St Michael's CE Primary School
Sydenham

Online Safety Policy, including use of mobile phones and social media

Agreed by the Governing Body on: 26th *November 2019*

Signed (Chair): *Beryl Fielder*

Review Date: Autumn 2022

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.
- To ensure the school is in line with statutory requirements.

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Searching, screening and confiscation

It also refers to the Department's guidance on protecting children from radicalisation.
It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so. The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The link governor for safeguarding will regularly meet with appropriate staff to discuss online safety, and monitor online safety concerns logged on MyConcern, as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

Report online safety to governing board, as part of the termly safeguarding report

3.3 The designated safeguarding lead

Details of the school's DSL and deputy are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, Business Manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged on MyConcern and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school's behaviour policy/anti-bullying policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary

This list is not intended to be exhaustive.

3.4 The School Business Manager, in liaison with the IT support company

The School Business Manager, in liaison with the IT support company, is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged on MyConcern and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy/anti-bullying policy
- Users may only access the networks and devices through properly enforced password protections. Passwords are not shared and in the event of a password being compromised that the user's password is immediately reset.

This list is not intended to be exhaustive.

3.5 All staff and volunteers

Staff and volunteers are instructed to always keep professional and private communication separate.

When using personal social media accounts, it is good practice to remember the following:

- Nothing is completely private
- Nothing can be completely deleted
- Staff are not permitted to have parents, carers or children as friends or personal contacts in any social media, unless agreed to by the headteacher.

- Staff are not to engage in any discussion online with parents, carers, or children outside of formal channels. Some parents may feel that it is quicker or easier to raise concerns about their child, etc. via a facebook wall or message board. Parents should be encouraged to use professional and confidential discussion channels for this and staff should not engage in a social media correspondence.
- Personal opinions should not be attributed to the school or local authority and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute.
- Security settings on staff's personal social media profiles should be regularly checked to minimise risk of loss of personal information and to ensure content that is public, is appropriate.

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged, using MyConcern, and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy/anti-bullying policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the end of primary school, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety by running workshops and sharing information on our website and school blog. This policy will also be published on the website.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one

person or group by another person or group, where the relationship involves an imbalance of power. (See also the school anti-bullying policy)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. As part of the school's computing curriculum, as well as the school's bespoke 'Body, Mind & Spirit' curriculum (PSCHE), the teachers will discuss cyber-bullying with the children, and the issue will also be addressed in assemblies.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also share information on cyber-bullying, via the school blog, to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6.4 Cyberbullying involving staff

All forms of bullying, including cyberbullying) should be handled as a community issue for the whole school. It is important that we as a school take measures to prevent and tackle bullying among pupils, but it is equally important that schools make it clear that bullying of staff, whether by pupils, parents or colleagues, is unacceptable.

School leaders, teachers, school staff, parents and pupils all have rights and responsibilities in relation to cyberbullying and should work together to create an environment in which pupils can learn and develop and staff can have fulfilling careers free from harassment and bullying.

We will always aim to foster a good school-parent relationship, as it helps to create an atmosphere of trust that encourages parents to raise concerns in an appropriate manner. We will also offer support to parents on how to help their children engage safely and responsibly with social media, through workshops, advice in our school blog or signposting to other sources of support and advice. Part of this is making sure that parents and carers are aware and understand how to communicate with the school.

It is not acceptable for pupils, parents or colleagues to denigrate and bully school staff via social media in the same way that it is unacceptable to do so face to face. Schools should encourage all members of the school community including parents to use social media responsibly.

Parents have a right to raise concerns about the education of their child, but they should do so in an appropriate manner.

Staff who feel subject to cyber-bullying, should:

- Never respond or retaliate to cyberbullying incidents.
- Report incidents appropriately and seek support from your line manager or a senior member of staff.
- Save evidence of the abuse; take screen prints of messages or web pages and record the time and date.
- Where the perpetrator is known to be a current pupil or colleague, the majority of cases can be dealt with most effectively through the school's own mediation and disciplinary procedures.
- Where the perpetrator is known to be an adult, in nearly all cases, the first action should be for a senior staff member to invite the person to a meeting to address their concerns, and if they have a reasonable complaint, to make sure they know how to raise this appropriately. They can request that the person removes the offending comments. If the perpetrator is a parent or significant member of the community, the person might become subject to the Persistent complaints and harassment policy.
- If they refuse, it should be an organisational decision what to do next – either the school or you could report the matter to the social networking site if it breaches their terms, or seek guidance from the local authority, legal advisers or support from other agencies for example, The UK Safer Internet Centre.
- If the comments are threatening or abusive, sexist, of a sexual nature or constitute a hate crime, you or a representative from the school may consider contacting the local police. Online harassment is a crime whether Staff should never personally engage with cyberbullying incidents amongst other adults. Where appropriate, they should report incidents to the nominated person and/or seek support.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8. Pupils using mobile devices in school

