Keeping Children Safe in Education 2020

Working Together to Safeguard Children 2018

EYFS - Ofsted Framework

Kent and Medway Child protection

Online Safety

Policy and procedures

Cobtree Playschool for Special Children

Maidstone Mencap Charitable Trust Ltd

This policy is to read alongside but not limited to: Child Protection, Acceptable Use Policies, Policies and procedures for the use of Social Media, Mobile Phones, and Digital Cameras.

Key Details

Designated Safeguarding Lead:

Liane Morris
Child and Young Person Welfare Manager

Board of Trustees for Maidstone Mencap Charitable Trust Ltd:

James Burrows (Treasurer)
Lead responsibility for Online Safety, and System Management

Reviewed: March 2021

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.

Contents

Online Safety Policy

1. Policy Aims

- This online safety policy has been written by Maidstone Mencap Charitable Trust Ltd, building on the Kent County Council (KCC) online safety policy template, with specialist advice and input as required.
- It takes into account the DfE statutory guidance "Keeping Children Safe in Education" 2020, Early Years and Foundation Stage 2017 and the Kent Safeguarding Children Board procedures.

- The purpose of Maidstone Mencap online safety policy is to:
    - Safeguard and protect all members of Maidstone Mencap community online.
    - Identify approaches to educate and raise awareness of online safety throughout the 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 use when responding to online safety concerns.

- Maidstone Mencap 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.

2. Policy Scope

- Maidstone Mencap believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all children, young people and staff are protected from potential harm online.
- Maidstone Mencap identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- Maidstone Mencap believes that children and young people should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- This policy applies to all staff including the board of trustees, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the charity (collectively referred to as 'staff 'in this policy) as well as children, young people and parents/carers.
- This policy applies to all access to the internet and use of technology, including personal devices, or where children, young people, staff or other individuals have been provided with Maidstone Mencap issued devices for use off-site, such as a work laptops, tablets or mobile phones.

2.2 Links with other policies and practices

- This policy links with a number of other policies, practices and action plans including:
    - Anti-bullying policy
    - Acceptable Use Policies (AUP) and the Code of conduct
    - Behaviour and discipline policy
    - Child protection policy
    - Confidentiality policy
    - Data security
    - Image use policy

3. Mobile phone and social media policies Monitoring and Review

- Maidstone Mencap will review this policy at least annually
    - The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure
- We will ensure that we 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 board of trustees for Maidstone Mencap will be informed of online safety concerns, as appropriate.
- The named lead for the board of trustees and the DSL for safeguarding will report on a regular basis to the governing body on online safety incidents, including outcomes.
- Any issues identified will be incorporated into Maidstone Mencap's action planning.

4. Roles and Responsibilities

- The charity has appointed Liane Morris, as Designated Safeguarding Lead to be the online safety lead, with system management by James Burrows (treasurer@maidstonemencap.org)
- Maidstone Mencap recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

4.1 The leadership and management team will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a Code of conduct and/or an AUP, which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place.
- Work with technical staff to monitor the safety and security of school systems and networks.
- Ensure that online safety is embedded within a progressive curriculum, which enables all children and young people to develop an age-appropriate understanding of online safety.
- Support the Designated Safeguarding Lead by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the Maidstone Mencap community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology. Audit and evaluate online safety practice to identify strengths and areas for improvement.

4.2 The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the Maidstone Mencap community, as appropriate.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.

- 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 charities safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate, to the management team and Board of trustees
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually).

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

- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and AUPs.
- Take responsibility for the security of the charities systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the school's safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

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

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures *(including password policies and encryption)* to ensure that the charities IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that the charities filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Report any filtering breaches to the DSL and leadership team, as well as, the charities Internet Service Provider or other services, as appropriate.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL, in accordance with the school's safeguarding procedures.

4.5 It is the responsibility of children and young people (at a level that is appropriate to their individual age, ability and vulnerabilities) to:

- Engage in age appropriate online safety education opportunities.

