The Khalsa Academy Wolverhampton – A Khalsa Academies Trust School

TKAW Online Safety Policy

This policy is applicable to Khalsa Academy Wolverhampton

This policy will be reviewed at least annually. It will also be revised following any concerns and/or updates to national and local guidance or procedures.

Document control	
Date Approved	September 2023
Date for Review	September 2024
Authorised By	
Published Location	School Website
Document Owner	A. Notta / J. de las Heras
Designated Safeguarding Lead	B. Dusanj
Names Trustee with lead responsibility	Susan Jackson

TKAW Contact Information

Role/Agency	Name	Telephone	E-mail
Head of School	Mr S Shoker	01902 925390	s.shoker@tkaw.org
DSL	Mrs B Dusanj	01902 925390	b.dusanj@tkaw.org
Deputy DSL's & Digital DDSL	Mr M Dhillon Mr N Seabridge	01902 925390	m.dhillon@tkaw.org n.seabridge@tkaw.org
Trust Safeguarding Lead	Mr S Shoker	01902 925390	s.shoker@tkaw.org
CEO	Mrs A Notta	01902 925390	a.notta@tkaw.org
Safeguarding Trustee	Mrs S Jackson		s.jackson@khalsaacademiestrust.com
Online Safety Lead / Digital DDSL	Mr N Seabridge	01902 925390	n.seabridge@tkaw.org
SENDCO	Mrs A Evans	01902 925390	a.evans@tkaw.org
PSHE / SRE Coordinator	Mrs C Harding	01902 925390	c.harding@tkaw.org
Looked After Children Lead	Mrs B Dusanj	01902 925390	b.dusanj@tkaw.org
Technical Support Lead	Mr J Geary	01902 925390	j.geary@tkaw.org
Multi-Agency Safeguarding Hub (MASH)	Social Care	01902 555392	
Social Care Out of Hours	Social Care	01902 552999	
Designated Officer / LADO	N/A	01902 550661	lado@wolverhampton.gov.uk
CME Attendance Manager	Angela Bailey	01902 550203	Angela.bailey@wolverhampton.gov.uk
Prevent Counter-Community Safety Team	Wolverhampton Prevent Team	01902 551214	safer@wolverhampton.gov.uk
FGM	Police	101 or 999	
Police	Police	101 Option 3 for WMP or 999	
Wolverhampton Virtual School Head	Darren Martindale	01902 551039	Darren.martindale@wolverhampton.gov.uk
Wolverhampton CSE Lead	Sandeep Gill		Sandeep.gill@wolverhampton.gov.uk
NSPCC Whistleblowing Helpline	NSPCC	0800 028 0285	help@nspcc.org.uk

If there is immediate risk of harm to a child, call the Police on 999

Table of Contents

The Khalsa Academy Wolverhampton Online Safety Policy

1. Policy aims

- This online safety policy has been written by The Khalsa Academy Wolverhampton, involving staff, learners and parents/carers, building on the Kent County Council/The Education People online safety policy template, with specialist advice and input as required.

- It takes into account the DfE statutory guidance 'Keeping Children Safe in Education' 2023, 'Working Together to Safeguard Children' 2018, Relationships and sex education (RSE) and health education and Teaching online safety in schools.

- Additional risks are mentioned in KCSIE 2023, e.g. extra-familial harms where children are at risk of abuse or exploitation to multiple harms in situations outside their families including sexual exploitation, criminal exploitation, serious youth violence, upskirting and sticky design.

- The purpose of The Khalsa Academy Wolverhampton online safety policy is to
    - safeguard and promote the welfare of all members of The Khalsa Academy Wolverhampton community online.
    - identify approaches to educate and raise awareness of online safety throughout our community.
    - enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
    - identify clear procedures to follow when responding to online safety concerns.

- Current concerns (2023) include past and potential future remote learning and lockdowns as there is a greater risk for grooming and exploitation (CSE, CCE and radicalisation) as children spend more time at home and on devices.

- The Khalsa Academy Wolverhampton identifies that the issues classified within online safety are considerable but can be broadly categorised into three areas of risk.
    - Content: being exposed to illegal, inappropriate or harmful material
    - Contact: being subjected to harmful online interaction with other users
    - Conduct: personal online behaviour that increases the likelihood of, or causes, harm.

- This policy complements existing and forthcoming subjects including Health, Relationships and Sex Education, Citizenship and Computing.

2. Policy scope

- The Khalsa Academy Wolverhampton recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.
- Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads.
- The Khalsa Academy Wolverhampton identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles are an important part of everyday life which present positive and exciting opportunities, as well as challenges and risks.
- The Khalsa Academy Wolverhampton will empower our learners to acquire the knowledge needed to use the internet and technology in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks.
- This policy applies to all staff including the leadership team, teachers, and support staff.
- This policy applies to the local advisory board, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (collectively referred to as "staff" in this policy) as well as learners and parents and carers.
- This policy applies to all access to the internet and individuals use of technology, including mobile technology, or where learners, staff or other individuals have been provided with setting issued devices for use, both on and off-site.

2.1 Links with other policies and practices

- This policy links with several other policies, practices and action plans, including but not limited to:
    - Anti-bullying policy
    - Acceptable Use Policies (AUP) and Staff Code of Conduct policy
    - Behaviour policy
    - Safeguarding policy
    - Data Protection policy
    - Mobile phone policy
    - Keeping Children Safe in Education 2023

This policy sits alongside the school's safeguarding and child protection procedures and any issues or concerns must follow these procedures.

2.2 How this policy will be distributed

- Posted on the school website
- Available on the internal staff network/drive
- Part of school induction pack for all new staff (including temporary, supply and non-classroom-based staff)

- Integral to safeguarding updates and training for all staff (especially in September refreshers)
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, trustees, students and parents/carers (which must be in accessible language appropriate to these groups).
- AUPs issued to whole school community, on entry to the school, with annual reminders of where to find them if unchanged, and reissued if updated after annual review
- AUPs are displayed in appropriate classrooms/corridors (not just in Computing corridors/classrooms)
- Reviews of this online-safety policy will include input from staff, students and other stakeholders, helping to ensure further engagement

3. Monitoring and review

- Technology evolves and changes rapidly; as such The Khalsa Academy Wolverhampton will review this policy at least annually. The policy will be revised following any national or local policy updates, any local child protection concerns and/or any changes to our technical infrastructure.
- We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the Principal/safeguarding team will be informed of online safety concerns, as appropriate.
- The named local advisory board member for safeguarding will report on online safety practice and incidents, including outcomes, on a regular basis to the wider local advisory board.
- Any issues identified via monitoring policy compliance will be incorporated into our action planning.

4. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL) is recognised as holding overall lead responsibility for online safety. Whilst activities of the DSL may be delegated to an appropriately trained deputy, overall the ultimate lead responsibility for safeguarding and child protection, including online safety remains with them.
- The Khalsa Academy Wolverhampton recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

4.1 The Principal and Senior Leaders will:

- Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information.
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL, governors and trustees to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information.

- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles.
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles.
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident.
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of students, including risk of children being radicalised.
- Ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online-safety procedures.
- Ensure governors and trustees are regularly updated on the nature and effectiveness of the school's arrangements for online safety.
- Ensure the school website meets statutory requirements (https://www.gov.uk/guidance/what-maintained-schools-must-publish-online).
- Create a whole setting culture that incorporates online safety throughout all elements of school life.
- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Implement appropriate and up-to-date policies regarding online safety which addresses the acceptable use of technology, peer on peer abuse, use of social media and mobile technology.
- Work with IT support to ensure that suitable and appropriate filtering and monitoring systems are in place.
- Support the DSL and any deputies by ensuring they have enough time and resources to carry out their responsibilities.
- Ensure robust reporting channels are in place for the whole community to access regarding online safety concerns.
- Undertake appropriate risk assessments regarding the safe use of technology on site.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.
- Ensure that staff, learners and parents/carers are proactively engaged in activities which promote online safety.
- Support staff to ensure that online safety is embedded within a progressive whole setting curriculum which enables all learners to develop an appropriate understanding of online safety.

4.2 The Designated Safeguarding Lead (DSL) will:

- The designated safeguarding lead should take lead responsibility for safeguarding and child protection including online safety. This lead responsibility should not be delegated.
- Work with the Principal and technical staff to review protections for students in the home [e.g. DfE Umbrella scheme filtering for the home] and remote-learning procedures, rules and safeguards, and provide an infographic overview of safeguarding considerations for remote teaching technology.

- Liaise with staff (especially pastoral support staff, school nurses, IT Technicians, and the SENCO, or the named person with oversight for SEN and Mental Health Leads) on matters of safety and safeguarding (including online and digital safety) and when deciding whether to make a referral by liaising with relevant agencies.
- Take day-to-day responsibility for online safety issues and be aware of the potential for serious child protection concerns.
- Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online safety and behaviour apply.
- Work with the Principal, DPO, governors and trustees to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information.
- Undertake Prevent awareness training.
- Update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors/trustees.
- Ensure that online safety education is embedded across the curriculum in line with the statutory RSHE guidance (e.g. by use of the updated UKCIS framework 'Education for a Connected World – 2020 edition') and beyond, in wider school life.
- Promote an awareness of and commitment to online safety throughout the school community, with a strong focus on parents, who are often appreciative of school support in this area, but also including hard-to-reach parents.
- Communicate regularly with SLT and the designated safeguarding and online safety Trustee to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring work and have been functioning/helping.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.
- Ensure adequate provision for staff to flag issues when not in school and for students to disclose issues when off site, especially when in isolation/quarantine/lockdown, e.g. a safe, simple, online form on the school home page that gets mailed securely to the DSL inbox.
- Oversee and discuss 'appropriate filtering and monitoring' with the Trustees and ensure staff are aware of this. (NB: Ofsted inspectors have asked classroom teachers about this).
- Facilitate training and advice for all staff, including supply teachers:
    - all staff must read KCSIE Part 1 and all those working with children Annex A.
    - it would also be advisable for all staff to be aware of Annex C (online safety).
    - cascade knowledge of risks and opportunities throughout the organisation.

- Act as a named point of contact within the setting on all online safeguarding issues.
- Liaise with other members of staff, such as pastoral support staff, IT technicians and the SENDCO, Miss A Evans on matters of online safety.
- Ensure appropriate referrals are made to relevant external partner agencies, as appropriate.

- Work alongside deputy DSLs to ensure online safety is recognised as part of the settings safeguarding responsibilities, and that a coordinated whole school approach is implemented.
- 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 learners safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and child protection training.
- 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 and school policies and procedures.
- Report online safety concerns, as appropriate, to the school management team and local advisory board.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly (termly) with the local advisory board member with a lead responsibility for safeguarding and online safety.
- Will ensure that online tutors, both those engaged by the school as part of the DfE scheme and those hired by parents can be asked to sign the contractor AUP.

4.3 It is the responsibility of all members of staff to:

- Pay particular attention to safeguarding provisions for home-learning and remote-teaching technologies. There are further details in the staff AUP and remote learning safeguarding policies.
- Recognise that RSHE will be introduced in this academic year and that it is a whole-school subject requiring the support of all staff; online safety has become core to this new subject.
- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up.
- Read Part 1 and Part 5 of Keeping Children Safe in Education 2023.
- Read and follow this policy in conjunction with the school's main safeguarding policy.
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.
- Sign the Staff AUP and adhere to its contents.
- Notify the DSL/OSL if policy does not reflect practice at TKAW and follow escalation procedures if concerns are not promptly acted upon.

- Identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RSHE curriculum, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for students).
- Whenever overseeing the use of technology in school or for homework or remote teaching, encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites (find out what appropriate filtering and monitoring systems are in place).
- When supporting students remotely, be mindful of additional safeguarding considerations.
- Carefully supervise and guide students when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age appropriate materials and signposting, and legal issues such as copyright and GDPR.
- Be aware of security best-practice at all times, including password strength and phishing strategies.
- Prepare and check all online sources and resources before using them.
- Encourage students to follow their acceptable use policy at home as well as at school, remind them about it and enforce school sanctions.
- Notify the DSL/OSL of new trends and issues before they become a problem.
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) around the school - inform the DSL/OSL promptly.
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.
- Contribute to the development of our online safety policies.
- Read and adhere to our online safety policy and acceptable use policies.
- Take responsibility for the security of IT systems and the electronic data they use or have access to.
- Model good practice when using technology with learners.
- 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 learners in their care.
- Identify online safety concerns and take appropriate action by following the school safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including reporting to the DSL and signposting learners and parents/carers to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

4.4 It is the responsibility of staff managing the technical environment to:

- As listed in the 'all staff' section, plus:
- Support the Principal and DSL team as they review protections for students in the home [e.g. DfE Umbrella scheme filtering for the home] and remote-learning procedures, rules and safeguards.
- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- Meet the RSHE lead to see how the online-safety curriculum delivered through this new subject can complement the school IT system and vice versa, and ensure no conflicts between educational messages and practice.
- Work closely with the designated safeguarding lead / online safety lead / data protection officer to ensure that school systems and networks reflect school policy.
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc.
- Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL and senior leadership team.
- Maintain up-to-date documentation of the school's online security and technical procedures.
- To report online-safety related issues that come to their attention in line with school policy.
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls.
- Take advantage of solutions which help protect the network and users on it, such as Impero.
- Monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy.
- Work with the Principal to ensure the school website meets statutory DfE requirements.
- Provide technical support and perspective to the DSL and school leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures including network firewall, security software and hardware, content monitoring for staff and students to ensure safe use of the school computer systems as directed by the leadership team to ensure that the settings IT infrastructure is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that our filtering policy and monitoring systems and approaches are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Ensure appropriate technical support and access to our filtering and monitoring systems is given to the DSL and/or deputies to enable them to take appropriate safeguarding action when required.

4.5 It is the responsibility of learners (at a level that is appropriate to their individual age and ability) to:

- Read, understand, sign and adhere to the student acceptable use policy and review this annually.
- Treat home learning during any isolation/quarantine or bubble/school lockdown in the same way as regular learning in school and behave as if a teacher or parent were watching the screen.
- Avoid any private communication or use of personal logins/systems to communicate with or arrange meetings with school staff or tutors.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials, including any concerns about a member of school staff or supply teacher or online tutor.
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology, at school, home or anywhere else.
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media.
- Remember the rules on the misuse of school technology – devices and logins used at home should be used just like if they were in full view of a teacher.
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems.
- Engage in age/ability appropriate online safety education.
- Contribute to the development of online safety policies.
- Read and adhere to the acceptable use and behaviour policies.
- Respect the feelings and rights of others, on and offline.
- Take an appropriate level of responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if they are concerned about anything, they or others experience online.

