



St Mildred's PI School

Acceptable Use Policy

Inc Mobile and Smart Tech

2025-26



Contents:

- Pupil AUP
- Parents AUP and information
- Staff AUP and information
- Visitor/Volunteer AUP
- Wi-Fi AUP
- Flow chart for Dealing with inappropriate material online
- Flow chart for Responding to an Online safety concern
- Mobile and Smart Technology Policy

Our AUP Statement

At St Mildred's we want to ensure that all members of our community are safe and responsible users of technology. We will support our learners to...

- Become empowered and responsible digital creators and users
- Use our resources and technology safely, carefully and responsibly
- Be kind online and help us to create a community that is respectful and caring, on and offline
- Be safe and sensible online and always know that you can talk to a trusted adult if you need help



Pupils Acceptable Use Policy:

- I understand that the St Mildred's online rules will help keep me safe and happy when I go online.
- I only go online when an adult is with me.
- I only click on online things online when I know what they do. If I am not sure, I ask an adult first.
- I keep my personal information and passwords safe
- I only send polite and friendly messages online.
- I know the school can see what I am doing online when I use our school computers, tablets and online reading
- If I see something online that makes me feel upset, unhappy, or worried I will always tell an adult.
- I can visit our school website www.st-mildreds.kent.sch.uk/online-safety-1/ or www.thinkuknow.co.uk/5_7/ or www.ceopeducation.co.uk to learn more about keeping safe online
- I know that if I do not follow the rules:
 - I may be stopped from using school devices and the internet.
 - I will need to talk about it with an adult.
 - It will be discussed with my parents/carers if necessary.
- I have read and talked about these rules with my parents/carers

Please sign and return this part to school

St Mildred's Acceptable Use of Technology Policy – Learner Agreement

I, with my parents/carers, have read and understood the Acceptable Use of Technology Policy (AUP).

I agree to follow the AUP when:

1. I use school systems and devices at school and at home.
2. I use my own equipment out of the school, including communicating with other members of our school or when accessing school systems.

Name..... Class.....

Parent/Carers Signature.....

Date.....

Be

SAFE

Online

1 I only go online with a grown up



2 I am kind online



3 I keep information about me safe



4 I tell a grown up if something online makes me unhappy



Published by EIS Kent • 0300 065 8800 • www.eiskent.co.uk

Dear Parent/Carer

All pupils at St Mildred's PI School use computer facilities and internet access, as an essential part of learning as required by the National Curriculum. Your child will have the opportunity to access a wide range of information and communication technology (ICT) resources. This includes access to:

- Computers, laptops and other digital devices
- Internet which may include search engines and educational websites
- Email
- Digital cameras, web cams
- Game-based technologies

St Mildred's recognises the essential and important contribution that the online world and technology plays in promoting children's learning and development and believe it offers a fantastic range of positive activities and experiences. We do recognise however that this can bring risks. We take your child's online safety seriously and, as such, will take all reasonable precautions, including monitoring and filtering systems, to ensure that pupils are safe when they use our internet and systems. This includes:

- Educating children about online safety
- Children using the internet under adult supervision
- Access to the internet through a Kent Approved provider (BT)
- Fortinet Internet filtering

We recognise however that no technical system can replace online safety education and believe that children themselves have an important role to play in developing responsible behaviour. In order to support the school in developing your child's knowledge and understanding about online safety, we request that you read the attached Acceptable Use Policy with your child, discuss the content with them and return the attached slip. *We understand that your child is too young to give informed consent on their own; however, we feel it is good practice to involve them as much as possible in the decision making process, and believe a shared commitment is the most successful way to achieve this.*

Hopefully, you will also find this Acceptable Use Policy provides you with an opportunity for conversations between you and your child about safe and appropriate use of the technology, both at school and at home.

We request that all parents support our approach to online safety by role modelling safe and positive online behaviour and by discussing online safety whenever children access technology at home. Parents can visit the school website's www.st-mildreds.kent.sch.uk/online-safety/ for more information about our approach to online safety. Full details of the school's online safety policy are available on the school website or on request.

Parents/carers may also like to visit the following links for more information about keeping children safe online:

- www.thinkuknow.co.uk
- www.childnet.com
- www.nspcc.org.uk/onlinesafety
- www.saferinternet.org.uk
- www.internetmatters.org

Should you wish to discuss the matter further, please do not hesitate to contact the school Designated Safeguarding Lead Mrs Crutchley, Mrs Hill or myself.

Yours sincerely,

James Williams Executive Headteacher

Parent/Carers Acceptable Use Policy

1. I know that my child will be provided with internet access and will use a range of IT systems in order to access the curriculum and be prepared for modern life whilst at St Mildred's P I School.
2. I understand that the AUP applies to my child's use of St Mildred's devices and systems on site and at home, and personal use where there are safeguarding and/or behaviour concerns. This may include if online behaviour poses a threat or causes harm to another pupil, could have repercussions for the orderly running of the St Mildred's, if a pupil is identifiable as a member of the St Mildred's, or if the behaviour could adversely affect the reputation of the St Mildred's.
3. I am aware that use of mobile and smart technology, such as mobile phones by children, is not permitted at St Mildred's. On the rare occasion that a child may need a mobile phone to either support a medical need or parental communication then this must be put in writing and agreed by the school with the phone signed in and out at the office.
4. I understand that any use of St Mildred's devices and systems are appropriately filtered; this means our school uses Fortinet filtering systems to block inappropriate content online.
5. I am aware that my child's use of St Mildred's provided devices and systems will be monitored for safety and security reasons, when used on and offsite. This includes monitoring software and reports through our internet provider Cantium. Monitoring approaches are in place to keep my child safe and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.
6. I understand that the St Mildred's will take every reasonable precaution, including implementing appropriate monitoring and filtering systems as above, to ensure my child is safe when they use St Mildred's devices and systems, on and offsite. I however understand that the St Mildred's cannot ultimately be held responsible for filtering breaches that occur due to the dynamic nature of materials accessed online.
7. I am aware that my child will receive online safety education to help them understand the importance of safe use of technology and the internet, both in and out of St Mildred's.
8. I have read and discussed St Mildred's Learner Acceptable Use of Technology Policy (AUP) with my child.
9. I will support St Mildred's safeguarding policies and will ensure that I use appropriate parental controls, will appropriately supervise/monitor my child's use of the internet outside of St Mildred's and will discuss online safety with them when they access technology at home.