Pupils should not use mobile phones within the school grounds and should not bring in mobile phones (or any other form of recording devise) to school, except where parents have requested permission and signed the disclaimer and consent has been given by the Headteacher. In such circumstances, the child's phone must be kept in the school office until they go home. Even though the phones are kept in the office, the school do not accept responsibility for any lost or stolen phones. Mobile phones are not permitted on school trips or school journeys. *See appendix 4

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Appropriate use of mobile phones by staff

St Michael's recognises that staff may need to have access to mobile phones on site during the working day. However, there are concerns regarding staff having mobile phones and these concerns are mainly based around the following issues:
- Staff being distracted from their work with children
- The inappropriate use of mobile phones, including taking photos or videos of children

The school allows staff to bring into school their mobile phones. However, mobile phones must be kept in their bag or in a cupboard or drawer at all times when children are present and may not be used at any time other than before and after school and break times.

If staff fail to follow this guidance, disciplinary action will be taken in accordance with staff contracts. Staff must ensure that there is no inappropriate or illegal content on the device.

School phones (landline and mobile) must be used for all school purposes including emergency calls. When children undertake a school trip or journey, the school's mobile phone should be used. If more phones are needed, the staff accompanying the group may use their own phone, but for the limited purpose to contact the other adults in the group, the school office or the venues being visited or an emergency number if needs be.

Personal mobile phone technology may not be used to take photographs or videos. Only digital devices that belong to the school should be used to record visual information within the consent criteria guidelines of the local authority and the schools.

10. Ensuring the safe and appropriate use of mobile phones for volunteers& visitors and parents/carers

Upon their initial visit volunteers and visitors are given information regarding the use mobile phones in school. If they wish to make or take an emergency call they may use the schools' phones. Volunteers or visitors are not permitted to take photographs or recordings of the children on their mobile phones.

Parents and carers are not permitted to use their phone for recording/photographs in any situation, including assemblies/performances or school events.
All parents are asked for signed permission for this to occur when their child starts school. On each occasion parents are reminded that under our online safety policy (which they have signed) no photos should be used for any public use or posted on any social media site.

11. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the Business Manager, who will seek advice from the IT support company as appropriate.

Work devices must be used solely for work activities.

12. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, according to the acceptable use agreement (appendices 1 & 2), action will be taken. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct and/or disciplinary policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

13. Social media

13.1 Use of social media at work

Employees must not use social media to express personal viewpoints of School Policy or Headteacher or Governor's decisions.

Employees must limit their use of social media to their official break times such as their lunch break and before and after their normal working hours (unless it is a genuine requirement of the employee's job).

Employees are allowed to access social media websites, which are not blocked by the service provider, from the school's computers or devices at certain times (provided that they are not undertaking overtime).

Employees must limit their use of social media on their own equipment to their official break times, such as their lunch break. They should ensure that use of social media does not interfere with their other duties. The School understands that employees may wish to use their own computers or devices, such as laptops, palm-top and hand-held devices, to access social media websites while they are at work, however must adhere to school policies.

13.2 Monitoring use of social media during work time

Communications using School facilities may be intercepted, recorded and monitored for business use and where appropriate for the detection and prevention of crime. This includes, but is not limited to, telephone calls, internet use, email and post.

The School considers that valid reasons for checking employees' internet usage include suspicions that employees have:

- been using social media websites when he/she should be working; or
- acted in a way that is in breach of the rules set out in this policy.

The School reserves the right to retain information that it has gathered on employees' use of the internet. Employees must note that the majority of social media websites are prohibited through the schools filtering.

13.3 Social media staff's personal life

The School recognises that many employees make use of social media in a personal capacity. While they are not acting on behalf of the School, employees must be aware that they can damage the reputation of the organisation if they are recognised as being one of our employees and are posting text, images (or both) that could be deemed inappropriate.

Employees should use their professional judgment when posting on social media and should review their social media history to ensure that there are no inappropriate historic posts or pictures, which could damage their professional reputation.

Employees should review their social network accounts, particularly the content and privacy settings in place.

Even if an employee does not specifically name the School on social media, it is likely that some viewers will know who they are employed by and as such communications still have the potential to bring the organisation into disrepute.

Employees are allowed to say that they work for the School, which recognises that it is natural for its staff to sometimes want to discuss their work on social media. However, the employee's online profile (for example, the name of a blog or a Twitter name) must not contain the School's name.

If employees do discuss their work on social media (for example, giving opinions on their specialism or the education sector), they should make it evident that any view expressed is their own.

Photographs of pupils and school activities must not be uploaded or shared by employee's through social media.

Any communications that employees make in a personal capacity through social media should be completed with professional judgment and must not:

- have the potential to bring the School into disrepute, for example:
    - by criticising or arguing with parents, colleagues or rivals;
    - by making defamatory comments about individuals or other organisations or groups; or
    - by posting images that are inappropriate or links to inappropriate content;
- breach confidentiality, for example:
    - by sharing confidential information about an individual (such as a colleague or pupils) or the School; or
    - by discussing the School's internal workings (such as future plans that have not been communicated to the public, parents or pupils);
- breach copyright, for example:
    - by using someone else's images or written content without permission;
    - by failing to give acknowledgement where permission has been given to reproduce something; or
- do anything that could be considered discriminatory, bullying or harassment of an individual or group, for example:
    - by making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
    - by using social media to bully or criticise another individual (such as an employee of the organisation); or
    - by posting images that are discriminatory or offensive, or links to such content.