4.6 It is the responsibility of parents and carers to:

- Encourage children to engage fully in home-learning during any period of isolation/quarantine or bubble/school closure and flag any concerns.
- Support the child during remote learning to avoid video calls in a bedroom if possible and if not, to ensure the child is fully dressed and not in bed, with the camera off.
- If organising private online tuition, remain in the room if possible, ensure the child knows tutors should not arrange new sessions directly with the child or attempt to communicate privately.
- Read our acceptable use policies 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 and abide by the school policies that constitute the home school agreement.
- Seek help and support from the school or other appropriate agencies, if they or their child encounter online issues.
- Contribute to the development of our online safety policies.
- Use our systems, such as parental engagement platforms and other IT resources, safely and appropriately.

- Take responsibility for their own awareness in relation to the risks and opportunities posed by the new and emerging technologies that their children access and use at home.

5. Education and engagement approaches

5.1 Education and engagement with learners

- The setting will establish and embed a whole school culture and will raise awareness and promote safe and responsible internet use amongst learners by:
  - ensuring our curriculum and whole school approach is developed in line with the UK Council for Internet Safety (UKCIS) 'Education for a Connected World Framework' and DfE 'Teaching online safety in school' guidance.
  - ensuring online safety is addressed in Relationships Education, Relationships and Sex Education, Health Education, Citizenship, assemblies, whole school online safety day and Computing programmes of study.
  - reinforcing online safety principles in other curriculum subjects as appropriate, and whenever technology or the internet is used on site.
  - implementing appropriate peer education approaches during whole school online safety day, assemblies, focus groups and online safety education during computing programmes of study.
  - creating a safe environment in which all learners feel comfortable to say what they feel, without fear of getting into trouble and/or being judged for talking about something which happened to them online.
  - involving the DSL (or a deputy) as part of planning for online safety lessons or activities, so they can advise on any known safeguarding cases, and ensure support is in place for any learners who may be impacted by the content.
  - making informed decisions to ensure that any educational resources used are appropriate for our learners.
  - using external visitors, where appropriate, to complement and support our internal online safety education approaches.
  - providing online safety education as part of the transition programme across the key stages and/or when moving between establishments.
  - rewarding positive use of technology through the use of the behaviour policy. (section 4, rewards policy).

- The Khalsa Academy Wolverhampton will support learners to understand and follow our acceptable use policies in a way which suits their age and ability by:
  - displaying acceptable use posters in all rooms with internet access.
  - informing learners that network and internet use will be monitored for safety and security purposes, and in accordance with legislation.
  - seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.

- The Khalsa Academy Wolverhampton will ensure learners develop the underpinning knowledge and behaviours needed to navigate the online world safely, in a way which suits their age and ability by:
    - ensuring age appropriate education regarding safe and responsible use precedes internet access.
    - teaching learners to evaluate what they see online and recognise techniques used for persuasion, so they can make effective judgements about if what they see is true, valid or acceptable.
    - educating them in the effective use of the internet to research, including the skills of knowledge location, retrieval and evaluation.
    - enabling them to understand what acceptable and unacceptable online behaviour looks like.
    - preparing them to identify possible online risks and make informed decisions about how to act and respond.
    - ensuring they know how and when to seek support if they are concerned or upset by something they see or experience online.

5.2 Vulnerable Learners

- The Khalsa Academy Wolverhampton recognises that any learner can be vulnerable online, and vulnerability can fluctuate depending on their age, developmental stage and personal circumstances. However, there are some learners, for example looked after children and those with special educational needs, who may be more susceptible or may have less support in staying safe online.
- The Khalsa Academy Wolverhampton will ensure that differentiated and appropriate online safety education, access and support is provided to vulnerable learners as noted in the SEND policy.
- Staff at The Khalsa Academy Wolverhampton will seek input from specialist staff as appropriate, including the DSL and SENDCO to ensure that the policy and curriculum is appropriate to our community's needs.

5.3 Training and engagement with staff

- We will
    - provide and discuss the online safety policy and procedures with all members of staff as part of induction and ongoing CPD.
    - provide up-to-date and appropriate online safety training for all staff which is integrated, aligned and considered as part of our overarching safeguarding approach.
        - During whole school training sessions provided as part of ongoing CPD
        - During staff training and induction
    - Staff training covers the potential risks posed to learners (content, contact and conduct) as well as our professional practice expectations.
    - build on existing expertise by provide opportunities for staff to contribute to and shape our online safety approaches, including curriculum, 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, including personal use of social media, can have an impact on their professional role and reputation.
- highlight useful educational resources and tools which staff could use with learners.
- ensure all members of staff are aware of the procedures to follow regarding online safety concerns involving learners, colleagues or other members of the community.

5.4 Awareness and engagement with parents and carers

- The Khalsa Academy Wolverhampton recognises that parents and 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 will build a partnership approach to online safety with parents and carers by
  - providing information and guidance on online safety in a variety of formats by providing information during specific training events offered to parents and carers and information sent home either via electronic or paper-based methods.
  - drawing their attention to our online safety policy and expectations in our newsletters and other external communication (such as letters and social media channels) as well as in our prospectus and on our website.
  - requesting parents and carers read online safety information as part of joining our community, for example, within our behaviour policy and other policies that form part of the whole school agreement.
  - requiring them to read our acceptable use policies and discuss the implications with their children.

6. Reducing Online Risks

- The Khalsa Academy Wolverhampton 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 educational benefit and undertake appropriate risk assessments before their use in the school is permitted.
  - ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that access is appropriate.
  - recognise that due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our systems or devices and as such identify clear procedures to follow if breaches or concerns arise.

- 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. This is clearly outlined in our

acceptable use policies and highlighted through a variety of education and training approaches.

7. Safer Use of Technology

7.1 Classroom use

- The Khalsa Academy Wolverhampton uses a wide range of technology. This includes access to:
    - Computers, laptops, tablets and other digital devices
    - Internet, which may include search engines and educational websites
    - Google classroom
    - Email
    - Games consoles and other games-based technologies
    - Digital cameras, web cams and video cameras
- All setting owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, (particularly YouTube), tools and apps fully before use in the classroom or recommending for use at home.
- The setting will use appropriate search tools as identified following an informed risk assessment.
    - Learners are allowed to use Google search in line with the schools digital vision, Google safe search is enforced along with administrative control of Google Chrome and removal of other web browsers.
- We will ensure that the use of internet-derived materials, by staff and learners complies with copyright law and acknowledge the source of information.
- Supervision of internet access and technology use will be appropriate to learners' age and ability.
    - Key Stage 3, 4, 5
        - Learners will use age-appropriate search engines and online tools.
        - Learners will be appropriately supervised when using technology, according to their ability and understanding.

7.2 Managing internet access

- We will maintain a written record of users who are granted access to our devices and systems, including Wi-Fi.
- All staff, learners and visitors will read and agree an acceptable use policy before being given access to our computer system, IT resources or the internet.

7.3 Filtering and monitoring

- The Khalsa Academy Wolverhampton uses Sonicwall and Senso to control access to internet content. In order to unblock a website it would need to be checked via the DSL to ensure suitability.

7.3.1 Decision making

- The Khalsa Academy Wolverhampton local advisory board members and leaders have ensured that our school has age and ability appropriate filtering and monitoring in place to limit learner's exposure to online risks.
- Changes to the filtering and monitoring approach will be risk assessed by DSL with support from staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- The local advisory board members and leaders are mindful to ensure that "over blocking" does not unreasonably restrict access to educational activities and safeguarding materials.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.