- Contribute to the development of online safety policies.
- Read and adhere to the charities AUPs.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

4.6 It is the responsibility of parents and carers to:

- Read the charities AUPs and encourage their children to adhere to them.
- Support Maidstone Mencap in their online safety approaches by discussing online safety issues with their children and reinforce appropriate, safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the settings home-school agreement and/or AUPs. Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from Maidstone Mencap, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the school online safety policies.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

5. Education and Engagement Approaches

5.1 Education and engagement with pupils

- Maidstone Mencap will establish and embed an online safety awareness throughout the whole charity and its service users, to raise awareness and promote safe and responsible internet use amongst the children and young people by:
    - Ensuring education regarding safe and responsible use precedes internet access.
    - Reinforcing online safety messages whenever technology or the internet is in use.
    - Supporting children and young people in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
    - Supporting children and young people to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- Maidstone Mencap will support children and young people to read and understand the AUP in a way which suits their age and ability by:
    - Displaying acceptable use posters in all rooms with internet access.
    - Informing children that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
    - Rewarding positive use of technology
    - Using support, such as external visitors, where appropriate, to complement and support the charities internal online safety approaches.

5.1.1 Vulnerable Pupils

- Maidstone Mencap is aware that are service users are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- Maidstone Mencap will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils.
- Maidstone Mencap will seek input from specialist staff as appropriate, including the SENCO, Child in Care Lead.

5.2 Training and engagement with staff

Maidstone Mencap Charitable Trust ltd will:

- Provide and discuss the online safety policy with all members of staff as part of induction.
    - This will cover the potential risks posed to pupils (Content, Contact and Conduct) as well as our professional practice expectations.
- Make staff aware that systems are monitored, and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with school's policies when accessing the charities systems and devices.
- Make staff aware that their online conduct out of the setting, including personal use of social media, could have an impact on their professional role and reputation within the setting
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting children, young people, colleagues or other members of the Maidstone Mencap community.

5.3 Awareness and engagement with parents and carers

- Maidstone Mencap recognises that parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies.
- The charity will build a partnership approach to online safety with parents and carers by:
    - Providing information highlighting online safety at events such as parent consultations, transition events, fundraising events.
    - Drawing their attention to Maidstone Mencap online safety policy and expectations in newsletters, letters, and on our website.
    - Requesting that they read online safety information as part of joining our Maidstone Mencap community for example, within our home agreement.
    - Requiring them to read Maidstone Mencap AUP and discuss its implications with their children.

6. Reducing Online Risks

- Maidstone Mencap 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 use in our setting is permitted.
    - Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.

    - Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via computer or device whilst in our setting or environment.
- All members of the Maidstone Mencap community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in our AUP.

Safer Use of Technology

7.1

- Maidstone Mencap has access to a wide range of technology. This includes
    - Computers, laptops and other digital devices
    - Internet which may include search engines and educational websites
    - Email
    - Games consoles and other games based technologies
    - Digital cameras,
- All Maidstone Mencap owned devices will be used in accordance with the charities AUP and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools and apps fully before use in our setting or recommending for use at home.
- Maidstone Mencap will use age appropriate search tools, following an informed risk assessment, to identify which tool best suits the needs of our community.
- Maidstone Mencap will ensure that the use of internet-derived materials, by staff children and young people, complies with copyright law and acknowledge the source of information.
- Supervision of children and young people will be appropriate to their age and ability.
    - **Early Years Foundation Stage: Cobtree playschool**
        - access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the child's' age and ability.
    - **Juniors, Youth club and holiday club:**
        - Children and young people will be appropriately supervised when using technology, according to their ability and understanding.
        - Maidstone Mencap will balance children's ability to take part in age appropriate peer activities online, with the need to detect and prevent abuse, bullying or unsafe practice by children in accordance with the national minimum standards (NMS).

