MacIntyre School Online safety Policy

Policy Date: September 2023
Review Date: September 2024

I. Introduction

At Macintyre School we recognise that over the last years, there has been an increased dependence on Internet access and the use of new technologies for schooling and communicating with friends and family. Being connected online can bring huge benefits and opportunities for children such as:

- Ability to self-express
- Gain knowledge and access learning tools
- Communicate with friends
- Bring people together

However along with these benefits there are significant risks. The internet is a dangerous place to explore if the right advice and guidance is not provided.

Staff who are confident and well trained in online safety can help children and young people enjoy the online world and get the most out of it whilst also remaining safe and aware of the various online harms and dangers they may encounter.

Macintyre School adopts a comprehensive whole-school approach to ensure the safety and well-being of our students, both in the online and offline worlds. Our school is dedicated to creating a culture of safety that encompasses all aspects of our students' lives, recognizing the unique challenges they face due to their severe learning difficulties and additional complex needs. We are committed to providing a secure and inclusive learning environment where students can thrive, explore, and learn safely.

Please Note

- This policy must be read together with the safeguarding policy.

Our intentions are grounded in the following principles:

1. Creating a Culture of Safety: Our primary objective is to foster a culture where safety, both online and offline, is paramount. This culture extends across our entire school community, ensuring that every student feels protected and supported in their educational journey.

2. Proactive Engagement: We proactively engage pupils, staff, parents, and carers in the pursuit of online safety. Collaboration and communication are at the core of our approach, promoting a shared responsibility for the safety of our students.

3. Regular Review: We are committed to regularly reviewing and maintaining our online safety principles. In a rapidly evolving digital landscape, we recognize the importance of staying up-to-date and responsive to emerging risks.

4. Embedding Principles: Our approach involves embedding online safety principles into the fabric of our educational practices. We believe that these principles should become an integral part of how we teach, interact, and learn, ensuring that they are not just guidelines but lived values.

5. Modelling Principles: As an educational institution, we understand the power of modelling behaviour. We strive to model online safety principles for our students, staff, and parents, setting an example of responsible and secure online behaviour.

6. Systematic teaching: Ensuring a systematic way of teaching online safety skills across the curriculum and the whole school

All staff members share the responsibility for the safety of our students, encompassing both offline and online safety. To this end, all staff undergo annual safeguarding and online safety training, with the recognition that additional training may be necessary for specific situations. Class teachers and members of the Executive Leadership Team (ELT) actively communicate and provide staff with additional training opportunities throughout the year, ensuring that our staff members are equipped to meet the diverse needs of our students.

Online safety education is delivered incrementally and woven into the curriculum, taking into account the individual needs of each young person. Given the significant needs of our students, learning is based on repetition, reinforcing key concepts to promote comprehension and retention. This approach becomes particularly vital when pupils share specific concerns. Our students are systematically taught where and how to seek support, and they are encouraged to openly share any concerns, including those related to online safety. If a young person discloses a safeguarding issue, staff are obligated to follow the procedures outlined in the safeguarding policy and report to the Designated Safeguarding Lead (DSL) or Deputy Designated Safeguarding Officer (DSO).

In parallel, we empower our pupils to communicate their concerns with their parents and carers, emphasizing the importance of a collaborative approach to online safety. Parents and carers in the children's homes receive regular updates and information from the school regarding online safety, including guidance on reporting offered by organizations such as the NSPCC. This collaborative effort ensures that our students receive consistent support and guidance both at school and at home, promoting a holistic approach to online safety.

A. Purpose of the Policy

Our online safety policy is crafted to address the unique vulnerabilities and challenges faced by our students with Severe Learning Difficulties, other complex needs, as well as our autistic students. We firmly believe that by implementing tailored measures and guidelines, we can empower our students to explore and benefit from the digital world while ensuring their safety and protecting them from potential harm.

Our approach strives to strike a balance between providing access to new technologies and taking the utmost care to safeguard our students. Given their specific needs, we acknowledge that our students require additional support and supervision. Thus, it is our responsibility to establish a safe and controlled environment that facilitates their learning, growth, and engagement with technology.

Through this policy, we aim to lay out clear procedures and guidelines for all stakeholders to ensure the responsible and secure use of technology within our school community. By working collaboratively with our dedicated staff, parents, and caregivers, we aspire to create an environment that not only promotes online safety but also encourages digital literacy and nurtures essential skills for our students in an inclusive and protective manner.

This policy forms the bedrock of our commitment to establishing a secure digital space for our students, empowering them to harness the benefits of technology while mitigating potential risks. We are unwavering in our dedication to staying abreast of the latest advancements in online safety.

B. Scope of the Policy

Students: This policy applies to all students enrolled in Macintyre School, irrespective of their age or specific special educational needs. It is designed to ensure that every student is protected and receives tailored guidance in their online activities, taking into account their unique requirements and vulnerabilities.

Staff: The policy extends to encompass all staff members, including teachers, support staff, administrators, and any individuals employed or contracted by the school who have access to online resources or interact with students online. It is essential that our staff members are equipped with the knowledge and tools to ensure online safety.

Parents/Guardians: The scope of this policy also includes parents or guardians of our students. It underscores the importance of their active involvement, collaboration, and adherence to the policy's guidelines in supporting and promoting online safety both at home and in our residential homes.

School Premises: This policy governs online activities that take place on the school premises, including the use of school-provided devices and networks, ensuring a safe and controlled digital environment.

Off-Site Activities: It is crucial to extend our online safety measures to activities that occur off-site, such as during school trips, remote learning, or when students access school resources from external locations.

Online Platforms and Resources: This policy covers a range of digital platforms, online resources, and communication channels, including school-managed websites, teaching and learning management systems, social media platforms used for educational purposes, and any other online tools provided or recommended by the school.

Time Frames: The policy will remain in effect indefinitely, subject to at least annual reviews and updates. These reviews will be conducted to ensure that the policy remains current in the face of evolving technologies and emerging risks.

C. Legal and Regulatory Context

This policy has been crafted in strict accordance with various regulatory and legal documents, as well as established best practices, to ensure the utmost safety and well-being of our students at Macintyre School, taking into account their complex learning needs.