7.3.2 Appropriate filtering

- The Khalsa Academy Wolverhampton's education broadband connectivity is provided through Virgin Media Business.
- The Khalsa Academy Wolverhampton uses Sonicwall filtering.
    - Sonicwall filtering blocks access to sites which could promote or include harmful and/or inappropriate behaviour or material. This includes content which promotes discrimination or extremism, drugs/substance misuse, malware/hacking, gambling, piracy and copyright theft, pro-self-harm, eating disorder and/or suicide content, pornographic content and violent material.
    - Sonicwall is a member of Internet Watch Foundation (IWF) and blocks access to illegal Child Abuse Images and Content (CAIC).
    - Sonicwall integrates the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'
- We work with Sonicwall and Senso to ensure that our filtering policy is continually reviewed to reflect our needs and requirements.
- If learners or staff discover unsuitable sites or material, they are required to report the concern immediately to DSL, report the URL of the site to technical staff/services.
- Filtering breaches will be reported to the DSL (or deputy) and technical staff and will be recorded and escalated as appropriate.
- Parents/carers will be informed of filtering breaches involving learners as appropriate.
- Any access to material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, the police and/or CEOP.
- Youtube is filtered for students and therefore all reasonable steps are taken to filter out inappropriate videos.
- Year 7 – 11 Students mobile phones are not allowed to be used in school as per the mobile phone policy and therefore are not connected to the school Wi-Fi. Sixth Formers are allowed

to use mobile phones only in the designated sixth form area using the filtered WiFi provided specifically for them using filters as mentioned above.
- Visitor devices will be joined to the guest Wi-Fi network where appropriate and therefore not have access to sensitive data.

7.3.3 Appropriate monitoring

- We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:
    - Physical monitoring (supervision)
    - Monitoring internet and web access (reviewing logfile information)
    - Active/pro-active technology monitoring services. (Senso)
- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.
- If a concern is identified via monitoring approaches we will respond in line with the safeguarding policy.

7.4 Managing personal data online

- Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation.
    - Full information can be found in our data protection policy which can be accessed at https://khalsatrust.s3.amazonaws.com/uploads/document/KAT-DATA-PROTECTION-FOI-and-SAR-POLICY-FINAL-vs-1.pdf?t=1637051496?ts=1637051496

7.5 Security and management of information systems

- We take appropriate steps to ensure the security of our information systems, including:
    - Virus protection being updated regularly.
    - Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
    - Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
    - Not downloading unapproved software to work devices or opening unfamiliar email attachments.
    - Preventing, as far as possible, access to websites or tools which could compromise our systems, including anonymous browsing and other filtering bypass tools eg disabling proxy in school.
    - Checking files held on our network, as required and when deemed necessary by leadership staff.
    - The appropriate use of user logins and passwords to access our network.
        - Specific user logins and passwords will be enforced for all users.
    - All users are expected to log off or lock their screens/devices if systems are unattended.
    - Further information about technical environment safety and security can be obtained from the school technical department.

7.5.1 Password policy

- All members of staff have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.
- From year 7 all learners are provided with their own unique username and private passwords to access our systems; learners are responsible for keeping their password private.
- We require all users to
    - use strong passwords for access into our system. (enforced by policy)
    - staff to change their passwords if they suspect it has been compromised.
    - not share passwords or login information with others or leave passwords/login details where others can find them.
    - not to login as another user at any time.
    - staff to lock access to devices/systems when not in use.

7.6 Managing the safety of our website

- We will ensure that information posted on our website meets the requirements as identified by the DfE. The school website is maintained by IT support in line with guidance from appropriate leadership link.

- 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 learners' 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.

7.7 Publishing images and videos online

- We will ensure that all images and videos shared online are used in accordance with the associated policies, including (but not limited to) data security, acceptable use policies, codes of conduct/behaviour, (use on social media and use of mobile devices is covered later).
- Written permission from parents or carers will be obtained before photographs of students / students are published on the school website / social media / local press
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school / academy equipment, the personal equipment of staff should not be used for such purposes.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.

7.8 Managing email

- Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including the safeguarding policy and data protection policy.
- The forwarding of any chain messages/emails is not permitted.
- Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email. Staff should only use recognised school email systems in relation to work.
- Setting email addresses and other official contact details will not be used to set up personal social media accounts.

- Members of the community will immediately tell the DSL or a DDSL, if they receive offensive communication, and this will be recorded in our safeguarding files/records.
- Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked on site at the discretion of the Principal.

7.8.1 Staff email

- All members of staff are provided with an email address to use for all official communication; the use of personal email addresses by staff for any official business is not permitted.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, learners and parents.

7.8.2 Learner email

- Leaners have access to email provided by the school and this is monitored by the school network manager. Additionally student email is limited to the school domain.

7.9 Educational use of videoconferencing and/or webcams

- The Khalsa Academy Wolverhampton recognise that videoconferencing and use of webcams can be a challenging activity but brings a wide range of learning benefits.
    - All video conferencing and webcam equipment will be switched off when not in use and will not be set to auto-answer.
    - Video conferencing equipment connected to the educational broadband network.
    - It will use the national E.164 numbering system and display their H.323 ID name; external IP addresses will not be made available to other sites.
    - Videoconferencing contact details will not be posted publicly.
    - Videoconferencing equipment will not be taken off the premises without prior permission from the Principal.
    - Staff will ensure that external videoconferencing opportunities and tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.
    - Video conferencing equipment and webcams will be kept securely and, if necessary, locked away or disabled when not in use.

7.9.1 Users

- Parents/carers consent will be obtained prior to learners taking part in videoconferencing activities.
- Learners will ask permission from a member of staff before making or answering a videoconference call or message.
- Videoconferencing will be supervised appropriately, according to the learners age and ability. This will include:
    - Only connecting to pre-approved videoconferencing calls

    - Ensuring the suitability of the content to be shown via videoconference link by prior discussion and agreement with the provider / destination of the call.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment.
- The unique log on and password details for the videoconferencing services will only be issued to members of staff and should be kept securely, to prevent unauthorised access.

7.9.2 Content

- When recording a videoconference lesson, it should be made clear to all parties at the start of the conference and written permission will be obtained from all participants; the reason for the recording must be given and recorded material will be stored securely.
- If third party materials are included, we will check that recording is permitted to avoid infringing the third-party intellectual property rights.
- We will establish dialogue with other conference participants before taking part in a videoconference; if it is a non-educational site, staff will check that the material they are delivering is appropriate for the learners.

7.10 Management of learning platforms

- The Khalsa Academy Wolverhampton uses Google Classroom as its official learning platform.
- Leaders and staff will regularly monitor the usage of the Learning Platform (LP), including message/communication tools and publishing facilities.
- Only current members of staff, learners and parents will have access to the LP.
- When staff and learners leave the setting, their account will be disabled or transferred to their new establishment.
- Learners and staff will be advised about acceptable conduct and use when using the LP.
- All users will be mindful of copyright and will only upload appropriate content onto the LP.
- Any concerns about content on the LP will be recorded and dealt with in the following ways:
    - The user will be asked to remove any material deemed to be inappropriate or offensive.
    - If the user does not comply, the material will be removed by the site administrator.
    - Access to the LP for the user may be suspended.
    - The user will need to discuss the issues with a member of leadership before reinstatement.
    - A learner's parents/carers may be informed.
    - If the content is illegal, we will respond in line with existing child protection procedures.
- Learners may require editorial approval from a member of staff. This may be given to the learner to fulfil a specific aim and may have a limited time frame.
- A visitor may be invited onto the LP by a member of the leadership as part of an agreed focus or a limited time slot.