10. I know I can seek support from the school about online safety, such as via the St Mildred's website [Online Safety | St Mildred's Primary Infant School \(st-mildreds.kent.sch.uk\)](http://Online Safety | St Mildred's Primary Infant School (st-mildreds.kent.sch.uk)), to help keep my child safe online at home.
11. I will support the St Mildred's approach to online safety. I will role model safe and positive online behaviour for my child by sharing images, text, and video online responsibly.
12. I, together with my child, will not deliberately upload or share any content that could upset, threaten the safety of or offend any member of the St Mildred's community, or content that could adversely affect the reputation of the St Mildred's
13. I understand that a partnership approach to online safety is required. If the school has any concerns about either my or my child's behaviour or safety online, then I will be contacted.
14. I understand that if I or my child do not abide by the St Mildred's AUP, appropriate action will be taken. This could include sanctions being applied in line with the St Mildred's policies and if a criminal offence has been committed, the police being contacted.
15. I know that I can speak to the Designated Safeguarding Lead (Mrs H Crutchley), my child's teacher or the Online Safety Lead (Mrs E Hill) if I have any concerns about online safety.

.....

Please return this part to school

I have read, understood and agree to comply with the St Mildred's Parent/Carer Acceptable Use of Technology Policy.

Child's Name..... Class.....

Parent/Carers Signature.....

Date.....

General information for staff

Dear Staff

At St Mildred's we recognise that staff can be vulnerable to online risks. Social media can blur the definitions of personal and working lives; it is important that all members of staff at St Mildred's take precautions to protect themselves both professionally and personally online. We request that all members of staff:

- Are conscious of their own professional reputation and that of the school when online.
 - All members of staff are strongly advised in to take steps to ensure that their personal information and content is not accessible to anybody who does not or should not have permission to access it.
 - Be aware that content shared online cannot be guaranteed to be "private" and could potentially be seen by unintended audiences.
- Are aware that as professionals, we must ensure that the content we post online does not bring the school or our professional role into disrepute and does not undermine professional confidence in our abilities.
 - The [teaching standards](#) state that as professionals we should be achieving the highest possible standards in our conduct, act with honesty and integrity and forge positive professional relationships.
- Are careful when publishing any information, personal contact details, video or images online.
 - It is very important to be aware that sometimes content shared online, even in jest, can be misread, misinterpreted or taken out of context, which can lead to complaints or allegations being made. Don't be afraid to be yourself online but do so respectfully.
 - Consider if you would feel comfortable about a current or prospective employer, colleague, child in your care or their parent/carer, viewing or sharing your content. If the answer is no, consider if it should be posted online at all.
- Do not accept learners (past or present) or their parents/carers as "friends" on a personal account.
 - You may be giving them access to your personal information and allowing them to contact you inappropriately through unregulated channels. They may also be giving you access to their personal information and activities which could cause safeguarding concerns.
 - If you have a pre-existing relationship with a child or parent/carer or there is any other situation that may compromise your ability to comply with this, please speak to the Designated Safeguarding Lead (Hannah Crutchley).

- Always use work provided contact information, such as approved school learning platforms/app, a work email address and/or a work phone number to contact learners and parents/carers.
- If you are concerned about a learner's wellbeing or online behaviour, please speak to the Designated Safeguarding Lead. If you are targeted online by a member of the community or are concerned about a colleague, please speak to the Heads of School/Executive Head or Chair of governors (Jan Brazier).
 - If you are unhappy with the response you receive, or do not feel able to speak to the Designated Safeguarding Lead, Heads of School/Executive Head or Chair of governors then we request you follow our Whistleblowing procedure.
- If you have any questions regarding online conduct expected of staff, please speak to the Designated Safeguarding Lead (Hannah Crutchley) or Online Safety lead (Elena Hill)

Additional advice to help you consider how to protect yourself online is available via:

- www.childnet.com/teachers-and-professionals/for-you-as-a-professional
- www.gov.uk/government/publications/preventing-and-tackling-bullying
- www.saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/professional-reputation
- www.saferinternet.org.uk/professionals-online-safety-helpline

We would like to remind all staff of our Acceptable Use of Technology Policy and the importance of maintaining professional boundaries online. Failure to follow this guidance and the school behaviour policy/code of conduct could lead to disciplinary action; it is crucial that all staff understand how to protect themselves online.

Please speak to me, your line manager or the Designated Safeguarding Lead if you have any queries or concerns regarding this.

Yours sincerely,

James Williams
Executive Head.

Staff Acceptable Use of Technology Policy

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use St Mildred's IT systems in a professional lawful, and ethical manner. To ensure that members of staff understand their professional responsibilities when using technology, they are asked to read and sign the staff Acceptable Use Policy (AUP).

Our AUP is not intended to unduly limit the ways in which members of staff teach or use technology professionally, or indeed how they use the internet personally; however the AUP will help ensure that all staff understands St Mildred's expectations regarding safe and responsible technology use, and can manage the potential risks posed. The AUP will also help to ensure that school systems are protected from any accidental or deliberate misuse which could put the safety and security of our systems or members of the community at risk.

Policy Scope

1. I understand that this Acceptable Use of Technology Policy (AUP) applies to my use of technology systems and services, either provided to me by the school or accessed by me as part of my role within St Mildred's professionally and personally, both on and offsite. This may include my use of devices such as laptops, mobile phones, tablets, digital cameras, as well as IT systems and networks, email, data and data storage, remote learning systems and communication technologies.
2. I understand that St Mildred's Acceptable Use of Technology Policy (AUP) should be read and followed in line with the school staff handbook/code of conduct.
3. I am aware that this AUP does not provide an exhaustive list; all staff should ensure that technology use is consistent with the school ethos, staff behaviour/handbook and safeguarding policies, national and local education and child protection guidance, and the law.