13.4 Disciplinary action over social media misuse

Misuse of social media websites can, in certain circumstances, constitute a criminal offence or otherwise give rise to legal liability against the employee and/or the School. It may also cause embarrassment to the School.

In particular uploading, posting, forwarding or posting a link to any of the following types of material on a social media website or via email, whether in a professional or personal capacity, will amount to gross misconduct:

- pornographic material;
- a knowingly false or defamatory statement about any person or organisation;
- material which is potentially offensive, obscene, discriminatory, derogatory or may cause embarrassment to the School, or its staff;
- online bullying of colleagues (see also section 6, Cyber Bullying);
- promotion of radicalisation and extremism;
- confidential information about the School, any of our staff or pupils (for which there is no express authority to disseminate);
- any other statement which is likely to create any liability (criminal or civil);
- material which breaches copyright or other intellectual property rights, or which invades the privacy of any person.

Any such action will be addressed under the Schools Disciplinary Procedure and is likely to result in summary dismissal.

Where evidence of misuse is found the School may undertake a more detailed investigation in accordance with its Disciplinary Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the investigation. If necessary such information may be handed to the police in connection with a criminal investigation.

Any use of social media by other members of staff in breach of this policy must be reported to the Headteacher. If a breach is made by the Headteacher, this should be reported to the chair of Governors.

14. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and deputy will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

15. Monitoring arrangements

The DSL oversees logging the behaviour and safeguarding issues related to online safety, using MyConcern/Scholarpack.

This policy will be reviewed every three years. At every review, the policy will be shared with the governing board.

16. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff code of conduct and disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

EYFS & KS1: Think before you click
Responsible Internet Use Agreement

PUPIL _____

THINK BEFORE YOU CLICK

S

A

F

E

When I use the school's ICT systems (like the i-pads) and get onto the internet in school I will:

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
    - I click on a website by mistake
    - I receive messages from people I don't know
    - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- I will be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends.
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Pupil's Agreement

I have read and understood "Think before you click". I will use Internet in a responsible way and follow these rules at all times.

Signed: _____ Date: _____

Parents'/Carers' Consent

Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed: _____ Date: _____

KS2: Think before you click
Responsible Internet Use Agreement

PUPIL _____

THINK BEFORE YOU CLICK

S

A

F

E

When I use the school's ICT systems, like the i-pads and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Pupil's Agreement

I have read and understood "Think before you click". I will use Internet in a responsible way and follow these rules at all times.

Signed: _____ Date: _____

Parents'/Carers' Consent

Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed: _____ Date: _____

Appendix 3: **Acceptable use agreement (staff, governors, volunteers and visitors)**

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school
- Use the school's resources, such as printers, solely for school purposes

- ❖ I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.
- ❖ I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.
- ❖ I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.
- ❖ I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.
- ❖ I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4: Sample of letter to be sent home

Dear Parents,

At St Michael's we understand that when children walk to school or walk home alone, parents would want contact with their child via a phone. Therefore we will give permission in such circumstances, but on the following conditions:

- If the phone has internet access, it should not be accessed on school premises.
- Even though the phones will be stored in the office during the day, the school accepts no responsibility if it is lost or stolen.
- Phones must not be heard or seen on the school playground, or it will be confiscated.

To obtain authorisation, parents must please provide the reason of why your child needs a phone. Unless we have a child's name authorised, phones found on children will be confiscated for a whole term. Children, who are authorised to have phones, but do not follow the rules, will be banned from bringing phones into school and their phones will be confiscated. If you would like to ask permission for your child to bring a phone to school, please complete the form. You need to complete a new application for this year; if you had permission last year, you still need to complete the form. We ask your support in this matter.

Name of child:_____ Year:_____

Reason for why the child must bring a phone to school:

Parent's consent form

*I understand that my child may use a phone that has no internet/data access and if it comes to the school's knowledge that the phone has internet access, the child will be banned from having a phone in school.
*I understand it is my responsibility to ensure my child understands how to use a phone appropriately and as a parent I will regularly monitor their messages and camera roll.
*I understand and accept that if my child phone is seen or heard on school site the phone will be confiscated and he/she will be banned from bringing any other phone to school.
*I understand and accept that if the school has any evidence that my child uses their phone inappropriately whilst wearing school uniform the phone will be confiscated and he/she will be banned from bringing any other phone to school.
*I understand that if my child does not hand in his phone at the beginning of the day, the phone will be confiscated and he/she will be banned from bringing any other phone to school.
*I understand that the school accepts no responsibility if the phone gets lost or stolen.

Signed
Parent: _____ Pupil: _____ Date: _____

To be returned to parent

Name of child: _____
Your child has been authorised/has not been authorised to bring a phone to school.