7.11 Management of applications (apps) used to record children's progress

- We use Classcharts to track learners progress and share appropriate information with parents and carers.
- The Principal will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that use takes place in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.
- To safeguard learner's data
    - only learner issued devices will be used for apps that record and store learners' personal details, attainment or photographs.
    - personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store learners' personal details, attainment or images.
    - devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
    - all users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
    - parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

8. Social Media

8.1 Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of The Khalsa Academy Wolverhampton community.
- The term social media may include (but is not limited to) blogs, wikis, social networking sites, forums, bulletin boards, online gaming, apps, video/photo sharing sites, chatrooms and instant messenger.
- All members of The Khalsa Academy Wolverhampton community are expected to engage in social media in a positive and responsible manner.
    - All members of The Khalsa Academy Wolverhampton community are advised not to post or share content that may be considered threatening, hurtful or defamatory to others on any social media service.
- We will control learner and staff access to social media whilst using school provided devices and systems on site. This controlled via the school internet filtering systems.
    - The use of social media during teaching/PPA hours for personal use is not permitted for staff.
    - The use of social media during school hours for personal use is not permitted for learners.
    - Inappropriate or excessive use of social media during school hours or whilst using school devices may result in removal of internet access and/or disciplinary or legal action.
- Concerns regarding the online conduct of any member of The Khalsa Academy Wolverhampton community on social media, will be reported to the DSL and be managed in

accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.

8.2 Staff personal use of social media

- The safe and responsible use of social media sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff, including volunteers, as part of our code of conduct and acceptable use policies.

8.2.1 Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the school
    - Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media services. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include, but is not limited to:
    - Setting appropriate privacy levels on their personal accounts/sites.
    - Being aware of the implications of using location sharing services.
    - Opting out of public listings on social networking sites.
    - Logging out of accounts after use.
    - Using strong passwords.
    - Ensuring staff do not represent their personal views as being that of the setting.
- Members of staff are encouraged not to identify themselves as employees of The Khalsa Academy Wolverhampton on their personal social networking accounts; this is to prevent information being linked with the setting and to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online. Staff are expected to ensure that their social media use is compatible with their professional role and is in accordance our policies, and the wider professional and legal framework.
- Information and content that staff members have access to as part of their employment, including photos and personal information about learners and their family members or colleagues, will not be shared or discussed on social media sites.
- Members of staff will notify the leadership team immediately if they consider that any content shared on social media sites conflicts with their role.

8.2.2 Communicating with learners and parents/carers

- Staff will not use personal social media accounts to contact learners or parents/carers, nor should any contact be accepted.
- All members of staff are advised not to communicate with or add any current or past learners or their family members, as 'friends' on any personal social media sites, applications or profiles.
- Any pre-existing relationships or exceptions which compromise this requirement will be discussed with the DSL and the Principal.
    - Decisions made and advice provided in these situations will be formally recorded in order to safeguard learners, the setting and members of staff.
- If ongoing contact with learners is required once they have left the setting, members of staff will be expected to use existing alumni networks, or use official setting provided communication tools.
    - Any communication from learners and parents received on personal social media accounts will be reported to the DSL (or deputy) and the line manager or Principal as appropriate.

8.3 Learners use of social media

- Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach via age appropriate sites and resources.
- We are aware that many popular social media sites are not permitted for use by children under the age of 13, or in some cases higher. As such, we will not create accounts for learners under the required age as outlined in the services terms and conditions.
- Any concerns regarding learners use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour.
- Concerns regarding learners use of social media will be shared with parents/carers as appropriate, particularly when concerning underage use of social media services and games.
- Learners will be advised:
    - to consider the benefits and risks of sharing personal details or information 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 appropriate adults' permission, and to only do so when a trusted adult is present.
    - to 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 on social media, both within the setting and externally.

8.4 Official use of social media

- The Khalsa Academy Wolverhampton official social media channels are:
    - https://www.facebook.com/The-Khalsa-Academy-Wolverhampton-115806705789330
- The official use of social media sites by The Khalsa Academy Wolverhampton only takes place with clear educational or community engagement objectives and with specific intended outcomes.
    - The official use of social media as a communication tool has been formally risk assessed and approved by the Principal.
    - Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.
- Official social media channels have been set up as distinct and dedicated accounts for official educational or engagement purposes only.
    - Staff use setting provided email addresses to register for and manage official social media channels.
    - Official social media sites are suitably protected and, where possible, run or linked from our website.
    - Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.
- Official social media use will be conducted in line with existing policies, including but not limited to anti-bullying, image/camera use, data protection, confidentiality and child protection.
- All communication on official social media platforms by staff on behalf of the setting will be clear, transparent and open to scrutiny.
- Parents/carers and learners will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
    - Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.
    - Any official social media activity involving learners will be moderated if possible.
- Parents and carers will be informed of any official social media use with learners; written parental consent will be obtained, as required.
- We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.
- Leadership team use platforms such as WhatsApp for business related communication but this does not include any sensitive information such as student names.

8.4.1 Staff expectations

- Members of staff who follow and/or like our official social media channels will be advised to use dedicated professionals accounts where possible, to avoid blurring professional boundaries.

- If members of staff are participating in online social media activity as part of their capacity as an employee of the setting, they will:
    - Sign our social media acceptable use policy.
    - Be aware they are an ambassador for the setting.
    - Be professional, responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
    - Always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection and equalities laws.
    - Ensure appropriate consent has been given before sharing images on the official social media channel.
    - Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.
    - Not engage with any private/direct messaging with current or past learners or parents/carers.
    - Inform their line manager, the DSL (or deputy) and/or the Principal of any concerns, such as criticism, inappropriate content or contact from learners.

9. Mobile Technology: Use of Personal Devices and Mobile Phones

The Khalsa Academy Wolverhampton recognises and accepts that parents/carers give their children mobile phones to protect them from everyday risks involving personal security and safety. Many students travel alone on public transport, commute long distances to school and/or take part in extracurricular activities outside of normal school hours.

There is considerable evidence that mobile phone use in schools, harms student attainment.

With the above information coming to light, legislation allows schools and Head Teachers to ban mobile phones from their school premises. This is supported by the Department for Education and OFSTED.

The use of mobile phones/smart devices (if seen/heard) on our site is now prohibited.

See The Khalsa Academy Wolverhampton mobile phone policy at:

https://khalsatrust.s3.amazonaws.com/uploads/document/Mobile-Phone-Policy-Final.pdf?t=1576054865

9.1 Expectations

- All use of mobile technology including mobile phones and personal devices such as tablets, games consoles and wearable technology will take place in accordance with our policies, such as anti-bullying, behaviour and child protection and with the law.
- Electronic devices of any kind that are brought onto site are the responsibility of the user.
    - All members of The Khalsa Academy Wolverhampton community are advised to take steps to protect their mobile phones or personal devices from loss, theft or damage;

we accept no responsibility for the loss, theft or damage of such items on our premises.
    - All members of The Khalsa Academy Wolverhampton community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- Mobile phones and personal devices are not permitted to be used while in school.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with in line with our anti-bullying and behaviour policies.
- All members of The Khalsa Academy Wolverhampton community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or child protection policies.