Use of School Devices and Systems

4. I will only use the equipment and internet services provided to me by the school for example school provided laptops, tablets, mobile phones and internet access, when working with learners.
5. I understand that any equipment and internet services provided by my workplace is intended for educational purposes and/or professional use and should only be accessed by members of staff. Reasonable personal use of setting IT systems and/or devices by staff is allowed.

Data and System Security

6. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or securing/locking access.
 - o I will use a 'strong' password to access school systems.
 - o I will protect the devices in my care from unapproved access or theft. E.g. devices must be kept in the boot of the car to protect from theft when travelling to and from work etc

7. I will respect system security and I will not disclose my password or security information to others.
8. I will not open any hyperlinks or attachments in emails unless they are from a known and trusted source. If I have any concerns about email content sent to me, I will report them to the IT system manager (Ben Cliff).
9. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager (Ben Cliff)
10. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including UK GDPR in line with the school information security policies.
 - All personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely.
 - Any data being removed from the school site, such as via email or on memory sticks or CDs, will be suitably protected. This may include data being encrypted by a method approved by the school eg encrypted memory sticks and password protected email systems.
 - Any data being shared online, such as via cloud systems or artificial intelligence tools (AI), will be suitably risk assessed and approved by the schools Data Protection Officer and leadership team prior to use to ensure it is safe and legal.
11. I will not keep documents which contain school-related sensitive or personal information, including images, files, videos and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. Where possible I will use OneDrive to upload any work documents and files in a password protected environment.
12. I will not store any personal information on the school computer system including any school laptop or similar device issued to members of staff that is unrelated to school activities, such as personal photographs, files or financial information.
13. I will ensure that school owned information systems are used lawfully and appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation
14. I will not attempt to bypass any filtering and/or security systems put in place by the school.
15. If I suspect a computer or system has been damaged or affected by a virus or other malware, then I will report this to the ICT Technician, Ben Cliff, as soon as possible
16. If I have lost any school related documents or files, I will report this to the ICT Technician and school Data Protection Officer (Alan Martin via Jeannette Read – school Data Protection Lead) as soon as possible.
17. Any images or videos of learners will only be used as stated in the school camera and image use policy (attached below). I understand images of learners must always be appropriate and should only be taken with the school provided equipment and taken/published where learners and their parents/carers have given explicit written consent.

18. I understand that it is part of my roles and responsibilities to ensure that appropriate filtering and monitoring is implemented by St Mildred's as detailed in the Child Protection policy, Online Safety Policy and AUP and as discussed with me as part of my induction and/or ongoing safeguarding and child protection staff training.
19. If there is failure in the filtering software or abuse of the filtering or monitoring systems, for example, I witness or suspect accidental or deliberate access to illegal, inappropriate or harmful material, I will report this to the DSL and IT Technician in line with the Child Protection/Online Safety policy.
20. I am aware of the expectations relating to safe technology use in the classroom, safe remote learning, and other working spaces as listed in the Child Protection policy, Online Safety Policy and AUP.
21. I am aware that generative artificial intelligence (AI) tools may have many uses which could benefit our school community. However, I also recognise that AI tools can also pose risks, including, but not limited to, bullying and harassment, abuse and exploitation (including child sexual abuse), privacy and data protection risks, plagiarism and cheating, and inaccurate, harmful and/or biased material. Additionally, its use can pose moral, ethical and legal concerns if not carefully managed. As such I understand that:
- AI tools are only to be used responsibly and ethically, and in line with our school child protection, data protection, and staff code of conduct policy expectations.
 - A risk assessment will be undertaken, and written approval will be sought from the senior leadership team prior to any use of AI tools, for example if used in the classroom, or to support lesson planning.
 - A Data Protection Impact Assessment (DPIA) will always be completed prior to any use of AI tools that may be processing any personal, sensitive or confidential data and use will only occur following approval from the DPO.
 - I am required to critically evaluate any AI-generated content for accuracy, bias, and appropriateness before sharing or using it in educational contexts.
 - AI must not be used to replace professional judgement, especially in safeguarding, assessment, or decision-making involving pupils.
 - Only approved AI platforms may be used with pupils. Pupils must be supervised when using AI tools, and I must ensure age-appropriate use and understanding prior to use.
 - Any misuse of AI will be responded to in line with relevant school policies, including but not limited to, anti-bullying, staff and pupil behaviour and child protection.
22. I will promote online safety with the children in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create by:
- exploring online safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used.
 - creating a safe environment where children feel comfortable to report concerns and say what they feel, without fear of getting into trouble and/or be judged for talking about something which happened to them online.

- involving the Designated Safeguarding Lead (DSL) (Hannah Crutchley) or a deputy (E Hill, A Rosedon, N Reeves, J Williams) as part of planning online safety lessons or activities to ensure support is in place for any children who may be impacted by the content.
- Informing the DSL and/or leadership team if I am teaching topics which could create unusual activity on the filtering logs, or if I believe the filtering system is placing unreasonable restrictions on teaching, learning or administration.
- make informed decisions to ensure any online safety resources used with children is appropriate.

23. I will respect copyright and intellectual property rights and ensure my use of online platforms and tools is safe, legal and ethical; I will obtain appropriate permission to use content, and if videos, images, text, or music are protected, I will not copy, share, misuse, plagiarise, or distribute them.

Mobile Devices and Smart Technology

24. I have read and understood the school Mobile and Smart Technology section of the Online Safety Policy which addresses use by children and staff.

25. I will ensure that my use of mobile devices and smart technology is compatible with my professional role, does not interfere with my work duties and takes place in line with the staff handbook/code of conduct and the school Online Safety policy (Mobile and Smart Technology section) and the law.