7.2 Managing Internet Access

- Maidstone Mencap will maintain a written record of users who are granted access to the charities devices and systems.
- All staff, and visitors will read and sign an AUP before being given access to a computer system, IT resources or internet

7.3 Filtering and Monitoring

7.3.1 Decision Making

- Maidstone Mencap trustees and management will have ensured that the settings have age and ability appropriate filtering and monitoring in place, to limit children's exposure to online risks.
- Maidstone Mencap are aware of the need to prevent "over blocking", as that may unreasonably restrict what children can be taught, with regards to online activities and safeguarding.
- Maidstone Mencap's decision regarding filtering and monitoring will be informed by a risk assessment, taking into account our settings specific needs and circumstances.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy will be 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.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard children and young people; effective management and regular education about safe and responsible use is essential.

7.3.2 Filtering (**filtering systems have as yet not been implemented at Maidstone Mencap and will be monitored as the need arises)**

- Maidstone Mencap will use an educational broadband connectivity as appropriate through a registered internet provider to support filtering systems which will blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
    - as appropriate Maidstone Mencap will use a filtering system that blocks all sites on the Internet Watch Foundation (IWF) list.
- Maidstone Mencap will work with the internet provider to ensure to ensure that our filtering policy is continually reviewed.

Dealing with Filtering breaches

- Maidstone Mencap will have a clear procedure for reporting filtering breaches.
    - If children or young people discover unsuitable sites, they will be required to turn off monitor/screen and report the concern immediate to a member of staff.
    - The member of staff will report the concern (including the URL of the site if possible) to the Designated Safeguarding Lead and/or technical staff.
    - The breach will be recorded and escalated as appropriate.
    - Parents/carers will be informed of filtering breaches involving their child.
- Any material that Maidstone Mencap believes is illegal will be reported immediately to the appropriate agencies, such as: IWF, Kent Police or CEOP.

7.3.4 Monitoring

- Maidstone Mencap will appropriately monitor internet use on all l owned or provided internet enabled devices. This is achieved by: supervision, physical monitoring and managing interact and web access.
- Maidstone Mencap will follow safeguarding reporting procedures for responding to concerns identified via monitoring approaches:
- All users will be informed that use of systems on Maidstone Mencap owned devices can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

7.4 Managing Personal Data Online

- Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations (GDPR) and Data Protection legislation.
    - Full information can be found in the information privacy policy.

7.5 Security and Management of Information Systems

- Maidstone Mencap takes 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.
    - Regularly checking files held on the charities network,
    - The appropriate use of user logins and passwords to access systems.
    - All users are expected to log off or lock their screens/devices if systems are unattended.

7.5.1 Password policy

- All members of staff will have their own unique username and private passwords to access Maidstone Mencap systems; members of staff are responsible for keeping their password private.
- We require all users to:
    - set strong passwords for access into our system.
    - Always keep their password private; users must not share it with others or leave it where others can find it.
    - Not to login as another user at any time.

7.6 Managing the Safety of our Website

- Maidstone Mencap will ensure that information posted on our website meets and complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff or children and young people's personal information will not be published on our website; the contact details on the website will be the Charities work related email and telephone numbers.
- The administrator account for Maidstone Mencap's website is secured with an appropriately strong password.
- Maidstone Mencap will post appropriate information about safeguarding, including online safety, on our website for members of the community.

7.7 Publishing Images and Videos Online

- Maidstone Mencap will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to): The Image use policy, Data security, AUPs, Codes of conduct, Social media and Use of personal devices and mobile phones.
- Written consent will be sought before any image is shared on our website or social media accounts.

7.8 Managing Email

- Access to Maidstone Mencap's email systems will always take place in accordance with Data protection legislation and in line with other policies, including: Confidentiality, AUPs and Code of conduct.
    - 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.
    - Maidstone Mencap email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the Maidstone Mencap community will immediately tell DSL if they receive offensive communication, and this will be recorded in the safeguarding files/records.

7.8.1 Staff

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

7.8.2 Children and young people.

Maidstone Mencap will not issue any email address for use by any of our service users.