9.2 Staff use of personal devices and mobile phones

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant policy and procedures, such as confidentiality, child protection, data security and acceptable use.
- Staff will be advised to
    - keep mobile phones and personal devices in a safe and secure place (such as in a locked drawer or on their person) during lesson time.
    - keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
    - ensure that Bluetooth or other forms of communication, such as 'airdrop', are hidden or disabled during lesson times.
    - not use personal devices during teaching periods, unless written permission has been given by the Principal or line manager such as in emergency circumstances.
    - ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting learners or parents and carers.
    - Any pre-existing relationships which could undermine this, will be discussed with the DSL (or deputy) and Principal.
- Staff will not use personal devices or mobile phones:
    - to take photos or videos of learners and will only use work-provided equipment for this purpose.
    - directly with learners and will only use work-provided equipment during lessons/educational activities.
- If a member of staff breaches our policy, action will be taken in line with our staff behaviour and allegations policy.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device, or have committed a criminal offence using a personal device or mobile

phone, the police will be contacted and the LADO (Local Authority Designated Officer) will be informed in line with our allegations policy.

9.3 Learners use of personal devices and mobile phones

- Learners will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
    - The Khalsa Academy Wolverhampton expects learners' personal devices and mobile phones to be switched off and in their bag in line with the mobile phone policy.

- If a learner needs to contact his/her parents or carers they will be allowed to use a school phone.
    - Parents are advised to contact their child via the school office; exceptions may be permitted on a case-by-case basis, as approved by the Principal.
- Mobile phones or personal devices will not be used by learners during lessons or formal educational time unless as part of a prescribed learning activity.
    - The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.
    - If members of staff have an educational reason to allow learners to use their mobile phones or personal devices as part of an educational activity, it will only take place when approved by the Leadership Team.
- Mobile phones and personal devices must not be taken into examinations.
    - Learners found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations.
- If a learner breaches the policy, the phone or device will be confiscated and held in a secure place.
    - Staff may confiscate a learner's mobile phone or device if it is seen in line with the mobile phone policy.
    - Searches of mobile phone or personal devices will be carried out in accordance with our mobile phone policy and in line with the DfE 'Searching, Screening and Confiscation' guidance.
    - Learner's mobile phones or devices may be searched by a member of the leadership team, with the consent of the learner or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes our mobile phone policy and in line with the DfE 'Searching, Screening and Confiscation' guidance.
    - Mobile phones and devices that have been confiscated will be released to parents/ carers at the end of the day.
    - If there is suspicion that material on a learner's personal device or mobile phone may be illegal, or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

9.4 Visitors' use of personal devices and mobile phones

- Parents/carers and visitors, including volunteers and contractors, should ensure that mobile phones are only used when appropriate and not in the presence of students.
- Appropriate signage and information is provided to inform parents/carers and visitors of expectations of use.
- Visitors, including volunteers and contractors, who are on site for regular or extended periods of time are expected to use their mobile phones and personal devices in accordance with our acceptable use policy and other associated policies, including but not limited to anti-bullying, behaviour, child protection and image use.
- Members of staff are expected to challenge visitors if they have concerns and inform the DSL (or deputy) or Principal of any breaches of our policy.

10. Responding to Online Safety Incidents

- All members of the community will be made aware of the reporting procedure for online safety concerns, including breaches of filtering, peer on peer abuse, including cyberbullying and youth produced sexual imagery (sexting), online sexual violence and harassment, online abuse and exploitation and illegal content.
- All members of the community will respect confidentiality and the need to follow the official procedures for reporting concerns.
    - Learners, parents 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 learners to work in partnership with us to resolve online safety issues.
- After any investigations are completed, leadership staff will debrief, identify lessons learnt and implement any policy or curriculum changes, as required.
- If we are unsure how to proceed with an incident or concern, the DSL (or deputy) will seek advice from the Wolverhampton Safeguarding/Local Authority.
- Where there is a concern that illegal activity has taken place, we will contact the police using 101, or 999 if there is immediate danger or risk of harm as appropriate.
- If information relating to a specific incident or a concern needs to be shared beyond our community, for example if other local settings are involved or the wider public may be at risk, the DSL and/or Principal will speak with the police and the Wolverhampton Safeguarding first, to ensure that potential criminal or child protection investigations are not compromised.

10.1 Concerns about learner online behaviour and/or welfare

- The DSL (or deputy) will be informed of all online safety concerns involving safeguarding or child protection risks in line with our child protection policy.
- All concerns about learners will be recorded in line with our child protection policy.

- The Khalsa Academy Wolverhampton recognises that whilst risks can be posed by unknown individuals or adults online, learners can also abuse their peers; all online peer on peer abuse concerns will be responded to in line with our child protection and behaviour policies.
- The DSL (or deputy) will ensure that online safety concerns are escalated and reported to relevant partner agencies in line with local policies and procedures.
- Appropriate sanctions and/or pastoral/welfare support will be offered to learners as appropriate. Civil or legal action will be taken if necessary.
- We will inform parents/carers of online safety incidents or concerns involving their child, as and when required.

10.2 Concerns about staff online behaviour and/or welfare

- Any complaint about staff misuse will be referred to the Principal in accordance with our allegations against staff policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate disciplinary, civil and/or legal action will be taken in accordance with our staff code of conduct.
- Welfare support will be offered to staff as appropriate.

10.3 Concerns about parent/carer online behaviour and/or welfare

- Concerns regarding parents/carers behaviour and/or welfare online will be reported to the Principal and/or DSL (or deputy). The Principal and/or DSL will respond to concerns in line with existing policies, including but not limited to child protection, anti-bullying, complaints, allegations against staff, home-school agreements, acceptable use and behaviour policy.
- Civil or legal action will be taken if necessary.
- Welfare support will be offered to parents/carers as appropriate.

11. Procedures for Responding to Specific Online Concerns

11.1 Online sexual violence and sexual harassment between children

- Our Principal and DSL and appropriate members of staff have accessed and understood part 5 of 'Keeping children safe in education' 2023.
    - Full details of our response to peer on peer abuse, including sexual violence and harassment can be found in our child protection policy.
- The Khalsa Academy Wolverhampton 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
    - 'Upskirting', which typically involves taking a picture under a person's clothing without them knowing, with the intention of obtaining sexual gratification, or causing the victim humiliation, distress or alarm. It is a criminal offence

    - Unwanted sexual comments and messages on social media
    - Online sexual exploitation
- 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 any concerns relating to online sexual violence and sexual harassment, we will:
    - immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.
    - if content is contained on learners personal devices, they will be managed in accordance with the DfE '[searching screening and confiscation'](#) advice.
    - provide the necessary safeguards and support for all learners involved, such as implementing safety plans, offering advice on blocking, reporting and removing online content, and providing appropriate counselling/pastoral support.
    - implement appropriate sanctions in accordance with our behaviour policy.
    - inform parents and carers, if appropriate, about the incident and how it is being managed.
    - If appropriate, make referrals to partner agencies, such as Wolverhampton Safeguarding and/or the police.
    - if the concern involves children and young people at a different educational setting, the DSL will 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.
- The Khalsa Academy Wolverhampton recognises that 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.
- The Khalsa Academy Wolverhampton recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- To help minimise concerns, The Khalsa Academy Wolverhampton 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 by implementing a range of age and ability appropriate educational methods as part of our curriculum in line with the curriculum policies and curriculum progression maps of each department.
- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between learners.

11.2 Youth produced sexual imagery ("sexting")

- The Khalsa Academy Wolverhampton recognises youth produced sexual imagery (also known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).