Online Communication, including Use of Social Media

26. I will ensure that my use of communication technology, including use of social media is compatible with my professional role, does not interfere with my work duties and takes place in line with the staff handbook/code of conduct, the school Online Safety and AUP policy and the law. In line with these policies:

- I will take appropriate steps to protect myself and my reputation online when using communication technology, including the use of social media as outlined in the Online Safety Policy
- I will not discuss or share data or information relating to learners, staff, school business or parents/carers on social media.

27. My electronic communications with current and past learners and parents/carers will be transparent and open to scrutiny and will only take place within clear and explicit professional boundaries.

- I will ensure that all electronic communications take place in a professional manner via school approved and/or provided communication channels and systems, such as a school email address, user account or telephone number.
- I will not share any personal contact information or details with learners, such as my personal email address or phone number.
- I will not add or accept friend requests or communications on personal social media with current or past learners and/or their parents/carers.

- If I am approached online by a current or past learner or parents/carer, I will not respond and will report the communication to my line manager and the Designated Safeguarding Lead (DSL).
- Any pre-existing relationships or situations that compromise my ability to comply with the AUP will be discussed with the DSL and Heads of School.

28. If I have any queries or questions regarding safe and professional practise online either in St Mildred's Infant School or off site, I will raise them with the DSL/Headteacher.

29. I will not upload, download, or access any materials which are illegal, such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act.

30. I will not attempt to access, create, transmit, display, publish or forward any material or content online that is inappropriate or likely to harass, cause offence, inconvenience, or needless anxiety to any other person.

31. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the school into disrepute.

Policy Compliance

32. I understand that the school may exercise its right to monitor the use of its information systems, including internet access and the interception of emails, to monitor policy compliance and to ensure the safety of learners and staff. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

Policy Breaches and Concerns

33. If I have any queries or questions regarding safe and professional practise online, either in school or off site, I will raise them with the DSL and/or the Executive Headteacher.

34. I will report and record any concerns about the welfare, safety or behaviour of children or parents/carers online to the DSL in line with the school child protection policy.

35. I will report concerns about the welfare, safety, or behaviour of staff online to the heads of School, in line with school child protection policy and the allegations against staff policy.

36. I understand that the school may exercise its right to monitor the use of its devices information systems to monitor policy compliance and to ensure the safety of children and staff. This includes monitoring all school provided devices and school systems and networks including school provided internet access, whether used on or offsite and may include the interception of messages and emails sent or received via school provided devices, systems and/or networks. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

37. I understand that if the school believe that unauthorised and/or inappropriate use of school devices, systems or networks is taking place, the school may invoke its disciplinary procedures as outlined in the staff behaviour policy/code of conduct.
38. I understand that if the school believe that unprofessional or inappropriate online activity, including behaviour which could bring the school into disrepute, is taking place online, the school may invoke its disciplinary procedures as outlined in the staff behaviour policy/code of conduct.
39. I understand that if the school suspects criminal offences have occurred, the police will be informed.

I have read, understood and agreed to comply with St Mildred's Staff Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.

Name of staff member:

Signed:

Date (DDMMYY).....

Visitor/Volunteer Acceptable Use Policy

For visitors/volunteers and staff who do not access school ICT systems

As a professional organisation with responsibility for children's safeguarding it is important that all members of the community, including visitors and volunteers, are aware of our behaviour expectations and their professional responsibilities when using technology. This AUP will help St Mildred's ensure that all visitors and volunteers understand the school's expectations regarding safe and responsible technology use.

Policy Scope

1. I understand that this Acceptable Use of Technology Policy (AUP) applies to my use of technology systems and services, either provided to me by the school or accessed by me as part of my role within St Mildred's professionally and personally. This may include my use of devices such as laptops, mobile phones, tablets, digital cameras, as well as IT systems and networks, email, data and data storage, remote learning systems and communication technologies.
2. I understand that the St Mildred's AUP should be read and followed in line with the school staff handbook/code of conduct and Volunteer guidelines.
3. I am aware that this AUP does not provide an exhaustive list; visitors and volunteers should ensure that all technology use is consistent with the school ethos, staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.
4. I will not upload, download, or access any materials which are illegal, such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act.
5. I will not attempt to access, create, transmit, display, publish or forward any material or content online that is inappropriate or likely to harass, cause offence, inconvenience, or needless anxiety to any other person.
6. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the school into disrepute.

Data and Image Use

7. I will ensure that any access to personal data is kept in accordance with Data Protection legislation, including UK GDPR.

8. Any images or videos of learners will only be taken in line with the school camera and image use policy, using school provided equipment and by ensuring school staff are aware and permission is given.

Classroom Practice

9. I am aware of the expectations regarding safe use of technology in the classroom and other working spaces, including appropriate supervision of learners, as outlined in the school online safety policy.
10. I will support and reinforce safe behaviour whenever technology is used on site and I will promote online safety with the children in my care.
11. If I witness or suspect accidental or deliberate access to illegal, inappropriate or harmful material by any member of the school community, I will report this to the DSL and in line with the school child protection/online safety policies.
12. I will respect copyright and intellectual property rights and ensure my use of online platforms and tools is safe, legal and ethical; I will obtain appropriate permission to use content, and if videos, images, text, or music are protected, I will not copy, share, misuse, plagiarise, or distribute them.

Use of Social Media and Mobile Technology

13. I have read and understood the school online safety policy which covers expectations regarding staff use of social media and mobile technology.
14. I will ensure that my online reputation and use of technology and is compatible with my role within the school. This includes my use of email, text, social media, social networking, gaming and any other personal devices or websites.
 - I will take appropriate steps to protect myself online as outlined in the online safety policy.
 - I will not discuss or share data or information relating to learners, staff, St Mildred's business or parents/carers on social media.
 - I will ensure that my use of technology and the internet will not undermine my role, interfere with my duties and will be in accordance with the school volunteer guidelines and the law.
15. My electronic communications with learners, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny.
 - All communication will take place via school approved communication channels such as via a school provided email address or telephone number and not via personal

devices or communication channels such as via my personal email, social networking account or mobile phone number.

- Any pre-existing relationships or situations that may compromise this will be discussed with the DSL and headteacher.

Policy Compliance, Breaches or Concerns

16. If I have any queries or questions regarding safe and professional practise online either in school or off site, I will raise them with the Designated Safeguarding Lead and the Online Safety Lead.
17. I understand that the school may exercise its right to monitor the use of its devices information systems to monitor policy compliance and to ensure the safety of children and staff. This includes monitoring all school provided devices and school systems and networks including school provided internet access, whether used on or offsite and may include the interception of messages and emails sent or received via school provided devices, systems and/or networks. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.
18. I will report and record concerns about the welfare, safety or behaviour of learners or parents/carers to the Designated Safeguarding Lead in line with the school online safety/child protection policy.
19. I will report concerns about the welfare, safety or behaviour of staff to the headteacher, in line with the allegations against staff policy.
20. I understand that if the school believes that if unauthorised and/or inappropriate use, or unacceptable or inappropriate behaviour is taking place online, the school may invoke its disciplinary procedures.
21. I understand that if the school suspects criminal offences have occurred, the police will be informed

I have read, understood and agree to comply with the St Mildred's Visitor /Volunteer Acceptable Use Policy.

Signed: Print Name: Date:

Accepted by:.....Date:

Wi-Fi Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all members of the school community are fully aware of the school boundaries and requirements when using the school Wi-Fi systems, and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

This is not an exhaustive list and all members of the school community are reminded that technology use should be consistent with our ethos, other appropriate policies and the law.

1. The school provides Wi-Fi for the school community and allows access for educational use only.
2. I am aware that the school will not be liable for any damages or claims of any kind arising from the use of the wireless service. The school takes no responsibility for the security, safety, theft, insurance and ownership of any device used within the school premises that is not the property of the school.
3. The use of technology falls under the Acceptable Use of Technology Policy (AUP), online safety policy and behaviour policy, which all learners/staff/visitors and volunteers must agree to and comply with.
4. The school reserves the right to limit the bandwidth of the wireless service, as necessary, to ensure network reliability and fair sharing of network resources for all users.
5. School owned information systems, including Wi-Fi, must be used lawfully; I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
6. The school wireless service is not secure, and the school cannot guarantee the safety of traffic across it. Use of the school wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. I confirm that I knowingly assume such risk.
7. The school accepts no responsibility for any software downloaded and/or installed, email opened, or sites accessed via the school wireless service's connection to the internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other internet-borne programs is my sole responsibility; and I indemnify and hold harmless the school from any such damage.

8. The school accepts no responsibility regarding the ability of equipment, owned by myself, to connect to the school wireless service.
9. I will respect system security; I will not disclose any password or security information that is given to me. To prevent unauthorised access, I will not leave any information system unattended without first logging out or locking my login as appropriate.
10. I will not attempt to bypass any of the school security and filtering systems or download any unauthorised software or applications.
11. My use of school Wi-Fi will be safe and responsible and will always be in accordance with the school AUP and the law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.
12. I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring the school into disrepute.
13. I will report any online safety concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead as soon as possible.
14. If I have any queries or questions regarding safe behaviour online, I will discuss them with Designated Safeguarding Lead or the Online Safety Lead (Mrs E Hill)
15. I understand that my use of the school Wi-Fi may be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the school suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the school may terminate or restrict usage. If the school suspects that the system may be being used for criminal purposes, the matter will be brought to the attention of the relevant law enforcement organisation.

For those using school Wi-Fi

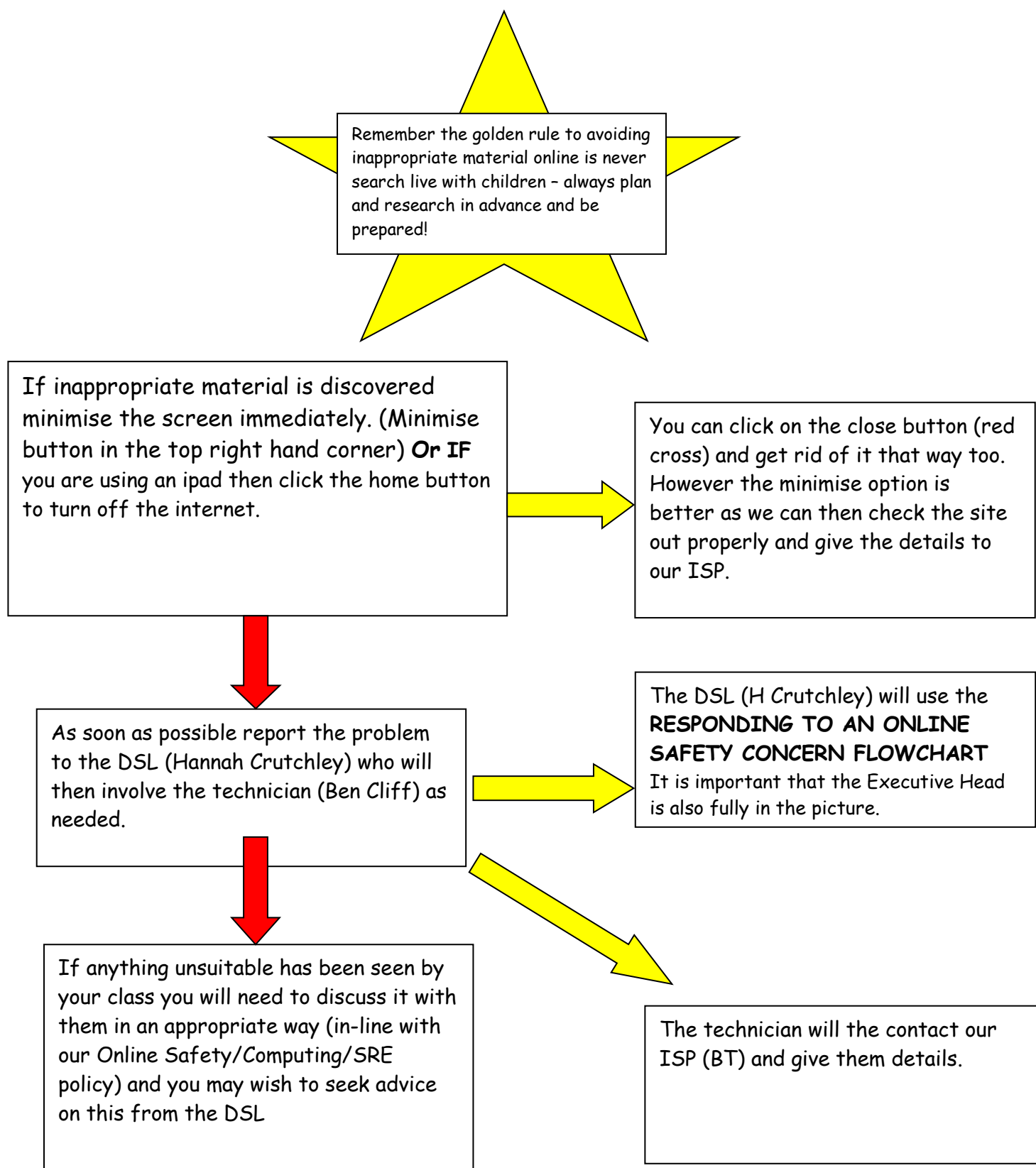
As a professional organisation with responsibility for children's safeguarding it is important

I have read, understood and agreed to comply with St Mildred's Wi-Fi acceptable Use Policy.

Name

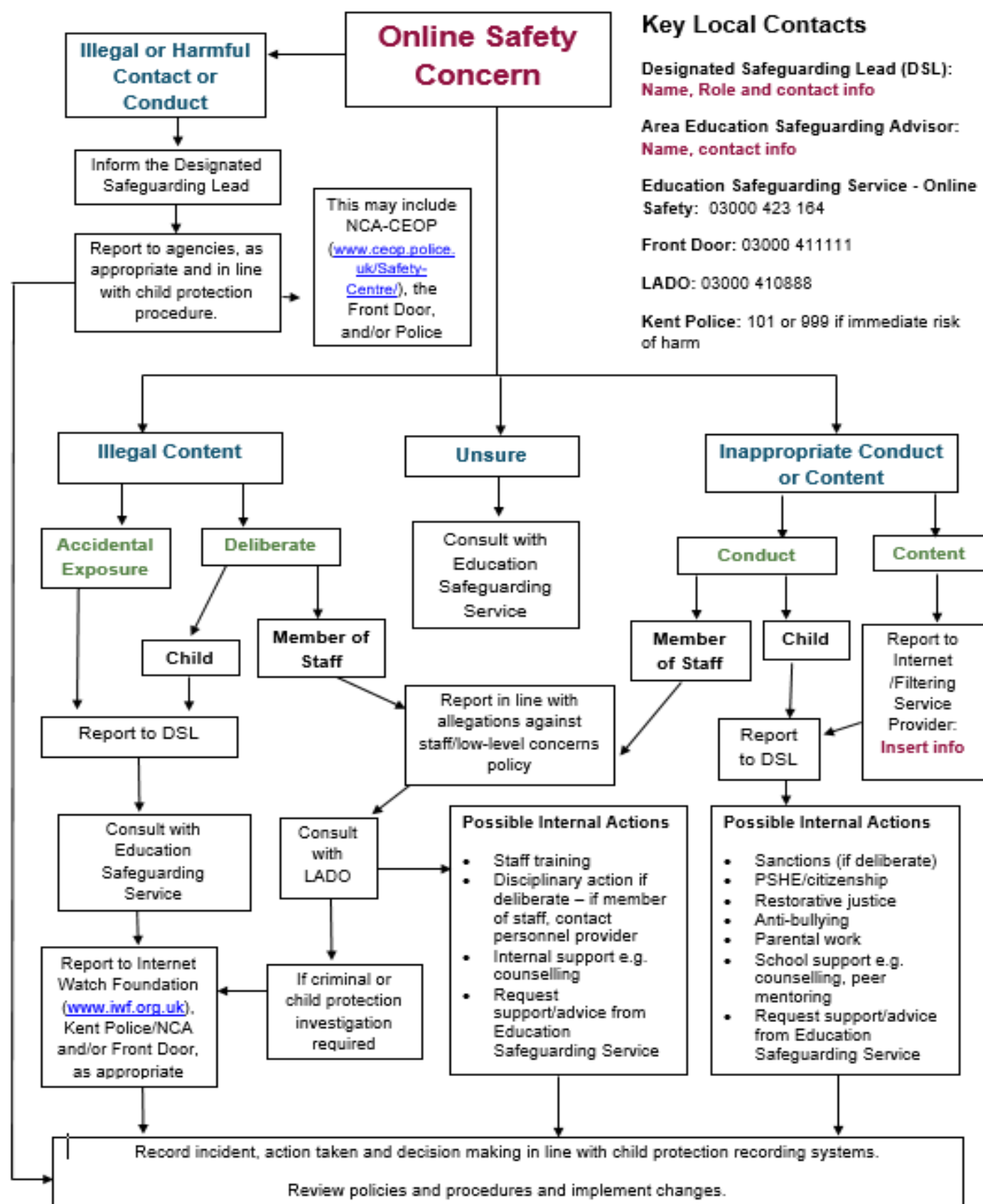
Signed:Date (DDMMYY).....

Dealing with inappropriate material online



PLEASE ALSO SEE **RESPONDING TO AN ONLINE SAFETY CONCERN FLOWCHART** ALONGSIDE THIS

Responding to an online safety concern



Mobile and Smart Technology Policy

1. Policy aims and scope

- This policy has been written by St Mildred's involving staff, pupils and parents/carers, building on Kent County Councils LADO Education Safeguarding Advisory Service mobile and smart technology policy template, with specialist advice and input as required.
- It takes into account the Department for Education (DfE) statutory guidance '[Keeping Children Safe in Education](#)' (KCSIE), [Early Years and Foundation Stage \(EYFS\)](#) '[Working Together to Safeguard Children](#)' (WTSC), the DfE non-statutory guidance '[Behaviour in Schools Advice for headteachers and school staff](#)', '[Mobile Phones in Schools](#)' and the local [Kent Safeguarding Children Multi-agency Partnership](#) (KSCMP) procedures.
- The purpose of this policy is to safeguard and promote the welfare of all members of our community when using mobile devices and smart technology.
 - St Mildred's recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all pupils and staff are protected from potential harm when using mobile and smart technology.
 - As outlined in our Child Protection Policy, the Designated Safeguarding Lead (DSL), Hannah Crutchley, is recognised as having overall responsibility for online safety.
- This policy applies to all access to and use of all mobile and smart technology on site; this includes but is not limited to mobile/smart phones and personal devices such as tablets, e-readers, games consoles and wearable technology, such as smart watches and fitness trackers, which facilitate communication or have the capability to record sound and/or images.
- This policy applies to children, parents/carers and all staff, including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy).

2. Links with other policies

- This policy links with several other policies, practices and action plans, including but not limited to:
 - Anti-bullying policy
 - Acceptable Use Policies (AUP)
 - Behaviour and relationships policy
 - Cameras and image use policy
 - Child protection policy
 - Staff code of conduct/staff handbook
 - Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
 - GDPR
 - Online Safety

3. Safe use of mobile and smart technology expectations

- St Mildred's recognises that use of mobile and smart technologies is part of everyday life for many children, staff and parents/carers.

- Electronic devices of any kind that are brought onto site are the responsibility of the user. All members of our community are advised to:
 - take steps to protect their personal mobile phones or other smart devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
 - use passwords/PIN numbers to ensure that unauthorised access, calls or actions cannot be made on personal phones or devices.
- Mobile devices and other forms of smart technology are not permitted to be used in specific areas on site; this includes classrooms, and other areas where children are.
- The sending of abusive or inappropriate messages or content, including via personal mobile devices and/or smart technology is forbidden by any member of the community; any breaches will be dealt with in line with our anti-bullying, behaviour and child protection policies.
- All members of the St Mildred's community are advised to ensure that their personal mobile and smart technology devices do not contain any content which may be offensive, derogatory or illegal, or which would otherwise contravene our behaviour or child protection policies.

4. School provided mobile phones and devices

- Members of staff will be issued with a work phone number in addition to their work email address, where contact with parents/carers is required.
- Staff providing formal remote/online learning will do so using school provided equipment in accordance with our Acceptable Use Policy (AUP)/remote learning AUP.
- School mobile phones and/or devices will be suitably protected via a passcode/password/PIN and must only be accessed or used by members of staff.
- School mobile phones and/or devices will always be used in accordance with our staff code of conduct/behaviour policy, acceptable use of technology policy and other relevant policies.
- Where staff (or pupils if using school provided ipads) are using school provided mobile phones and/or devices, they will be informed prior to use via our Acceptable Use Policy (AUP) that activity may be monitored for safeguarding reasons and to ensure policy compliance.

5. Staff use of mobile and smart technology

- Members of staff will ensure that use of any mobile and smart technology, including personal phones, wearable technology and other mobile/smart devices, will take place in accordance with the law, as well as relevant school policy and procedures, including confidentiality, child protection, GDPR, staff behaviour/code of conduct, Online Safety and Acceptable Use Policies.
- Staff will be advised to:
 - Keep personal mobile and smart technology devices in a safe and secure place (eg staff room lockers/in classroom staff cupboards) during lesson time.
 - Keep personal mobile phones and devices switched off or set to 'silent' or 'do not disturb' modes during lesson times.
 - Ensure that Bluetooth or other forms of communication, such as 'airdrop', are hidden or disabled during lesson times.
 - Not use personal mobile or smart technology devices during teaching periods, unless permission has been given by the Heads of School, such as in emergency circumstances/medical phone calls. Please discuss this with Heads of School as necessary.

- Ensure that any content bought onto site via personal mobile and smart technology devices is compatible with their professional role and our behaviour expectations.
- Members of staff are not permitted to use their own personal mobile and smart technology devices for contacting pupils or parents and carers.
 - Any pre-existing relationships or circumstance, which could compromise staff's ability to comply with this, will be discussed with the DSL/Heads of School.
- Staff will only use school provided equipment (not personal devices):
 - to take photos or videos of pupils in line with our image use policy.
 - to work directly with pupils during lessons/educational activities.
 - to communicate with parents/carers.
- Where remote learning activities take place, staff will use school provided equipment. If this is not available, staff will only use personal devices with prior approval from the Heads of School, following a formal risk assessment. Staff will follow clear guidance outlined in the Acceptable Use Policy and/or remote learning AUP.
- If a member of staff breaches our policy, action will be taken in line with our staff behaviour policy/code of conduct, child protection policy and/ Online Safety Policy.
- If a member of staff is thought to have illegal content saved or stored on a personal mobile or other device or have committed a criminal offence using a personal device or mobile phone, the police will be contacted, and the LADO (Local Authority Designated Officer) will be informed in line with our behaviour/allegations policy.

6. Pupils use of mobile and smart technology

- Safe and appropriate use of mobile and smart technology will be taught to pupils as part of an embedded and progressive safeguarding education approach using age-appropriate sites and resources. Further information is contained within our child protection and relevant specific curriculum policies for example, RSE and Computing.
- Personal mobile or smart technology devices are not permitted on site for children due to their young age.
- If a pupil requires access to personal mobile or smart technology devices in exceptional circumstances, for example medical assistance and monitoring, this will be discussed with the Heads of School and an appropriate risk assessment being put in place prior to use being permitted.
 - Any arrangements regarding access to personal mobile or smart technology devices in exceptional circumstances will be documented and recorded by the school.
 - Any specific agreements and expectations (including sanctions for misuse) will be provided in writing and agreed by the child and their parents/carers before use is permitted.

6.1 Searching, screening and confiscation of electronic devices

Due to our pupils not having mobile and smart tech in school we would not need a Searching, Screening and Confiscation Policy. If in exceptional circumstances a child needs to bring in a mobile device for the reasons listed above and this was needed then the following would apply.

- Where there are any concerns regarding pupils use of mobile or smart technology or policy breaches, they will be dealt with in accordance with our existing policies, including anti-bullying, child protection and behaviour.
- Staff may confiscate a child's/pupils/students' personal mobile or smart technology device if they believe it is being used to contravene our school policies, for example our child protection or behaviour policy.
- Personal mobile or smart technology devices that have been confiscated will be held in a secure place and released to parents/carers.
- Where a concern involves potentially indecent images/videos of children, including images/videos generated by Artificial Intelligence (AI), on a pupils personal mobile or smart technology device, staff will respond in line with our child protection policy; they will confiscate devices, avoid looking at any content and refer the incident to the DSL (or deputy) urgently.
- If there is suspicion that data or files on a pupils personal mobile or smart technology device may be illegal, or may provide evidence relating to a criminal offence, the device will be confiscated and handed over to the police for further investigation.
- If deemed to be necessary and appropriate, searches of personal mobile or smart technology devices may be carried out in accordance with our behaviour policy and the DfE [‘Searching, Screening and Confiscation’](#) guidance.
- Staff will respond in line with our child protection policy and follow the most appropriate safeguarding response if they find images, data or files on a pupil's electronic device that they reasonably suspect are likely to put a person at risk.
- The DSL (or deputy) will always be informed of any searching incidents where authorised members of staff have reasonable grounds to suspect a pupil was in possession of prohibited items, as identified in our behaviour policy.
- The DSL (or deputy) will be involved without delay if staff believe a search of a pupil's personal mobile or smart technology device has revealed a safeguarding risk.
- In exceptional circumstances and in accordance with our behaviour policy ([link](#)) and the DfE [‘Searching, Screening and Confiscation’](#) guidance, the headteacher or authorised members of staff may examine or erase data or files if there is a good reason to do so.
 - In determining whether there is a ‘good reason’ to examine images, data or files, the DSL/Heads of School or an authorised member of staff will need to reasonably suspect that the images, data or files on the device has been, or could be used, to cause harm, undermine the safe environment of the school and disrupt teaching, or be used to commit an offence.
 - In determining whether there is a ‘good reason’ to erase any images, data or files from the device, the member of staff should consider whether the material found may constitute evidence relating to a suspected offence. In those instances, the data or files should not be deleted, and the device must be handed to the police as soon as it is reasonably practicable.
 - If the data or files are not suspected to be evidence in relation to an offence, the headteacher or an authorised member of staff may delete the images, data or files if the continued existence of the data or file is likely to continue to cause harm to any person and the pupil and/or the parent refuses to delete the data or files themselves.
- If the Heads of School/DSL or a member of staff finds any data or files that they suspect might constitute a specified offence, they will be delivered to the police as soon as is reasonably practicable.

7. Visitors' use of mobile and smart technology

- Parents/carers and visitors, including volunteers and contractors, are expected to ensure that:
 - mobile phones and personal devices are not to be used around children or in areas children use and should only be used in permitted specific areas eg staffroom or are only permitted for specific purpose, for example, as part of multi-agency working arrangements.
- Appropriate signage and information are in place as visitors sign in to inform visitors of our expectations for safe and appropriate use of personal mobile or smart technology.
- Visitors, including volunteers and contractors, who are on site for regular or extended periods of time are expected to use mobile and smart technology in accordance with our acceptable use of technology policy and other associated policies, including child protection.
- If visitors require access to mobile and smart technology, for example when working with pupils as part of multi-agency activity, this will be discussed with the Heads of School prior to use being permitted.
 - Any arrangements regarding agreed visitor access to mobile/smart technology will be documented and recorded by the school. This may include undertaking appropriate risk assessments if necessary.
- Members of staff are expected to challenge visitors if they have concerns about their use of mobile and smart technology and will inform the DSL or Heads of School of any breaches of our policy.

8. Policy monitoring and review

- Technology evolves and changes rapidly. St Mildred's will review this policy at least annually. The policy will be revised following any national or local policy updates, any local concerns and/or any changes to our technical infrastructure.
- We monitor internet and technology use taking place via all school provided devices and systems and regularly evaluate online safety mechanisms to ensure this policy is consistently applied. Full information about the appropriate filtering and monitoring systems in place are detailed in our Child Protection Policy and Online Safety Policy. Any issues identified as part of the implementation of our monitoring approaches will be incorporated into our action planning.
- All members of the community will be made aware of how the school will monitor policy compliance through staff training, staff meetings and discussion of relevant policies.

9. Responding to policy breaches

- All members of the community are informed of the need to report policy breaches or concerns in line with existing school policies and procedures. This includes Child Protection. Behaviour and Relationships Policy and Online Safety.
- Where pupils breach this policy:
 - appropriate sanctions and/or pastoral/welfare support will be implemented in line with our behaviour policy.
 - concerns will be shared with parents/carers as appropriate.
 - we will respond in line with our child protection policy, if there is a concern that a child is at risk of harm.
- After any investigations are completed, leadership staff will debrief, identify lessons learnt and implement any policy or curriculum changes, as required.
- We require staff, parents/carers and pupils to work in partnership with us to resolve issues.

- All members of the community will respect confidentiality and the need to follow the official procedures for reporting concerns.
- Parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
- If we are unsure how to proceed with an incident or concern, the DSL (or a deputy) or Heads of School/Executive Head will seek advice from the local authority or other agencies, as appropriate, in accordance with our child protection policy.