7.9 Educational use of Videoconferencing and/or Webcams.

We currently do not have access to any resources that would enable these.

7.9.1 Users

7.9.2 Content

7.10 Management of Learning Platforms

Maidstone Mencap does not use an official learning platform

7.11 Management of Applications which Record Children's Progress

- Cobtree playschool uses a "unique progress format", to monitor pupils progress and share appropriate information with parents and carers. These are not an online tool accessible to parents

- The manager is ultimately responsible for the security of any data or images held of children. As such, they will ensure that tracking systems are appropriately risk assessed prior to use, and that they are used in accordance with GDPR and data protection legislation
- To safeguard data:
    - Only Maidstone Mencap issued devices will be used for apps that record and store children's personal details, attainment or photographs. Personal staff mobile phones or devices will not be used to access or upload content.
    - 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.

8. Social Media

8.1 Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of Maidstone Mencap's 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 Maidstone Mencap's community are expected to engage in social media in a positive, safe and responsible manner, at all times.
    - All members of Maidstone Mencap's community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
    - The use of social media during working hours for personal use **is not** permitted.
    - Inappropriate or excessive use of social media during work hours or whilst using Maidstone Mencap devices may result in disciplinary or legal action and/or removal of internet facilities.
- Concerns regarding the online conduct of any member of Maidstone Mencap's community on social media, should be reported to the DSL and will 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 networking, social media and personal publishing 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 the Code of conduct within the AUP.

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 charity. Civil, legal or disciplinary action may be taken if they 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 sites. 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 the privacy levels of their personal sites as strictly as they can.
    - Being aware of location sharing services.
    - Opting out of public listings on social networking sites.
    - Logging out of accounts after use.
    - Keeping passwords safe and confidential.
    - Ensuring staff do not represent their personal views as that Maidstone Mencap.
- Members of staff are encouraged not to identify themselves as employees of Maidstone Mencap on their personal social networking accounts. This is to prevent information on these sites from being linked with the charity and also 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 and to ensure that their social media use is compatible with their professional role and is in accordance with schools 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 pupils 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 in Maidstone Mencap.

Communicating with children, young people and parents and carers

- All members of staff are advised not to communicate with or add as 'friends' any current or past children, young people current or past children's' family members via any personal social media sites, applications or profiles.
    - Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead
    - If ongoing contact with children is required once they have left setting, members of staff will be expected to use existing alumni networks or use official Maidstone Mencap provided communication tools.
- Staff will not use personal social media accounts to make contact with children or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the DSL.
- Any communication from children and parents received on personal social media accounts will be reported to the Designated Safeguarding Lead.

8.3 Children's and Young Peoples Personal Use of Social Media

- Safe and appropriate use of social media must be an embedded and a progressive education approach, via age appropriate sites and resources and family support.
- Maidstone Mencap is aware that many popular social media sites state that they are not for children under the age of 13, therefore we will not support or encourage use or accounts specifically for children under this age.
- Any concerns regarding children's' use of social media, both at home and whilst in our setting, will be dealt with in accordance with existing l policies including anti-bullying and behaviour. Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.

- Children and young people will be advised:
    - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location. Examples could include real/full name, address, mobile or landline phone numbers, school attended, other social media contact details, email addresses, full names of friends/family, specific interests and clubs.
    - To only approve and invite known friends on social media sites and to deny access to others by making profiles private/protected.
    - Not to meet any online friends without a parent/carer or other responsible adult's permission and only 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 and report concerns both within the setting and externally.