- We will follow the advice as set out in the non-statutory UKCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people'
    - Youth produced sexual imagery or 'sexting' is defined as the production and/or sharing of sexual photos and videos of and by young people who are under the age of 18. It includes nude or nearly nude images and/or sexual acts.
    - It is an offence to possess, distribute, show and make indecent images of children. The Sexual Offences Act 2003 defines a child, for the purposes of indecent images, as anyone under the age of 18.
- The Khalsa Academy Wolverhampton will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of creating or sharing youth produced sexual imagery by implementing preventative approaches, via a range of age and ability appropriate educational methods including but not limited to online safety presentations during assemblies and online safety days.
- We will ensure that all members of the community are aware of sources of support regarding the taking and sharing of youth produced sexual imagery. This will be made available through the official school website or other appropriate channels.
- 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.
- We will not:
    - view any suspected youth produced sexual imagery, unless there is no other option, or there is a clear safeguarding need or reason to do so.
        - If it is deemed necessary, the imagery will only be viewed where possible by the DSL, and any decision making will be clearly documented.
    - send, share, save or make copies of content suspected to be an indecent image/video of a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.
- 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 policies and the relevant local procedures.
    - ensure the DSL (or deputy) responds in line with the UKCIS guidance.
    - Store any devices containing potential youth produced sexual imagery securely
        - If content is contained on learners personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
        - If a potentially 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 in line with the UKCIS guidance which considers the age and vulnerability of learners involved, including the possibility of carrying out relevant checks with other agencies.
    - inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate.
    - make a referral to Wolverhampton Safeguarding and/or the police, as deemed appropriate in line with the UKCIS guidance.

- provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
- implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
- consider the deletion of images in accordance with the UKCIS 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.

11.3 Online abuse and exploitation (including child sexual abuse and sexual or criminal exploitation)

- The Khalsa Academy Wolverhampton recognises online abuse and exploitation, including sexual abuse and sexual or criminal exploitation, as a safeguarding issue and all concerns will be reported to and dealt with by the DSL (or deputy), in line with our child protection policy.
- The Khalsa Academy Wolverhampton will ensure that all members of the community are aware of online child abuse and sexual or criminal exploitation, including the possible grooming approaches which may be employed by offenders to target learners, and understand how to respond to concerns.
- We will implement preventative approaches for online child abuse and exploitation via a range of age and ability appropriate education for learners, staff and parents/carers. This will be through our safeguarding policy, online safety education programmes and through other appropriate channels.
- We will ensure that all members of the community are aware of the support available regarding online child abuse and exploitation, both locally and nationally.
- We will ensure that the 'Click CEOP' report button used to report online child sexual abuse is visible and available to learners and other members of our community on the school website.
- If made aware of an incident involving online child abuse and/or exploitation, we will:
    - act in accordance with our child protection policies and the relevant KSCMP procedures.
    - store any devices containing evidence securely.
        - If content is contained on learners personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
        - If any evidence is stored on our network or devices, we will act to block access to other users and isolate the content.
    - if appropriate, make a referral to Wolverhampton Safeguarding and inform the police via 101, or 999 if a learner is at immediate risk.
    - carry out a risk assessment which considers any vulnerabilities of learner(s) involved, including carrying out relevant checks with other agencies.

    - inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate.
    - provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.
    - review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.
- We will respond to concerns regarding online abuse and exploitation, regardless of whether the incident took place on our premises or using setting provided or personal equipment.
    - Where possible and appropriate, learners will be involved in decision making. If appropriate, they will be empowered to report concerns themselves with support, for example if the concern relates to online sexual abuse via CEOP: www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through Wolverhampton Safeguarding and/or police.
- 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 by the DSL (or deputy).
- If members of the public or learners at other settings are believed to have been targeted, the DSL (or deputy) will seek advice from the police and/or the Wolverhampton Safeguarding before sharing specific information to ensure that potential investigations are not compromised.

11.4 Indecent Images of Children (IIOC)

- The Khalsa Academy Wolverhampton will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC) as appropriate to the age and ability.
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- We will seek to prevent accidental access to IIOC by using an Internet Service Provider (ISP) which subscribes to the Internet Watch Foundation (IWF) block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the police and/or the Wolverhampton Safeguarding.
- If made aware of IIOC, we will:
    - act in accordance with our child protection policy and the relevant KSCMP procedures.
    - store any devices involved securely.
    - immediately inform appropriate organisations, such as the IWF and police.
- If made aware that a member of staff or a learner 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 IWF 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 and carers.
- 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 IWF via www.iwf.org.uk .
    - inform the police via 101 or 999 if there is an immediate risk of harm, and Children's Social Work Service, as appropriate.
    - only store copies of images (securely, where no one else has access to them and delete all other copies) following a written request from the police.
    - report concerns, as appropriate to parents/carers.
- If made aware that a member of staff is in possession of indecent images of children on school provided devices, we will:
    - ensure that the Principal is informed in line with our managing allegations against staff policy.
    - inform the Local LADO and other relevant organisations in accordance with our managing allegations against staff policy.
    - quarantine any devices until police advice has been sought.

11.5 Online bullying

- Online bullying, along with all other forms of bullying, will not be tolerated at The Khalsa Academy Wolverhampton.
- Full details of how we will respond to online bullying are set out in our values and rewards policy. https://khalsatrust.s3.amazonaws.com/uploads/document/TKAW-Values-Rewards-Policy.pdf?t=1647249841?ts=1652698742

11.6 Online hate

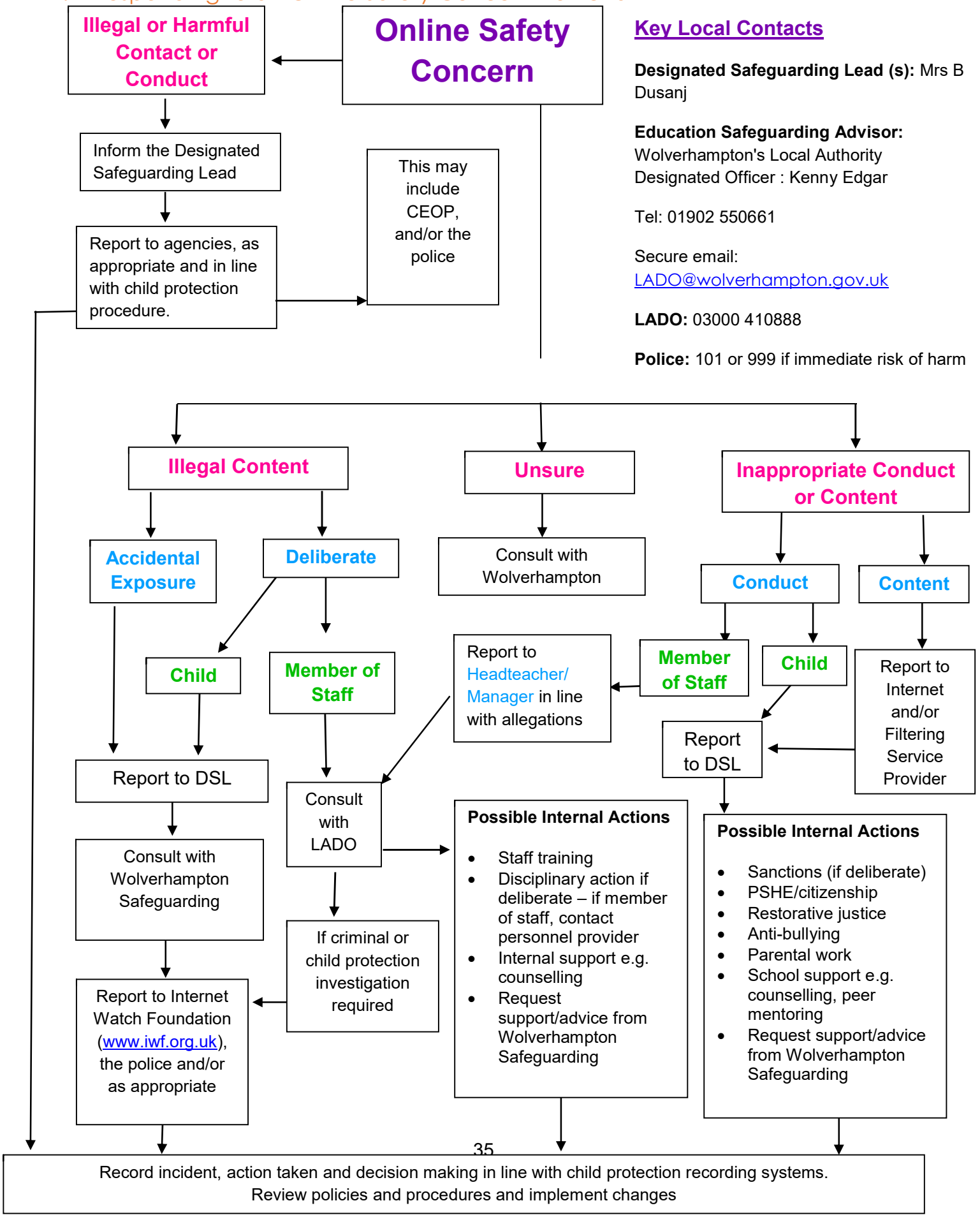
- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at The Khalsa Academy Wolverhampton and will be responded to in line with existing policies, including child protection, anti-bullying and behaviour.
- All members of the community will be advised to report online hate in accordance with 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 Wolverhampton Safeguarding and/or the police.

