or using setting provided or personal equipment.

14.2.5 We will not:

- View any images suspected of being youth-produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so. If it is deemed

necessary, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be documented.
- Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request students to do so.

14.2.6 If made aware of an incident involving the creation or distribution of youth-produced sexual imagery, we will:
- Act in accordance with our Child Protection and Safeguarding Policy
- Ensure the DSL (or deputy) responds in line with the 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
- Store the device securely. If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
- Carry out a risk assessment which considers any vulnerability of students involved; including carrying out relevant checks with other agencies.
- Inform parents/carers, if appropriate, about the incident and how it is being managed.
- Make a referral to Social Care and/or the Police, as deemed appropriate in line with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
- Provide the necessary safeguards and support for students, such as offering counselling or pastoral support.
- Implement appropriate sanctions in accordance with our Behaviour and Relationships Policy but taking care not to further traumatise victims where possible.
- Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance. Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
- Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

14.3 **Online Child Sexual Abuse and Exploitation (including child criminal exploitation).** Joseph Leckie Academy will ensure that all members of the community are aware of online child sexual abuse, including exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.

14.3.1 Joseph Leckie Academy Trustees recognise online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).

14.3.2 We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability-appropriate education for students, staff and parents/carers.

14.3.3 We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.

14.3.4 We will ensure that the 'Click CEOP' report button is visible and available to students and other members of our community (available on our website home screen)

14.3.5 If made aware of an incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:

- Act in accordance with our Child Protection and Safeguarding Policy
- If appropriate, store any devices involved securely.
- Make a referral to Social Care (if required/appropriate) and immediately inform police via 101, or 999 if a child is at immediate risk.
- Carry out a risk assessment which considers any vulnerabilities of a student (s) involved (including carrying out relevant checks with other agencies).
- Inform parents/carers about the incident and how it is being managed.
- Provide the necessary safeguards and support for students, such as offering counselling or pastoral support.
- Review the handling of any incidents to ensure that best practice is implemented; the leadership team will review and update any management procedures, where necessary.

14.3.6 We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using the setting provided or personal equipment. Where possible, students will be involved in decision-making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/

14.3.7 If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Police by using 101.

14.3.8 If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Police using 101 unless immediate concerns and 999 will be used by the DSL (or deputy).

14.3.9 If students in other settings are believed to have been targeted, the DSL (or deputy) will seek support from the Police first to ensure that potential investigations are not compromised. Indecent Images of Children (IIOC)

14.3.10 If made aware that a member of staff or a student has been inadvertently exposed to indecent images of children, we will:

- Ensure that the DSL (or deputy) is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk.
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Report concerns, as appropriate to parents/carers.

14.3.11 If made aware that indecent images of children have been found on the setting-provided devices, we will:

- Ensure that the DSL (or deputy) is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Inform the Police via 101 (999 if there is an immediate risk of harm) and Children's Services (as appropriate).
- Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
- Report concerns, as appropriate to parents/carers.

14.3.12 If made aware that a member of staff has indecent images of children on setting provided devices, we will:

- Ensure that the Principal is informed in line with our managing allegations against staff procedure immediately and without any delay.
- Inform the Local Authority Designated Officer (LADO).
- Quarantine any devices until police advice has been sought.

15. Cyberbullying, Online Hate, Radicalism and Extremism

15.1 **Cyberbullying.** Cyberbullying, along with all other forms of bullying, will not be tolerated at Joseph Leckie Academy. Full details of how we will respond to cyberbullying are set out in our Anti-Bullying Policy.

15.2 **Online Hate.** Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Joseph Leckie Academy and will be responded to in line with existing policies, including Anti-Bullying Policy and Behaviour and Relationships Policy.

All members of the community will be advised to report online hate following relevant policies and procedures. The Police will be contacted if a criminal offence is suspected. If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through the Police.

15.4 **Online Radicalisation and Extremism.** We will take all reasonable precautions to ensure that students and staff are safe from terrorist and extremist material when accessing the internet on site.

If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our Child Protection and Safeguarding Policy and Walsall Prevent pathway which may include a referral into Channel.

If we are concerned that a member of staff may be at risk of radicalisation online, the Principal will be informed immediately, and action will be taken in line with the Child Protection and Safeguarding Policy.

Appendix 1: Acceptable ICT Use Policy. Student Acceptable Use Policy Agreement

I understand that I must use the Academy ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the Academy will monitor my use of the ICT systems, email and other digital communications.
- I will not share my username or password, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line.
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the Academy ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the Academy has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the Academy:

- I will only use my personal hand held/external devices (mobile phones / USB devices etc…) in Academy if I have permission. I understand that, if I do use my own devices in the Academy, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I am aware that damage to personal hand held devices isn't the responsibility of the Academy unless permission for use was granted.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

- I will not open any attachments to emails, unless I know and trust the person/organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of the Academy:

- I understand that the Academy also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of the Academy and where they involve my membership of the Academy community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the Academy network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please note agreement of this Acceptable Use Agreement is necessary to continue. If you do not agree, access will not be granted to the Academy ICT systems.

Appendix Two: Acceptable ICT Use Policy. Staff and Volunteers Policy Agreement.

I understand that I must use the Academy ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users including students.

For my own personal safety:

- I understand that the Academy has the right to monitor all aspects of its IT systems (computers, internet, emails, social network use) including personal devices when connected to the Academy network and WiFi to ensure that the Academy IT systems are not compromised, used inappropriately and for our responsibilities with respect to Safeguarding and Prevent.
- I will not share my username or password, nor will I try to use any other person's username and password.
- I will not disclose or share personal information about myself or others when on-line.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I will ensure that when using the Academy systems and devices and any personal devices which connect to the Academy network/WiFi or are used for Academy business, that I will comply with the following policies:
    - Staff Code of Conduct
    - Data Protection Policy & Data Protection Act 2018 (GDPR)
    - E-Safety Policy
    - Whistleblowing Policy

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will not take or distribute images of anyone without consent

I recognise that the Academy has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the Academy:

- I am aware that damage to personal hand held devices isn't the responsibility of the Academy unless permission for use was granted.
- I will immediately report any damage or faults involving equipment or software, however this may have happened to ICT support and the line manager of the department.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings without first consulting the ICT Support Department.
- I understand that I should only store Academy related resources/files on the network areas, and not use these areas for storage of personal files.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of the Academy:

- I understand that the Academy also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of the Academy and where they involve my membership of the Academy community (examples would be cyber-bullying, misuse of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action as per the staff code of conduct and in the event of illegal activities involvement of the police.

Please note: Whilst using Academy ICT systems you should also abide by the policies listed above, these are available on the Academy website.