It is written with accordance with:

- **Education Act 1996 section 175**
- **The Children's Act 1989 and 2004**
- **Education (Independent School Standards) Regulations 2014:**
- **Keeping Children Safe in Education (KCSIE)**
- **General Data Protection Regulation (GDPR) now referred to as UK GDPR:**
- **Equality Act 2010**
- **Working together to Safeguard Children 2018 (update 2020)**
- **Prevent duty guidance: England and Wales**

– which

In addition to the above-mentioned legislation, Macintyre School also adheres to the following guidelines and frameworks:

1. Relationship and Sex Education:

- We align our online safety policy with guidelines related to relationship and sex education to ensure that our students receive age-appropriate and respectful information.

2. Teaching Online Safety in Schools:

- We incorporate guidelines on teaching online safety to ensure that our educational approach effectively addresses digital literacy and responsible online behaviour.

3. Education for a Connected World: :

- This resource serves as a valuable reference for embedding online safety principles into our curriculum and daily practices.

4. Sharing Nudes and Semi-Nudes:

- Advice for Education Settings: We follow best practices to address sensitive issues related to online behaviour and sharing explicit content.

5. Harmful Online Challenges:

- Our policy accounts for guidelines related to harmful online challenges, emphasizing prevention and awareness.

6. Education Inspection Handbook:

- We ensure that our online safety practices align with inspection guidelines, promoting a robust culture of safety.

7. Inspecting Safeguarding in Early Years, Education, and Skill Settings:

- We adhere to inspection guidelines to ensure that safeguarding, including online safety, is rigorously evaluated and maintained.

D. Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- logs of reported incidents
- Filtering and monitoring logs
- surveys/questionnaires of:
    - learners
    - parents and carers
    - staff.

II. Responsibilities

At Macintyre School, ensuring the online and offline safety of our students is a collective effort, involving a range of dedicated individuals and teams. Each party plays a vital role in upholding our commitment to safeguarding and promoting the welfare of our students, particularly those with Severe Learning Difficulties and additional complex needs.

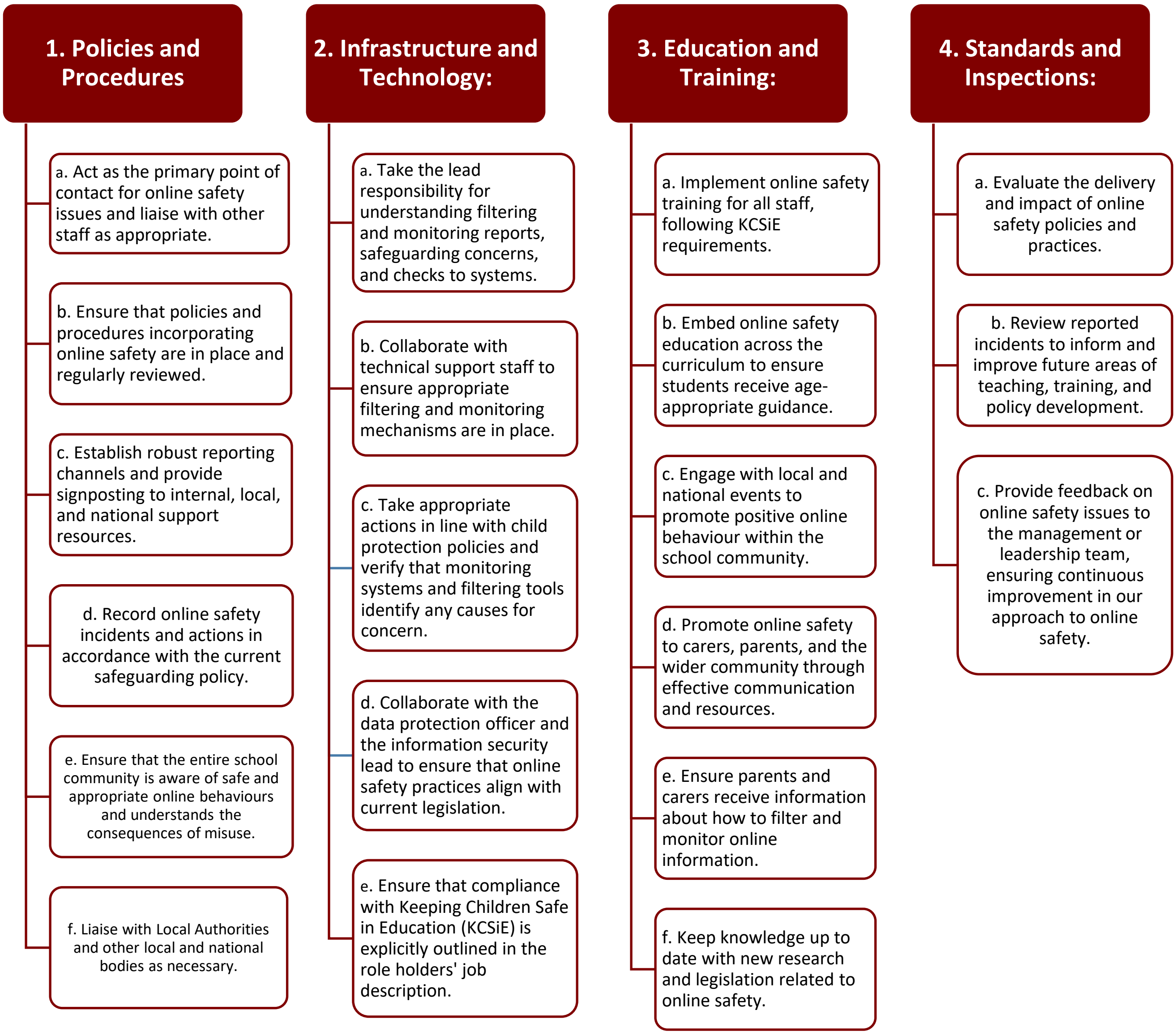
A. Designated Safeguarding Lead (DSL) and Deputy Designated Safeguarding Officers (DSOs)

Roles and Responsibilities of the DSL and DSOs

Keeping Children Safe in Education recognizes Online Safety as a safeguarding concern, and the DSL is entrusted with the responsibility of Online Safety. The DSL and DSOs take the lead in addressing online safety concerns and play a pivotal role in making initial decisions regarding appropriate responses to such concerns.