11.7 Online radicalisation and extremism

- As listed in this policy, we will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site. This will be in-line with the school content filtering system.

- If we are concerned that a learner or adult 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 policy.
- If we are concerned that 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 allegations policies.

12. Responding to an Online Safety Concern Flowchart



Key Local Contacts

Designated Safeguarding Lead (s): Mrs B Dusanj

Education Safeguarding Advisor: Wolverhampton's Local Authority Designated Officer : Kenny Edgar

Tel: 01902 550661

Secure email: LADO@wolverhampton.gov.uk

LADO: 03000 410888

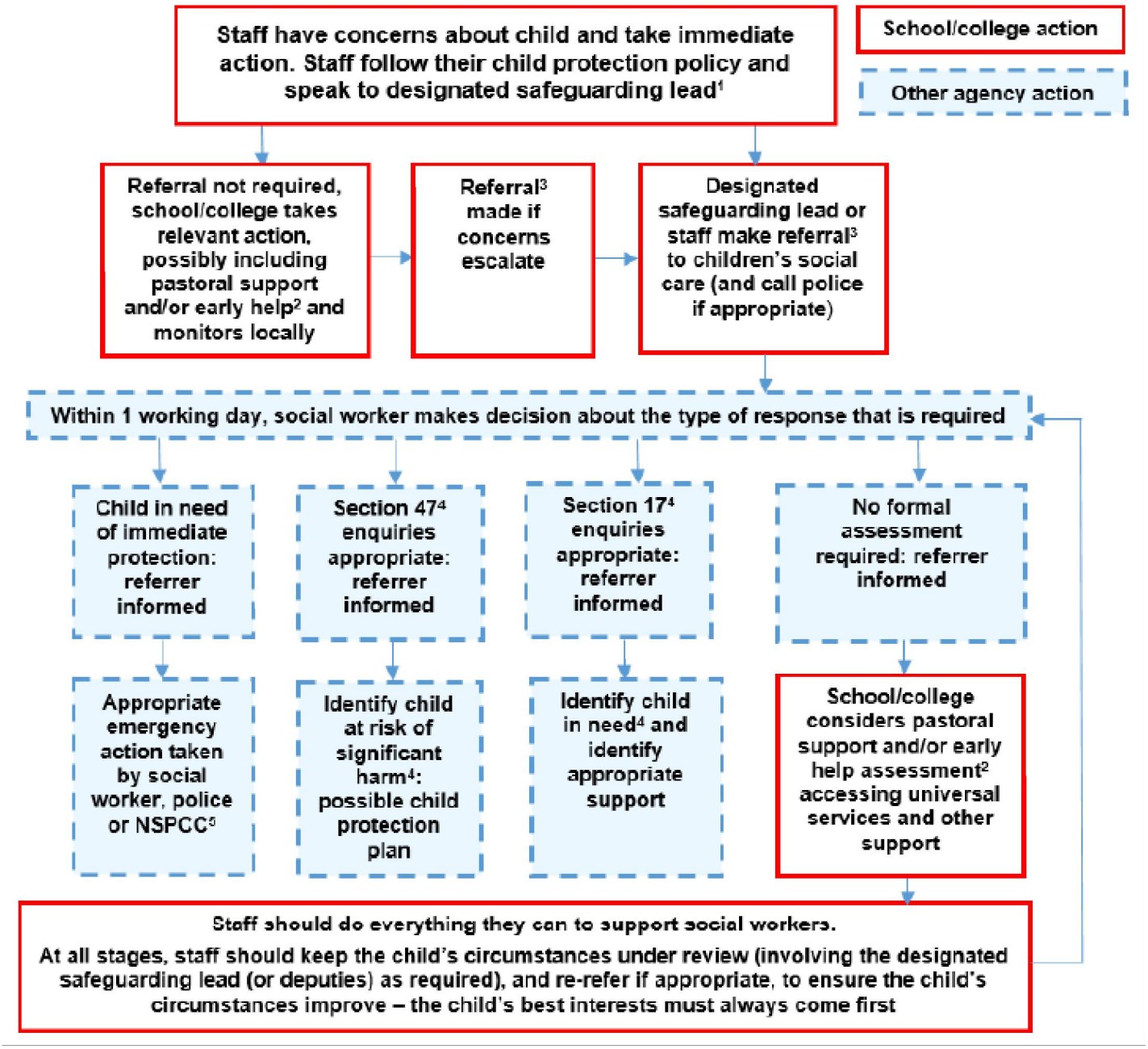
Police: 101 or 999 if immediate risk of harm

13. Useful Links

National Links and Resources for Settings, Learners and Parents/carers

- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Internet Watch Foundation (IWF): www.iwf.org.uk
- UK Council for Internet Safety (UKCIS): www.gov.uk/government/organisations/uk-council-for-internet-safety
- UK Safer Internet Centre: www.saferinternet.org.uk
  - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
  - Report Harmful Content: https://reportharmfulcontent.com/
- 360 Safe Self-Review tool for schools: www.360safe.org.uk
- Childnet: www.childnet.com
  - Step Up Speak Up – Online Sexual Harassment Guidance: www.childnet.com/resources/step-up-speak-up/guidance-and-training-for-schools-and-professionals
  - Cyberbullying Guidance: www.childnet.com/resources/cyberbullying-guidance-for-schools
- Internet Matters: www.internetmatters.org
- Parent Zone: https://parentzone.org.uk
- Parent Info: https://parentinfo.org
- NSPCC: www.nspcc.org.uk/onlinonline safety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- Action Fraud: https://www.actionfraud.police.uk/
- Get Safe Online: www.getsafeonline.org

14. Actions where there are concerns about a child



Source: Keeping children safe in education 2023.