8.4 Official Use of Social Media

Maidstone Mencap has official social media channels on our Website, Face- Book and Twitter

- The official use of social media sites, by Maidstone Mencap only takes place with clear educational or community engagement objectives, with specific intended outcomes.
    - The official use of social media as a communication tool has been formally risk assessed and approved by the board of trustees for Maidstone Mencap.
    - Only Administration management have access to inputting information into social media account
- Official Maidstone Mencap social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
    - Staff use Maidstone Mencap provided email addresses to register for and manage any official social media channels.
    - Official social media sites are suitably protected and, where possible, run or linked to our official website.
    - Public communications on behalf of the charity 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: Anti-bullying, Image use, Data protection, Confidentiality and Child protection.
    - All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Parents, carers and children will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
    - Social media tools **which** have been risk assessed and approved as suitable for educational purposes will be used.
- Parents and carers will be informed of any official social media use with children and young people and written parental consent will be obtained, as required.
- Maidstone Mencap 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.

Staff expectations

- Members of staff who follow and/or like the Maidstone Mencap 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 charity they will:
    - Sign the Maidstone Mencap Social media acceptable use policy.
    - Be professional at all times and aware that they are an ambassador for Maidstone Mencap.
    - Disclose their official role and/or position but make it clear that they do not necessarily speak on behalf of Maidstone Mencap.
    - Be responsible, credible, fair and honest at all times 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 that they have appropriate written consent before posting images on the official social media channel.
    - Not disclose information, make commitments or engage in activities on behalf of Maidstone Mencap unless they are authorised to do so.
    - Not engage with any direct or private messaging with current, or past, children young people, parents and carers.
    - Inform their line manager, the Designated Safeguarding Lead of any concerns, such as criticism, inappropriate content or contact.

9. Use of Personal Devices and Mobile Phones

- Maidstone Mencap recognises that personal communication through mobile technologies is an accepted part of everyday life for children, young people, staff and parents/carers, but technologies need to be used safely and appropriately within school.

9.1 Expectations

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate Maidstone Mencap policies, including, but not limited to: Anti-bullying, Behaviour and Child protection.
- Electronic devices of any kind that are brought onto site are the responsibility of the user at all times.
    - All members of Maidstone Mencap community are advised to take steps to protect their mobile phones or 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 Maidstone Mencap 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 in specific areas within the settings environment Where children and young people are present and must be stored safely away or kept in the office.
- The sending of abusive or inappropriate messages/ content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our Behaviour policy.
- All members of Maidstone Mencap's community are advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school 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, our Maidstone Mencap policies 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 during working hours.
    - Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during working times.
    - Not use personal devices during caring periods, unless written permission has been given by the 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 children young people or parents and carers.
    - Any pre-existing relationships, which could undermine this, will be discussed with the Designated Safeguarding Lead
- Staff will not use personal devices, such as: mobile phones, tablets or cameras:
    - To take photos or videos of children, only use work-provided equipment for this purpose.
    - Directly with children only use work-provided equipment during activities.
- If a member of staff breaches the Maidstone Mencap policy, action will be taken in line with the charities 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, the police will be contacted.

9.3 Children and Young Peoples' Use of Personal Devices and Mobile Phones

- Children will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- Maidstone Mencap expects service user personal devices and mobile phones to be kept in secure place, switched of but preferably not bought into our environment…
- If a service user needs to contact his/her parents or carers they will be allowed to use the office phone.
    - Parents are advised to contact their child via the office during attending hours; exceptions may be permitted on a case-by-case basis, as approved by the manager.
    - .

9.4 Visitors' Use of Personal Devices and Mobile Phones

- Parents, carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with Maidstone Mencap's Acceptable use policy and other associated policies, such as: Anti-bullying, Behaviour, Child protection and Image use.
- The setting will ensure appropriate signage and information is displayed to inform parents, carers and visitors of expectations of use.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the Designated Safeguarding Lead of any breaches of policy.