DSLs and DSOs are dedicated to maintaining and refreshing their knowledge and skills at regular intervals to stay abreast of changes in online risks and responses to online dangers. This commitment ensures they are well-equipped to provide effective support and guidance to our school community.

DSL Responsibilities in Relation to Online Safety



1. Policies and Procedures

a. Act as the primary point of contact for online safety issues and liaise with other staff as appropriate.

b. Ensure that policies and procedures incorporating online safety are in place and regularly reviewed.

c. Establish robust reporting channels and provide signposting to internal, local, and national support resources.

d. Record online safety incidents and actions in accordance with the current safeguarding policy.

e. Ensure that the entire school community is aware of safe and appropriate online behaviours and understands the consequences of misuse.

f. Liaise with Local Authorities and other local and national bodies as necessary.

2. Infrastructure and Technology:

a. Take the lead responsibility for understanding filtering and monitoring reports, safeguarding concerns, and checks to systems.

b. Collaborate with technical support staff to ensure appropriate filtering and monitoring mechanisms are in place.

c. Take appropriate actions in line with child protection policies and verify that monitoring systems and filtering tools identify any causes for concern.

d. Collaborate with the data protection officer and the information security lead to ensure that online safety practices align with current legislation.

e. Ensure that compliance with Keeping Children Safe in Education (KCSiE) is explicitly outlined in the role holders' job description.

3. Education and Training:

a. Implement online safety training for all staff, following KCSiE requirements.

b. Embed online safety education across the curriculum to ensure students receive age-appropriate guidance.

c. Engage with local and national events to promote positive online behaviour within the school community.

d. Promote online safety to carers, parents, and the wider community through effective communication and resources.

e. Ensure parents and carers receive information about how to filter and monitor online information.

f. Keep knowledge up to date with new research and legislation related to online safety.

4. Standards and Inspections:

a. Evaluate the delivery and impact of online safety policies and practices.

b. Review reported incidents to inform and improve future areas of teaching, training, and policy development.

c. Provide feedback on online safety issues to the management or leadership team, ensuring continuous improvement in our approach to online safety.

B. Local Advisory Board (Governing body)

The members of the Local Advisory Board (LAB) are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy

The members will receive regular information about online safety incidents and monitoring reports. A member of the governing body will take on the role of Safeguarding Governor which will include a responsibility for Online Safety. The Online Safety Governor role includes:

- **regular meetings with the Designated Safeguarding Lead / Online Safety Lead**
- **regularly receiving (collated and anonymised) reports of online safety incidents**
- **checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)**
- **Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually.** (The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible governor) - in-line with the DfE Filtering and Monitoring Standards
- **reporting to relevant *governors meetings***
- Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards

The Local Advisory Board will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

C. Roles and Responsibilities of teachers and support staff

While the DSL and DSOs bear specific responsibilities related to online safety, all staff members at Macintyre School share the overarching responsibility for the safety of our students, including online safety. Staff members are trained annually, with additional training provided as needed for specific situations. Class teachers and members of the Executive Leadership Team (ELT) actively communicate any additional training opportunities to staff throughout the year.

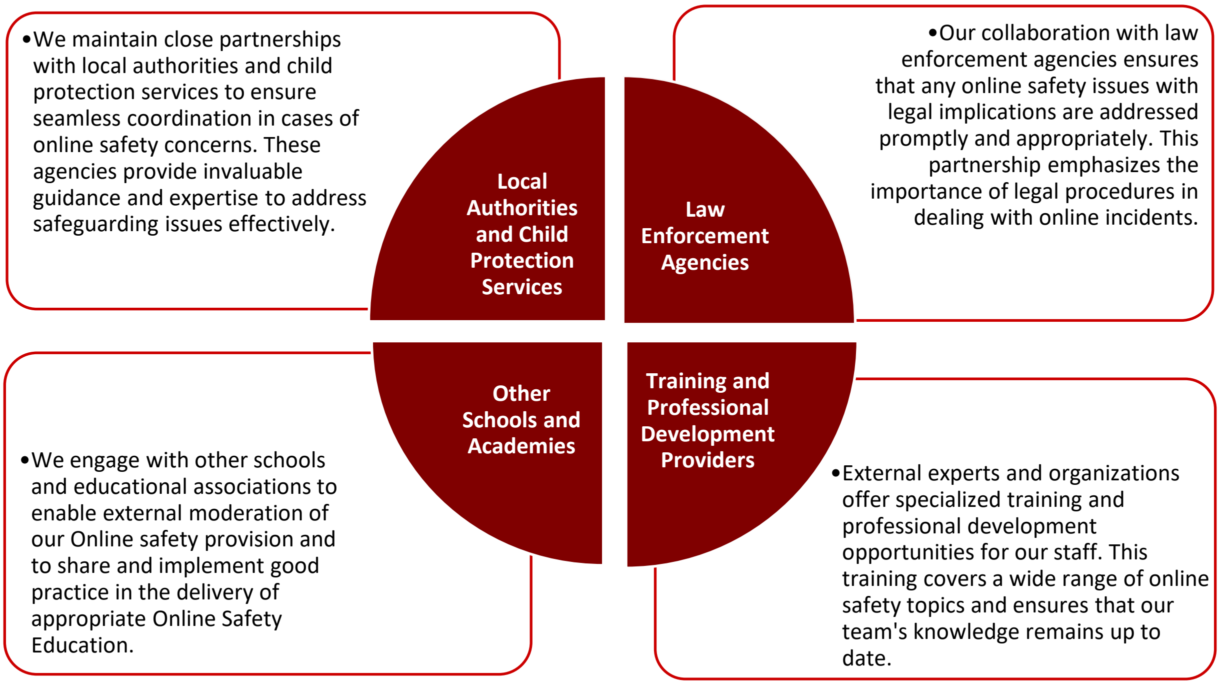
Online safety education is integrated into the curriculum, with lessons tailored to the individual needs of each student. This approach emphasizes repetition to ensure understanding, particularly when students express specific concerns. Staff members are responsible for teaching students how and where to seek support, and they must follow safeguarding procedures outlined in the school's policies if a student discloses a safeguarding issue.

Additionally, staff members play a critical role in promoting a culture of safety and responsibility, modelling appropriate online behaviour, and actively engaging with online safety initiatives and events to ensure a safe and inclusive online environment for our students.

D. Collaboration with external agencies or professionals

At Macintyre School, our dedication to ensuring the online safety and well-being of our students, including those with Severe Learning Difficulties and additional complex needs, extends beyond the confines of our school community. We recognize the invaluable contributions of external agencies and professionals in furthering our commitment to online safety. Our collaborative efforts with external partners are rooted in the collective responsibility to provide comprehensive support and resources for our students in the digital realm.

Types of Collaboration with External Agencies and Professionals:



Local Authorities and Child Protection Services

- We maintain close partnerships with local authorities and child protection services to ensure seamless coordination in cases of online safety concerns. These agencies provide invaluable guidance and expertise to address safeguarding issues effectively.

Law Enforcement Agencies

- Our collaboration with law enforcement agencies ensures that any online safety issues with legal implications are addressed promptly and appropriately. This partnership emphasizes the importance of legal procedures in dealing with online incidents.

Other Schools and Academies

- We engage with other schools and educational associations to enable external moderation of our Online safety provision and to share and implement good practice in the delivery of appropriate Online Safety Education.

Training and Professional Development Providers

- External experts and organizations offer specialized training and professional development opportunities for our staff. This training covers a wide range of online safety topics and ensures that our team's knowledge remains up to date.

Evaluation and Continuous Improvement:

We actively seek feedback from external agencies and professionals to assess the effectiveness of our online safety practices. Their insights and assessments contribute to our ongoing improvement efforts.

At Macintyre School, we view collaboration with external agencies and professionals as an integral part of our commitment to online safety. By working hand-in-hand with experts and organizations, we ensure that our students receive the comprehensive support and resources they need to navigate the digital world securely and confidently.

III. Risk Assessment

At Macintyre School, we recognize the unique vulnerabilities and challenges faced by our students with Severe Learning Difficulties (SLD), Autism (ASD), and other special needs in the digital world. Our approach to risk assessment takes into account the specific needs and circumstances of our students, ensuring their online safety remains a top priority. We understand that the accessibility of the digital world means that our learners are very likely to encounter a variety of risks and due to their additional needs and in many cases a lack of understanding of danger and risks, our young people are particularly vulnerable to these. Our staff understand that the learners that attend Macintyre School require high levels of support in order to stay safe from these risks.

A. Identifying potential risks and vulnerabilities specific to SEN students:

1. Online Relationships: Students with SLD, ASD, and special needs may struggle to distinguish between genuine and fake online relationships. They are at a higher risk of engaging with individuals who pose as friends or peers, making them susceptible to manipulation or exploitation.

2. Online Bullying or Cyberbullying: Due to their limited communication skills, non-verbal students are at increased risk of online bullying, often without the ability to report it. Cyberbullying can have severe emotional and psychological effects on these students.

3. Online Grooming: Groomers often target vulnerable children with special needs, knowing that they may have difficulty recognizing inappropriate or manipulative behaviour. Students with SLD and ASD may struggle to identify grooming attempts, putting them at greater risk.

4. Child Sexual Exploitation (CSE): CSE can occur online or start online and then transition to offline scenarios. Our students may find it challenging to comprehend or report such exploitation, making early detection and intervention crucial.

5. Sexting: Students may inadvertently engage in sexting, which is illegal for anyone under 18. Their limited understanding of consequences may lead to harmful situations. Immediate reporting and support are essential in such cases.

6. Livestreaming: Students may inadvertently access inappropriate content through livestreaming platforms. Their difficulty in discerning the risks associated with livestreaming makes education and supervision critical.

B. Assessing the impact of online activities on students' well-being:

While many of the young people at Macintyre School are not yet able to access the online world by themselves, it is important to reinforce healthy habits and behaviours at any levels of access. This can be done by staff modelling these behaviours online and offline, setting clear rules around use of technology or supporting access to technology in a healthy way.

When assessing the impact of online activities on student's wellbeing staff will take into consideration the following:

1. Online vs. Offline Identity:

- Our learners are very vulnerable and may be easily influenced by others. This can happen offline and online where they may adopt fake identities to fit in. This can have a huge impact on how our students see themselves and affect their self-esteem and wellbeing as well as their behaviour online and offline.

2. Social Media and Mental Health:

- There is a growing link between excessive social media use and mental health issues. Students, especially those with SLD and ASD, may be more susceptible to the negative effects of constant connectivity, including FOMO (fear of missing out) and exposure to cyberbullying.

3. Device Addiction:

- Students can develop device addiction, affecting their behaviour, interests, sleep patterns, school engagement, and physical health. This is particularly concerning for those with special needs and ASD that are prone to developing strong interest and hyper-focus on these more easily.

4. Online Challenges:

- Some students may participate in online challenges to feel accepted, but some challenges involve risks and sharing sensitive content. The fear of missing out can lead to excessive risk-taking behaviour.

5. Online Gambling:

- Although not of legal age to gamble, students may inadvertently access online gambling platforms through games. This exposure can have long-lasting effects on their attitudes towards money and risk.

6. Radicalization:

- Students are vulnerable to online radicalization, particularly given their difficulties in discerning extremist views. Our filtering systems help mitigate this risk, but awareness and vigilance remain essential.

7. Toxic Masculinity:

- Toxic masculinity views may influence some students online, affecting their behaviour and perceptions of gender roles. Students with SLD and ASD may be at risk of exposure to such content and subsequent changes in behaviour.

C. Considering reasonable adjustments for students with different needs:

At Macintyre School, our risk assessment strategies are designed to address the unique needs and vulnerabilities of our students, ensuring their online safety and well-being remain paramount. We are committed to continuous improvement, adapting our policies and practices to evolving challenges in the digital world.

1. Tailored Education: Online safety education is individualised and tailored to each learner's needs. The content is delivered in small, repetitive chunks across different areas of the curriculum in order to support generalisation of skills. Repetition is essential to reinforce learning, particularly for students with SLD and ASD.

2. Communication and Reporting: Students are systematically taught how and where to seek support and encouraged to openly share any concerns, including online safety issues. Staff must follow established procedures when students disclose safeguarding issues. We recognise that the majority of our pupils would struggle to share this type of information due to their additional needs. All staff are trained in online safety and communication strategies in order to support our learners at a level that is appropriate for them. Staff are also highly aware of the learner's vulnerabilities and are encouraged to closely supervise and report any concerns on their behalf.

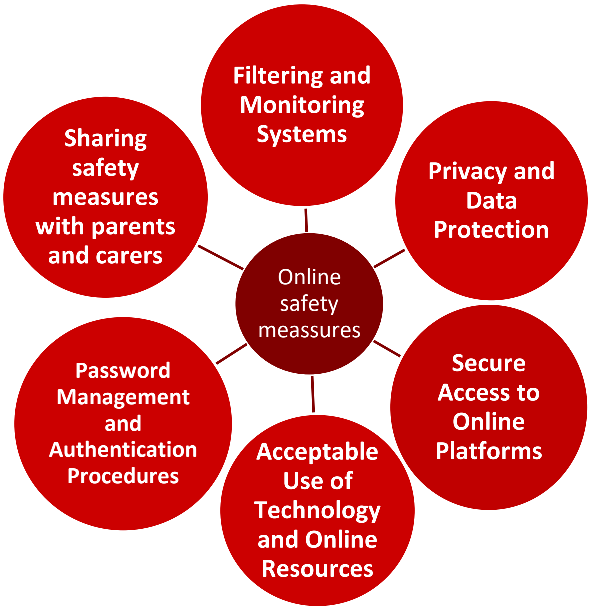
3. Parental Engagement: Parents receive regular information about online safety, including guidelines offered by organizations like the NSPCC. They are educated about filtering and monitoring options and encouraged to install parental controls on home devices.

4. Safe Environment: The staff at Macintyre School ensure the learning environment is as safe as possible. This is also true in the digital world. Staff support young people when accessing technology and closely monitor activities to ensure the content is relevant and appropriate. They are aware of the online platforms used and they are aware of any potential risks. Staff know how to request any changes to filtering and they can do this in a timely manner to ensure the safety of the learners at all times.

5. Cross curricular links and RSE Curriculum: Our curriculum includes coverage of topics such as misogyny and toxic masculinity, emphasizing respect and kindness both online and offline. Reflective discussions and teaching strategies are employed to address the effects of toxic masculinity.

IV. Online Safety Measures

At Macintyre School, we are dedicated to implementing comprehensive online safety measures to safeguard our students, especially those with special needs, from potential risks and vulnerabilities in the digital world. In our commitment to creating a secure online environment we focus our measures in the following areas:


Online safety meassures
Filtering and Monitoring Systems
Privacy and Data Protection
Secure Access to Online Platforms
Acceptable Use of Technology and Online Resources
Password Management and Authentication Procedures
Sharing safety measures with parents and carers

A. Filtering and Monitoring Systems:

1. Robust Filtering: We employ robust filtering systems to restrict access to inappropriate or harmful content, protecting students from exposure to potential online risks. These help to reduce exposure to possible online risks and provide a safe environment in which to learn.

2. Real-Time Monitoring: Continuous real-time monitoring of online activities within our network helps detect and prevent any suspicious or unsafe behaviour, ensuring a proactive approach to online safety.

3. Filtering and Monitoring Education: Whenever possible we educate students about the purpose of filtering and monitoring, ensuring they understand the protection these systems offer while fostering responsible online behaviour.

B. Acceptable Use of Technology and Online Resources:

1. Clear Guidelines: We provide clear guidelines to students' and staff on the acceptable use of technology (Annex A) and online resources, emphasizing responsible and ethical behaviour.

2. Educational Resources: Our curriculum includes content on digital citizenship and responsible online behaviour, empowering students to make informed choices while using technology as independently as possible.

3. Parental Involvement: We engage parents and carers, providing them with information on the school's acceptable use policies and encouraging them to reinforce these guidelines at home.

C. Privacy and Data Protection:

1. GDPR Compliance: Our school complies with the General Data Protection Regulation (GDPR), ensuring the protection of students' personal data and privacy rights.

2. Data Security: We have stringent data protection policies in place, safeguarding all personal data collected, processed, or stored by the school, including online data.

3. Data Breach Reporting: In the event of a data breach, we follow the necessary procedures, reporting incidents to the Information Commissioner's Office and taking appropriate actions to mitigate risks.

D. Secure Access to Online Platforms:

1. Authentication Procedures: We implement secure authentication procedures to ensure that only authorized users can access online platforms and resources.

2. Two-Factor Authentication (2FA): Where applicable, we encourage the use of two-factor authentication to add an extra layer of security to online accounts and platforms.

3. Regular Access Reviews: Access to online platforms is regularly reviewed and updated to align with the changing needs of students and staff while maintaining security.

E. Password Management and Authentication Procedures:

1. Strong Password: We promote the use of strong, unique passwords and advise students and staff on creating and maintaining secure passwords.

2. Regular Password Updates: Passwords are regularly updated to reduce the risk of unauthorized access to accounts and platforms.

3. Education on Authentication: We educate students on the importance of authentication and the risks associated with sharing passwords or personal information online. We also offer training to staff to ensure the safety of school data.

F. Sharing safety measures with parents and carers:

We share regular information on a range of online safety related topics with parents and carers. The aim of this information is to support them in better understanding the different online risks, especially those related to platforms that are regularly used by our students and to provide them with general guidelines to mitigate these risks. In addition we communicate any particular needs and added vulnerabilities of particular individuals and we support the families to implement strategies to support them with any additional needs related to online access and online safety whenever needed.

At Macintyre School, our online safety measures are designed to create a secure and supportive digital environment for our students. We remain committed to staying informed about evolving online risks and continuously improving our policies and practices to ensure the well-being of our students in the digital age.

V. Acceptable Use of Technologies, Internet, and Social Media

At Macintyre School, we prioritize the safe and responsible use of technology, the internet, and social media by our students and our staff. Our guidelines aim to educate our students and protect them from potential risks, ensuring a secure and positive online experience.

Staff follow the Acceptable Use of Technology and Online Resources Guidelines are familiar with the information provided in this section. All staff working with children and young adults at Macintyre School must support them to understand the students responsibilities described in Annex A.

A. Safe and Responsible Internet Use Guidelines:

1. Respectful Online Behaviour: We encourage students and staff to treat others online with kindness and respect, just as they would in face-to-face interactions.

2. Cyberbullying Awareness: Students are educated about the consequences of cyberbullying and are urged to report any instances immediately. We promote a culture of reporting to address online safety concerns.

3. Appropriate Content Sharing: We guide students on the responsible sharing of personal information and content online, emphasizing the importance of privacy and consent.

4. Critical Thinking: We foster critical thinking skills to help students evaluate online information critically, identify fake news, and make informed decisions while browsing the internet.

.

B. Age-Appropriate Content and Access Restrictions:

1. Content Restrictions: We implement age-appropriate content filters and access restrictions to prevent students from accessing harmful or inappropriate material.

2. Educational Access: Students are provided with access to online resources and educational content that aligns with their learning needs and age group.

C. Educating Students About Potential Risks and How to Report Concerns:

Educating learners on online safety and reporting methods across various curriculum areas such as 'My Independence,' 'My Communication,' 'My Problem Solving,' and 'My Wellbeing' is crucial. By seamlessly integrating these topics into the broader educational framework, we empower students with diverse learning needs to navigate the digital landscape confidently.

1. Risk Awareness: We educate students taking into account the complex special needs, about potential online risks, such as cyberbullying, online grooming, and inappropriate content.

2. Reporting Mechanisms: We teach students how to recognize online safety concerns and provide clear instructions on reporting such concerns to trusted adults, including school staff, parents, and carers.

D. Guidelines for Staff-Student Communication on Social Media:

Staff use of technologies:

- **1. Professionalism on Social Media:** Staff members are reminded to maintain professionalism on their personal social media accounts, refraining from discussing school-related matters, students, colleagues, or sensitive topics. All staff must read and agree to the terms and guidelines listed in Annex C, “SOCIAL MEDIA POSTS AND INTERNET ACTIVITY GUIDELINES”
- **2. Privacy Settings:** Staff should use privacy settings to control who can view their posts, keeping personal information private. They are encouraged to review and remove any offensive or inappropriate content from their profiles.
- **3. No Contact with Pupils or Their Families:** Staff must not accept or send friend requests to pupils or their family members on social media. They should promptly report any such requests or incidents to the Professional's Online Safety Helpline (POSH).

Staff Communication with Pupils and Families:

- **1. Official Communication Channels:** Staff must utilize official school communication channels, such as school email accounts and the Evidence for Learning platform, for communication with pupils and families.
- **2. Secure Email:** When sending confidential information, staff should always use secure email function and encryption for added protection.
- **3. Personal Accounts:** Staff should never use their personal social media accounts to contact pupils or their families, and they should avoid personal contact with former pupils or their families.

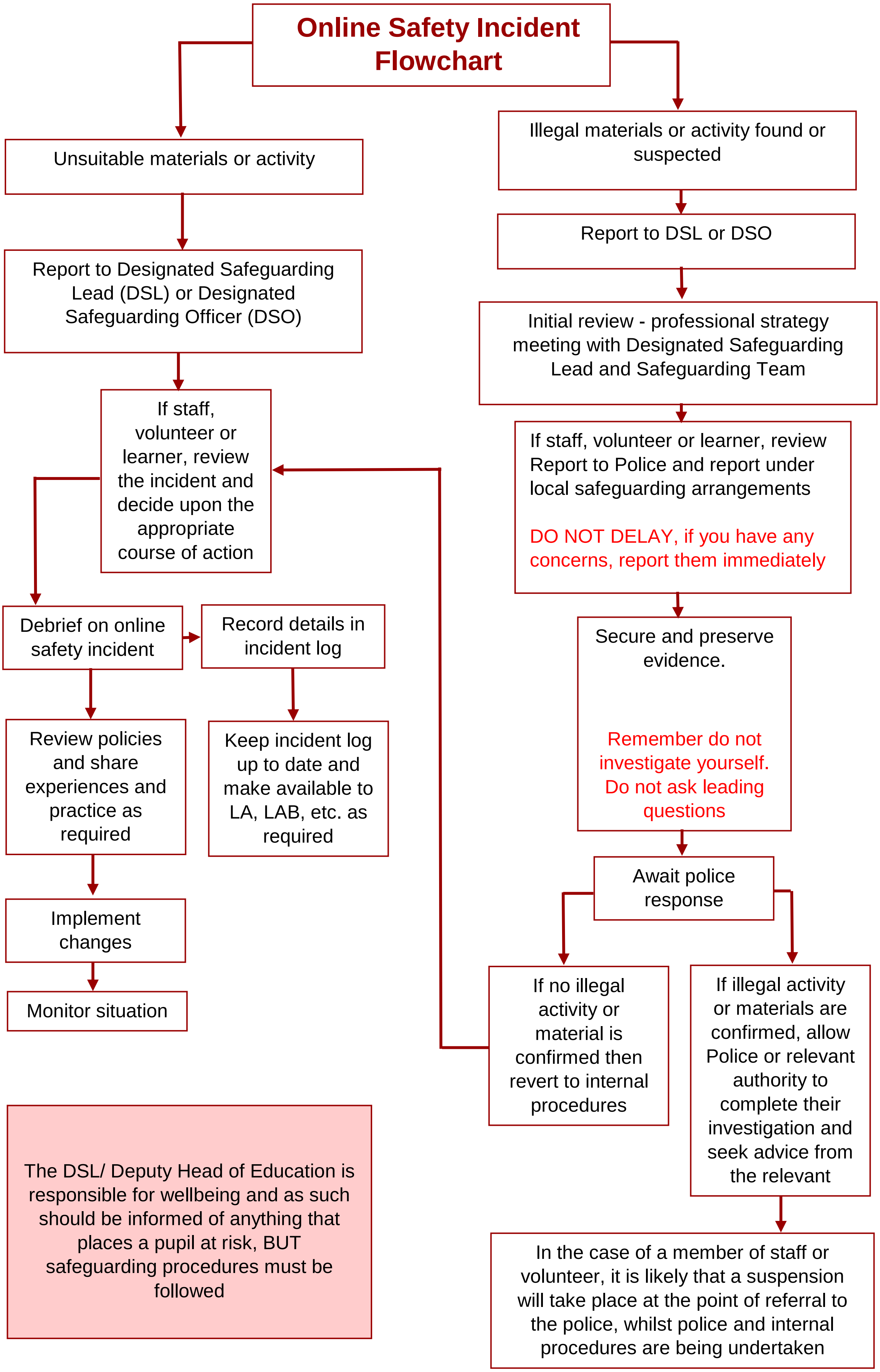
At Macintyre School, we are committed to fostering a safe and respectful online environment for our students, enhancing their digital literacy, and ensuring their well-being in the digital age. By adhering to these guidelines, we aim to create a positive online experience for all our students while minimizing potential risks.

VI. Reporting and Responding to Online Safety incidents

Macintyre School takes all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies. (Refer to Safeguarding policy)
- all members of the school community are made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm **(see flowchart and user actions chart below),** the incident must be escalated through the agreed school safeguarding procedures, this may include
    - Non-consensual images
    - Self-generated images
    - Terrorism/extremism
    - Hate crime/ Abuse
    - Fraud and extortion
    - Harassment/stalking
    - Child Sexual Abuse Material (CSAM)
    - Child Sexual Exploitation Grooming
    - Extreme Pornography
    - Sale of illegal materials/substances
    - Cyber or hacking
    - Copyright theft or piracy
- any concern about staff misuse will be reported to the Head of Education, unless the concern involves the Head of Education, in which case the complaint is referred to the Local Advisory Board
- where there is no suspected illegal activity, devices may be checked using the following procedures:
    - one or more senior members of will be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
    - conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
    - record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form
    - once this has been completed and investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
        - internal response or discipline procedures
        - involvement by local authority
        - police involvement and/or action
- Incidents should be logged in the safeguarding log
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police
- when relevant, those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
    - Safeguarding leads to discuss in safeguarding meetings
    - staff, through regular briefings
    - learners, through assemblies/lessons
    - parents/carers, through newsletters, school social media, website
    - governors, through regular safeguarding updates
    - local authority/external agencies, as relevant

Online Safety Incident Flowchart



Unsuitable materials or activity

Report to Designated Safeguarding Lead (DSL) or Designated Safeguarding Officer (DSO)

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

Debrief on online safety incident

Record details in incident log

Review policies and share experiences and practice as required

Keep incident log up to date and make available to LA, LAB, etc. as required

Implement changes

Monitor situation

Illegal materials or activity found or suspected

Report to DSL or DSO

Initial review - professional strategy meeting with Designated Safeguarding Lead and Safeguarding Team

If staff, volunteer or learner, review Report to Police and report under local safeguarding arrangements

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

Secure and preserve evidence.

Remember do not investigate yourself. Do not ask leading questions

Await police response

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

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

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

The DSL/ Deputy Head of Education is responsible for wellbeing and as such should be informed of anything that places a pupil at risk, BUT safeguarding procedures must be followed

VI. Impact

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, learners; parents/carers and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors
- parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
- the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

Acceptable Use of Technology and Online Resources Guidelines (Annex A)

For Students:

1. Respect Others: Treat fellow students, teachers, and online users with kindness and respect. Never use technology to hurt, tease, or bully others.

2. Privacy: Do not share personal information online, such as your full name, address, phone number, or school name, without permission from a trusted adult.

3. Cybersecurity: Keep your login information, passwords, and any school-related accounts safe and private. Report any suspicious activity or messages to a teacher or adult.

4. Appropriate Content: Only access and share content that is educational and appropriate for school. If you're unsure, ask a teacher or trusted adult for guidance.

5. Ask for Help: If you encounter something online that confuses you or makes you uncomfortable, ask a teacher or trusted adult for help and guidance.

For Staff:

1. Supervision: Always supervise students when they are using technology and online resources. Provide clear guidelines and monitor their online activities.

2. Educate Students: Teach students about responsible and ethical technology use, including online safety, privacy, and respecting others.

3. Digital Literacy: Help students develop digital literacy skills, including understanding online sources, distinguishing reliable information from unreliable sources, and using technology effectively for learning.

4. Safe Online Environment: Create and maintain a safe online environment by promoting positive online behaviour and promptly addressing any instances of cyberbullying, harassment, or inappropriate content.

5. Access Controls: Make sure you use devices that use appropriate content filters and access controls to ensure that students can only access age-appropriate and school-approved resources. Do not use your own devices to show any content to young people as they may not have these.

6. Reporting and Response: Encourage students to report any inappropriate or concerning online behaviour. Have a clear protocol for responding to such reports and supporting students as needed.

7. Professionalism: Model responsible and ethical technology use to students. Use technology for educational purposes. Do not use new technologies for personal use when working with children and young adults unless is previously cleared with a manager.

8. Personal phones and other personal devices: All personal devices must be locked away when working with young people.

9. Continual Learning: Stay updated on technology trends and online safety best practices to provide the best guidance and support to students.

10. School devices used at home: School devices may need to be used to work at home if previously agreed, however the main use should be for accessing work related content. Be very mindful on what type of content you access as this is monitored. Never leave any school devices in unlocked or unattended locations.

For Both Students and Staff:

1. Communication: Maintain open and honest communication between staff, students, and parents regarding technology use and online safety.

2. Consent: Always seek and obtain proper consent before sharing any information, photos, or videos of students or staff online.

3. Regular Review: Periodically review and update these guidelines to ensure they remain relevant and effective in promoting responsible and ethical technology use.

Annex B

What to do when you see online abuse or inappropriate content

If you or your student come across something upsetting or concerning online. It is important that you feel confident about what to do if you do see something inappropriate online, or if your students tells you they've seen something. If concerned, you must always inform the DSL or a DSO using the regular safeguarding procedure. If needed, they may support you to report your concern by following the advice below.

Inappropriate contact from an adult	The Child Exploitation and Online Protection Command (CEOP) helps keep children safe from online grooming. CEOP is part of the police service and sits within the National Crime Agency. If you suspect an adult is communicating with a child inappropriately, or a child is being sexually abused online, you should report this to the CEOP. CEOP have a reporting page, as well as resources on their website for support with online child sexual abuse, and their site, Thinkuknow, provides information for children.
Nude images of children online	Sometimes, innocent searches can lead to not so innocent results. If you come across an indecent image of a child online, it is important to report this to the Internet Watch Foundation (IWF) so that they can review this content. Some nude images of children are classed as Child Sexual Abuse material. If it is illegal, the IWF will take steps to take this down and safeguard the child. The IWF's reporting portal can be used anonymously. If nude images of your child are shared online: If you know a young person who has had a sexual image or video of themselves shared online, and they're under 18, talk to them about Childline and the Internet Watch Foundation's Report Remove tool. It allows young people to discreetly report a nude image or video shared online, to see if it's possible to get it taken down. Young people can get support from Childline throughout the process. They just need to follow 3 steps: 1. Follow the instructions to prove their age. They may need ID for this. 2. Log into or create a Childline account so they can receive updates on their report.

	3. Report and remove: the IWF will review it and work to have it removed if it breaks the law. You can also see advice on how to support a child dealing with pressure to share nudes on our sexting page, and read information for parents about Report Remove.
Online gaming abuse	Online games are a great way for children to have fun and connect with friends, though sometimes gaming can go wrong and abuse can occur on these platforms. If you have concerns that a child is being groomed through an online game, you can report this to CEOP. If you are concerned about other types of abuse via online gaming, Cybersmile has a Gaming Help Centre, where you can find: • In-game reporting systems for some of the most popular games • Reporting systems of game platforms, outside of the game • Cybersmile's Global Support Service – this can be used to get advice on online gaming related issues Remember, if you're worried that a child is being abused, or at risk of being abused, you should contact the NSPCC helpline for advice, as the Global Support Service can have a long waiting list. If you have concerns that the content in a game is inappropriate for its PEGI rating, you can raise this with the Video Standards Council by contacting them here.
Online hate content	Online content which incites hatred should be reported to True Vision at report-it.org.uk which covers the grounds of race, religion, disability, sexual orientation or gender. This content should also be reported directly to the platform on which it appears.
Other types of online abuse	For other forms of online abuse and harmful content, such as bullying, threats, or self-harm and suicide content, you can report this directly to the platform where the abuse took place. This also includes content designed to impersonate someone else (e.g. creating a fake account pretending to be someone else). It is a good idea to take screenshots so you can share this with the platform if needed. Report Harmful Content can walk you through the reporting process for many popular sites.

	If the content has remained online or the platform has not taken appropriate action, you can report this to Report Harmful Content. They will look into the issue and ensure the correct processes have been followed, and advise you on what steps you can take next.
Inappropriate add or videos	If you see an inappropriate online advert, you can report this to the Advertising Standards Agency (ASA). If you see online television content that you think is inappropriate, you can report this to Ofcom.
Online terror content	You can report terrorism-related content to the police's Counter Terrorism Internet Referral Unit at gov.uk/report-terrorism. You can get further information on what to do if you come across terrorism-related content, or have suspicions about a person relating to terrorism, at the Action Counters Terrorism site.
Any other concerns	If you're worried about something a child or young person may have experienced online, you can contact the NSPCC Helpline for free support and advice. Children can contact Childline any time to get support themselves. Childline's Calm zone is also packed with tools and activities to help your child de-stress and discover news techniques that can support them when they're feeling down. Young people can also talk about their worries with others on the Childline message boards.

Annex C

SOCIAL MEDIA POSTS AND INTERNET ACTIVITY GUIDELINES

Employees

• Must not use Email, the internet, social media and related types of electronic communication and information, and electronic equipment in a way which could constitute a breach of any school policies including those contained in the Staff Code of Conduct

• Must not post anything that may offend, insult or humiliate others, particularly on the basis of protected characteristics including: age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, and sex

• Must not post anything that could be reasonably interpreted as threatening, intimidating or abusive. Offensive posts or messages may be construed as cyber- bullying

• Must not post disparaging or derogatory remarks about Macintyre or Macintyre School or its Governors, staff, volunteers, pupils or parents

• Should always represent their own views and must not allude to other people's personal views in Emails or internet posts. Employees must make it clear that any opinions expressed are theirs alone and do not represent the views of their School or of the Foundation

• Must ensure that they are not committing plagiarism and/or breach of copyright when sending, receiving or using, without appropriate permission and acknowledgement, the intellectual property belonging to another

• Must not use photographic material captured on a mobile telephone or similar equipment with integrated camera in a manner which may constitute bullying, harassment or intimidation of others, including passing on or showing such images to others or posting the image/s on social media or similar electronic media.

Possession of such imagery may in itself constitute serious misconduct and may result in disciplinary action.

• Are responsible for reading, knowing and complying with the terms of service of any internet or social media sites that he/she may use. Employees should not open any social media account under a pseudonym.

They should familiarise themselves with the privacy settings of any social media used and ensure that public access is restricted. If an employee is not clear about how to restrict access, they should regard all their information as publicly available and behave accordingly

• Should consider whether the contents of any email would be more appropriate in a private message. While strict privacy controls may be in place, information could still be shared by others. It is always sensible to consider that any information posted may not remain private. Employees should protect their own privacy and that of others by omitting personal information from internet posts such as names, Email addresses, home or work addresses, phone numbers or other personal information

• Should have regard to the fact that Email messages can be retrieved even once deleted and may have to be disclosed in the event of subsequent litigation by Macintyre when sent or received on the School’s IT facilities and equipment

• Employees should also be circumspect in their communications with pupils so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming. They should not give their personal contact details to pupils including Email, home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/carers