9.5 Officially provided mobile phones and devices

- Members of staff will be issued with a work phone number and email address, where contact with parents/ carers is required.
- mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.
- mobile phones and devices will always be used in accordance with the Acceptable use policy and other relevant policies

10. Responding to Online Safety Incidents and Concerns

- All members of the Maidstone Mencap community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.
- All members of the community must respect confidentiality and the need to follow the official Maidstone Mencap procedures for reporting concerns.
    - Children, parents and staff will be informed of the complaints procedure and staff will be made aware of the whistleblowing procedure.
- The setting requires staff, parents, carers and pupils to work in partnership to resolve online safety issues.
- After any investigations are completed, Maidstone Mencap will debrief, identify lessons learnt and implement any policy or safety changes as required.
- If the charity is unsure how to proceed with an incident or concern, the DSL will seek advice from the Education Safeguarding Team.
- Where there is suspicion that illegal activity has taken place, the DSL will contact the Education Safeguarding Team or Kent Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond the Maidstone Mencap community (for example if other local schools are involved or the public may be at risk), theDSL will speak with Kent Police and/or the Education Safeguarding Team first, to ensure that potential investigations are not compromised.

10.1 Concerns about Pupils Welfare

- The DSL will be informed of any online safety incidents involving safeguarding or child protection concerns.
    - The DSL will record these issues in line with our child protection policy.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Kent Safeguarding Children Board thresholds and procedures.
- The DSL will inform parents and carers of any incidents or concerns involving their child, as and when required.

10.2 Staff Misuse

- Any complaint about staff misuse will be referred to the DSL, according to the Allegations policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).

- Appropriate action will be taken in accordance with the Behaviour policy and Code of conduct.

• Procedures for Responding to Specific Online Incidents or Concerns

11.1 Youth Produced Sexual Imagery or "Sexting"

- Maidstone Mencap recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; therefore, all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- Maidstone Mencap will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and KSCB guidance: "Responding to youth produced sexual imagery".
- Maidstone Mencap will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- The school will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

11.1.1 Dealing with 'Sexting'

- If Maidstone Mencap is made aware of an incident involving the creation or distribution of youth produced sexual imagery, the setting will:
    - Act in accordance with our Child protection and Safeguarding policies and the relevant Kent Safeguarding Child Board's procedures.
    - Immediately notify the Designated Safeguarding Lead.
    - Store the device securely.
        - If an indecent image has been taken or shared on Maidstone Mencap owned network or devices, Maidstone Mencap will take action to block access to all users and isolate the image.
    - Carry out a risk assessment which considers any vulnerability of children involved; including carrying out relevant checks with other agencies.
    - Inform parents and carers, if appropriate, about the incident and how it is being managed.
    - Make a referral to Specialist Children's Services and/or the Police, as appropriate.
    - Provide the necessary safeguards and support for children, such as offering counselling or pastoral support.
    - Implement appropriate sanctions in accordance with safeguarding concerns policies and procedures but taking care not to further traumatise victims where possible.
    - Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
        - Images will only be deleted once Maidstone Mencap 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.
- Maidstone Mencap will take action regarding youth produced sexual imagery, regardless of whether the incident took place on/off our premises, using our or personal equipment.
- Maidstone Mencap will not:
    - View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.

        - In this case, the image will only be viewed by the Designated Safeguarding Lead and their justification for viewing the image will be clearly documented.
    - Send, share, save or make copies of content suspected to be an indecent image of children (i.e. youth produced sexual imagery) and will not allow or request others to do so.

11.2 Online Child Sexual Abuse and Exploitation

- Maidstone Mencap will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- Maidstone Mencap recognises online child sexual abuse as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- Maidstone Mencap will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate education for children, staff and parents/carers.
- Maidstone Mencap will ensure that all members of the community are aware of the support available regarding online child sexual abuse, both locally and nationally.

11.2. 1 Dealing with Online Child Sexual Abuse and Exploitation

- If Maidstone Mencap are made aware of incident involving online sexual abuse of a child, the DSL will:
    - Act in accordance with our Child protection and Safeguarding policies and the relevant Kent Safeguarding Child Board's procedures.
    - Immediately notify the Designated Safeguarding Lead.
    - Store any devices involved securely.
    - Immediately inform Kent police via 101 (or 999 if a child is at immediate risk)
    - Carry out a risk assessment which considers any vulnerabilities of child(s) involved (including carrying out relevant checks with other agencies).
    - Inform parents/carers about the incident and how it is being managed.
    - Make a referral to Specialist Children's Services (if required/ appropriate).
    - Provide the necessary safeguards and support for children, such as, offering counselling or pastoral support.
    - Review the handling of any incidents to ensure that best practice is implemented; Maidstone Mencap's leadership team will review and update any management procedures, where necessary.
- Maidstone Mencap will take action regarding online child sexual abuse, regardless of whether the incident took place on/off our premises, using our or personal equipment.
- Where possible children and young people will be involved in decision making
- If Maidstone Mencap is unclear whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.
- If Maidstone Mencap is made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Child Sexual Exploitation Team (CSET) by the Designated Safeguarding Lead.
- If children and young people at other schools or settings are believed to have been targeted, the DSL will seek support from Kent Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

11.3 Indecent Images of Children (IIOC)

- Maidstone Mencap will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- Maidstone Mencap will take action regarding IIOC on our owned equipment and/or personal equipment, even if access took place off site.
- Maidstone Mencap will take action to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If Maidstone Mencap is unclear if a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through Kent Police and/or the Education Safeguarding Team.

- If made aware of IIOC, Maidstone Mencap will:
    - Act in accordance with our child protection and safeguarding policy and the relevant Kent Safeguarding Child Boards procedures.
    - Immediately notify the Designated Safeguard Lead.
    - Store any devices involved securely.
    - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Kent police or the LADO.

- If made aware that a member of staff or a child has been inadvertently exposed to indecent images of children whilst using the internet, Maidstone Mencap community will:
    - Ensure that the Designated Safeguard Lead is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    - Ensure that any copies that exist of the image, for example in emails, are deleted.
    - Report concerns, as appropriate to parents and carers.

- If made aware that indecent images of children have been found on the Maidstone Mencap devices, the setting will:
    - Ensure that the Designated Safeguard Lead is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    - Ensure that any copies that exist of the image, for example in emails, are deleted.
    - Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
    - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
    - Report concerns, as appropriate to parents and carers.

- If made aware that a member of staff is in possession of indecent images of children on Maidstone Mencap owned devices, the setting will:
    - Ensure that the DSL and board of trustees is informed.
    - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.
    - Quarantine any devices until police advice has been sought.

11.4 Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Maidstone Mencap

11.5 Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Maidstone Mencap *and* will be responded to in line with existing school policies, including 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 Maidstone Mencap is unclear on how to respond, or whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice through the Education Safeguarding Team and/or Kent Police.

11.6 Online Radicalisation and Extremism

- Maidstone Mencap will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in our setting
- If Maidstone Mencap is concerned that a child or parent/carer may be at risk of radicalisation online, the Designated Safeguarding Lead will be informed immediately, and action will be taken in line with the Child protection policy.
- If Maidstone Mencap is concerned that member of staff may be at risk of radicalisation online, the DSL and board of trustees will be informed immediately, and action will be taken in line with the Child protection and Allegations policies.

12. Useful Links for Educational Settings

Kent Support and Guidance

Kent County Council Education Safeguarding Team:

  - Online safety tel 03000 415797 esafetyofficer@kent.gov.uk Tel: 03000 415797
  - Education officer west kent tel 03000 412209

- A comprehensive contact list for all safeguarding concerns is available on our website and hall safeguarding notice boards.
- Guidance for Educational Settings:
  - www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding
  - www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-classroom-materials
  - www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-useful-links
- Kent e–Safety Blog: www.kentesafety.wordpress.com

Kent Police:

- www.kent.police.uk or www.kent.police.uk/internetsafety

- In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Kent Police via 101

Other:

- Kent Public Service Network (KPSN): www.kpsn.net
- EiS - ICT Support for Schools and Kent Schools Broadband Service Desk**:** www.eiskent.co.uk

National Links and Resources

- Action Fraud: www.actionfraud.police.uk
- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
  - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk