St Michael's C of E Primary School

Online Safety Policy

2017-18

This policy is part of the School's Statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes.

Contents

Appendices:

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at St Michael's C of E Primary school with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community.
- Have clear structures to deal with online abuse such as online bullying [noting that these need to be cross referenced with other school policies].
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

Scope

This policy applies to all members of St Michael's C of E Primary school community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school IT systems, both in and out of St Michael's C of E Primary school.

Roles and responsibilities

Role	Key Responsibilities
Head of School Clare Dyson	• Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance • To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding. • To take overall responsibility for online safety provision • To take overall responsibility for data management and information security (SIRO) ensuring school's provision follows best practice in information handling • To ensure the school uses appropriate IT systems and services including, filtered Internet Service, e.g. LGfL services • To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles • To be aware of procedures to be followed in the event of a serious online safety incident • Ensure suitable 'risk assessments' undertaken so the curriculum meets needs of pupils, including risk of children being radicalised • To receive regular monitoring reports from the Online Safety Co-ordinator • To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures, e.g. network manager • To ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety • To ensure school website includes relevant information.
Online Safety Co-ordinator **Clare Dyson** Designated Child Protection Lead **Clare Dyson and Tessa Harding**	• Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents • Promote an awareness and commitment to online safety throughout the school community • Ensure that online safety education is embedded within the curriculum

Role	Key Responsibilities
	• Liaise with school technical staff where appropriate • To communicate regularly with SLT and the designated online safety Governor/committee to discuss current issues, review incident logs and filtering/change control logs • To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident • To ensure that online safety incidents are logged as a safeguarding incident • Facilitate training and advice for all staff • Oversee any pupil surveys / pupil feedback on online safety issues • Liaise with the Local Authority and relevant agencies • Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns.
Governors Safeguarding governor **Judy Powell**	• To ensure that the school has in place policies and practices to keep the children and staff safe online • To approve the Online Safety Policy and review the effectiveness of the policy • To support the school in encouraging parents and the wider community to become engaged in online safety activities • The role of the online safety Governor will include: regular review with the online safety Co-ordinator.
Computing Curriculum Leader **Michelle Bessant**	• To oversee the delivery of the online safety element of the Computing curriculum

Network Manager /technician
 	
Jack Rice
	• To report online safety related issues that come to their attention, to the Online Safety Coordinator
	• To manage the school's computer systems, ensuring:
	  ○ school password policy is strictly adhered to.
	  ○ systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date)
	  ○ access controls/encryption exist to protect personal and sensitive information held on school-owned devices
	  ○ the school's policy on web filtering is applied and updated on a regular basis
	• That they keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant

Role	Key Responsibilities
	• That the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the online safety co-ordinator/Headteacher • To ensure appropriate backup procedures and disaster recovery plans are in place • To keep up-to-date documentation of the school's online security and technical procedures
Data and Information (Asset Owners) Managers (IAOs) **Camdens ICT Service (Colin Small)**	• To ensure that the data they manage is accurate and up-to-date • Ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements. • The school must be registered with Information Commissioner
LGfL Nominated contact(s)	• To ensure all LGfL services are managed on behalf of the school following data handling procedures as relevant
Teachers	• To embed online safety in the curriculum • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff, volunteers and contractors.	• To read, understand, sign and adhere to the school staff Acceptable Use Agreement/Policy, and understand any updates annually. The AUP is signed by new staff on induction. • To report any suspected misuse or problem to the online safety coordinator • To maintain an awareness of current online safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology **Exit strategy** • At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.

Role	Key Responsibilities
Pupils	• Read, understand, sign and adhere to the Pupil Acceptable Use Policy annually • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology • To understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school • To contribute to any 'pupil voice' / surveys that gathers information of their online experiences
Parents/carers	• To read, understand and promote the school's Pupil Acceptable Use Agreement with their child/ren • to consult with the school if they have any concerns about their children's use of technology • to support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images
External groups including Parent groups	• Any external individual/organisation will sign an Acceptable Use agreement prior to using technology or the Internet within school • to support the school in promoting online safety • To model safe, responsible and positive behaviours in their own use of technology.

Communication:

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website, staffroom.
- Policy to be kept in teacher's computing curriculum folders in each classroom.
- Policy to be part of school induction pack for new staff.
- Regular updates and training on online safety for all staff.
- Acceptable use agreements discussed with staff and pupils at the start of each year. Acceptable use agreements to be issued to whole school community, on entry to the school.

Handling Incidents:

- The school will take all reasonable precautions to ensure online safety.

- Staff and pupils are given information about infringements in use and possible sanctions.
- Online Safety Coordinator acts as first point of contact for any incident.
- Any suspected online risk or infringement is reported to Online Safety Coordinator that day
- Any concern about staff misuse is always referred directly to the Head of school, unless the concern is about the Head of School in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

Handling a sexting / nude selfie incident:

UKCCIS "Sexting in schools and colleges" should be used (see appendix). This extract gives the initial actions that should be taken. Any member of staff who suspects an incident of sexting / nude selfies should refer this immediately to the Head of School or online safety coordinator.

There should always be an initial review meeting, led by the DSL. This should consider the initial evidence and aim to establish:

- Whether there is an immediate risk to a young person or young people
  When assessing the risks the following should be considered:
    - Why was the imagery shared? Was the young person coerced or put under pressure to produce the imagery?
    - Who has shared the imagery? Where has the imagery been shared? Was it shared and received with the knowledge of the pupil in the imagery?
    - Are there any adults involved in the sharing of imagery?
    - What is the impact on the pupils involved?
    - Do the pupils involved have additional vulnerabilities?
    - Does the young person understand consent?
    - Has the young person taken part in this kind of activity before?
- If a referral should be made to the police and/or children's social care
- If it is necessary to view the imagery in order to safeguard the young person – in most cases, imagery should not be viewed
- What further information is required to decide on the best response
- Whether the imagery has been shared widely and via what services and/or platforms. This may be unknown.
- Whether immediate action should be taken to delete or remove images from devices or online services
- Any relevant facts about the young people involved which would influence risk assessment
- If there is a need to contact another school, college, setting or individual

- Whether to contact parents or carers of the pupils involved - in most cases parents should be involved

An immediate referral to police and/or children's social care should be made if at this initial stage:

1. The incident involves an adult
2. There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example owing to special educational needs)
3. What you know about the imagery suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. The imagery involves sexual acts and any pupil in the imagery is under 13
5. You have reason to believe a pupil or pupil is at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self-harming

If none of the above apply, then a school may decide to respond to the incident without involving the police or children's social care (a school can choose to escalate the incident at any time if further information/concerns come to light).

The decision to respond to the incident without involving the police or children's social care would be made in cases when the DSL is confident that they have enough information to assess the risks to pupils involved and the risks can be managed within the school's pastoral support and disciplinary framework and if appropriate local network of support.

Reviewing and Monitoring Online Safety

The online safety policy is referenced within other school policies (e.g. Safeguarding and Child Protection policy, Anti-Bullying policy, PSHE, Computing policy).

- The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school online safety policy will be disseminated to all members of staff and pupils.

2. Education and Curriculum

Pupil online safety curriculum

This school:

- has a clear, progressive online safety education programme as part of the Computing curriculum, PSHE and other curriculum areas as relevant. This covers a range of skills and behaviours appropriate to their age and experience;
- plans online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- will remind pupils about their responsibilities through the pupil Acceptable Use Agreement(s);
- ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright;
- ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- ensure pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments.

Staff and governor training

This school:

- makes regular training available to staff on online safety issues and the school's online safety education program;
- provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the Online Safety Policy and the school's Acceptable Use Agreements.

Parent awareness and training

This school:

- provides induction for parents which includes online safety;
- runs a rolling programme of online safety advice, guidance and training for parents.

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements;
- understand the significance of misuse or access to inappropriate materials and are aware of the consequences;
- understand it is essential to reporting abuse, misuse or access to inappropriate materials and know how to do so;
- understand the importance of adopting good online safety practice when using digital technologies in and out of school;
- know and understand school policies on the use of mobile and hand held devices including cameras;

Staff, volunteers and contractors

- know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils;

Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the online safety acceptable use agreement form;
- should know and understand what the school's 'rules of appropriate use for the whole school community' are and what sanctions result from misuse.

Incident Management

In this school:

- there is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions;
- all members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes;
- support is actively sought from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issues;
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school;
- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;
- we will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

4. Managing IT and Communication System

Internet access, security (virus protection) and filtering

This school:

- informs all users that Internet/email use is monitored;
- has the educational filtered secure broadband connectivity through the LGfL;
- uses the LGfL filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- uses USO user-level filtering where relevant;
- ensures network health through use of Sophos anti-virus software (from LGfL);
- Uses DfE, LA or LGfL approved systems including DfE S2S to send 'protect-level' (sensitive personal) data over the Internet
- Uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site;
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect pupils.

Network management (user access, backup)

This school

- Uses individual, audited log-ins for all users - the LGfL USO system;
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services;
- Has additional local network monitoring/auditing software installed;
- Ensures the Systems Administrator/network manager is up-to-date with LGfL services and policies/requires the Technical Support Provider to be up-to-date with LGfL services and policies;
- Has daily back-up of school data (admin and curriculum);
- Uses secure, 'Cloud' storage for data back-up that conforms to DfE guidance;
- Storage of all data within the school will conform to the EU and UK data protection requirements; Storage of data online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's online safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. The same credentials are used to access the school's network. We also provide a different username and password for access to our school's network;

- All pupils have their own unique username and password which gives them access to the Internet and other services;
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to log off when they have finished working or are leaving the computer unattended;
- Ensures all equipment owned by the school and/or connected to the network has up to date virus protection;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used primarily to support their professional responsibilities.
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies; e.g. Borough email or Intranet; finance system, Personnel system etc.
- Maintains equipment to ensure Health and Safety is followed;
- Ensures that access to the school's network resources from remote locations by staff is audited and restricted and access is only through school/LA approved systems:
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems;
- Has a clear disaster recovery system in place that includes a secure, remote off site back up of data;
- This school uses secure data transfer; this includes DfE secure S2S website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted.
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards;

Password policy

- This school makes it clear that staff and pupils must always keep their passwords private, must not share with others; If a password is compromised the school should be notified immediately.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.
- We require staff to use strong passwords.

- We require staff to change their passwords into the MIS, LGfL USO admin site, every 90 days.
- We require staff using critical systems to use two factor authentication.

E-mail

This school

- Provides staff with an email account for their professional use, London Staffmail/LA email and makes clear personal email should be through a separate account;
- We use anonymous or group e-mail addresses, for example info@schoolname.la.sch.uk/head@schoolname.la.sch.uk/.
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- We use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses.

Pupils:

- We use LGfL pupil email system which are intentionally 'anonymised' for pupil protection.
- Pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home.

Staff:

- Staff will use LGfL e-mail systems for professional purposes.
- Access in school to external personal e-mail accounts may be blocked.
- Never use email to transfer staff or pupil personal data. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

School website

- The Head of School, supported by the Governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- The school web site complies with statutory DFE requirements;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- Photographs published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;

Cloud Environments

- Uploading of information on the schools' online learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;
- Photographs and videos uploaded to the school's online environment will only be accessible by members of the school community;
- In school, pupils are only able to upload and publish within school approved 'Cloud' systems.

Social networking

Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.
- Teachers are instructed not to run social network spaces for pupil use on a personal basis or to open up their own spaces to their pupils, but to use the schools' preferred system for such communications.

School staff will ensure that in private use:

- No reference should be made in social media to pupils, parents/ carers or school staff;
- School staff should not be online friends with any pupil.
- They do not engage in online discussion on personal matters relating to members of the school community;
- 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 personal social media profiles are regularly checked to minimise risk of loss of personal information.

Pupils:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Pupils are required to sign and follow our [age appropriate] pupil Acceptable Use Agreement.

Parents:

- Parents are reminded about social networking risks and protocols through our parental Acceptable Use Agreement and additional communications materials when required.
- Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

CCTV – please delete if your school does not have a CCTV system

- We have CCTV in the school as part of our site surveillance for staff and pupil safety. The use of CCTV is clearly signposted in the school. We will not reveal any recordings without appropriate permission.
- We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

5. Data security

Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are. We have listed the information and information asset owners.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in a single central record

Technical Solutions

- Staff have secure area(s) on the network to store sensitive files.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes' idle time.
- We use the LGfL USO Auto Update, for creation of online user accounts for access to broadband services and the LGfL content.
- All servers are in lockable locations and managed by DBS-checked staff.
- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.
- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.
- We are using secure file deletion software.

6. Equipment and Digital Content

Mobile Devices (Mobile phones, tablets and other mobile devices)

- Mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile devices.

Pupils' use of personal devices

- No pupil should bring his or her mobile phone or personally-owned device into school. Any device brought into school will be confiscated and kept in the school office until the pupil's parent/ carer collects the phone from the school office.
- In exceptional circumstances pupils can request permission from the Head of School to bring their phone into school. If this is granted pupil's phones will be securely stored in the office during the school day. Pupil's will not be able to access their phone during the school day.

Staff use of personal devices

- The Executive Head Teacher, Head of School and Assistant Head may use their mobile phones during the school day.
- All other staff and visitors may not use their mobile telephones on school premises other than in the staffroom during the school day.
- Staff should never use personally-owned devices, such as mobile phones or cameras, to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Digital images and video

In this school:

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils;
- The school blocks/filter access to social networking sites unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their computing scheme of work;

- Pupils are advised to be very careful about placing any personal photos on any ‘social’ online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

APPENDIX 1

ACCEPTABLE USE AGREEMENT FOR STAFF, VOLUNTEERS AND GOVERNORS

Access and professional use

- All computer networks and systems belong to the school and are made available to staff for educational, professional and administrative purposes only.
- Staff are expected to abide by all school online safety rules and the terms of this acceptable use policy. Failure to do so may result in disciplinary action being taken.
- Staff should only take pictures of children on school cameras and these should only be downloaded on to the school system (no pictures on personal cameras or mobile phones).
- The school reserves the right to monitor internet activity and examine and delete files from the school's system.
- Staff have a responsibility to safeguard pupils in their use of the internet and to report all online safety concerns to the online safety contact officer or Head of School.
- Copyright and intellectual property rights in relation to materials used from the internet must be respected.
- E-mails and other written communications must be carefully written and polite in tone and nature.
- Anonymous messages and the forwarding of chain letters are not permitted.
- Staff should only access approved internet sites. The use of chat rooms or social networking sites is not allowed.

Data protection and system security

- Staff should ensure that any personal data sent over the internet will be encrypted or sent via secure systems. Where personal data is taken off the school premises via laptops and other mobile systems, the information must be encrypted beforehand.
- Use school USB sticks to transport data. Encrypted memory sticks will be provided to each teacher, these remain the property of the school and must be returned to the school on leaving.
- Downloading executable files or unapproved system utilities will not be allowed and all files held in the cloud will be regularly checked.
- Sharing and use of other people's log-ins and passwords is forbidden. Users should ensure that they log-out when they have finished using a computer terminal.
- Files should be saved, stored and deleted in line with the school policy.

Personal use

- Staff should not browse, download or send material that could be considered offensive to colleagues and pupils or is illegal.
- Staff should not allow school equipment or systems to be used or accessed by unauthorised persons and keep any computers or hardware used at home safe.

- Staff should ensure that personal websites or blogs do not contain material that compromises their professional standing or brings the school's name into disrepute.

I have read the above policy and agree to abide by its terms.

Name: _____

School: _____

Signed: _____

Date: _____

APPENDIX 2:
ACCEPTABLE USE AGREEMENT FOR PRIMARY SCHOOL PARENTS AND PUPILS

Name:

School:

Class:

I want to stay safe while I am using a computer and I know that anything I do on the computer may be seen by someone else.

I will:

- keep my password a secret;
- only open pages which my teacher has said are okay;
- tell my teacher if anything makes me feel scared or uncomfortable;
- make sure all the messages I send are polite;
- tell my teacher if I get a nasty message;
- not reply to any nasty message which makes me feel upset or uncomfortable;
- not give my mobile number, home number or address to anyone who is not a real friend;
- only email people I know or if my teacher agrees;
- only use my school email address;
- talk to my teacher before using anything on the internet;
- not tell people about myself on-line (I will not tell them my name, anything about where I live or where I go to school);
- not load photographs of myself onto the computer;
- never agree to meet a stranger.

Parents

- I have read the above school rules for responsible internet use and agree that my child may have access to Fronter. I understand that the school will take all reasonable precautions to ensure pupils do not have access to inappropriate websites, and that the school cannot be held responsible if pupils do access inappropriate websites.
- I agree that my child's work can be published on the school website.
- I agree that photographs that include my child may be published but that any photography will not clearly identify my child and that their name will not be published.

Signed:

Date:

APPENDIX 2:

PROTOCOL FOR RESPONDING TO ONLINE SAFETY INCIDENTS – HANDLING INFRINGEMENTS

Policy: How will infringements be handled?
Whenever a pupil or staff member infringes the Online-Safety Policy, the final decision on the level of sanction will be at the discretion of the school management and will reflect the school's behaviour and disciplinary procedures.

PUPIL	
Category A infringements	**Possible Sanctions:**
• Use of non-educational sites during lessons • Unauthorised use of email • Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends • Use of unauthorised instant messaging / social networking sites	**Refer to class teacher / tutor** Escalate to: senior manager / Online-Safety Coordinator / Head of School
Category B infringements	**Possible Sanctions:**
• Continued use of non-educational sites during lessons after being warned • Continued unauthorised use of email after being warned • Continued unauthorised use of mobile phone (or other new technologies) after being warned • Continued use of unauthorised instant messaging / chatrooms, social networking sites, NewsGroups • Use of Filesharing software e.g. Napster, Vanbasco, BitTorrent, LiveWire, etc • Trying to buy items over online • Accidentally corrupting or destroying others' data without notifying a member of staff of it • Accidentally accessing offensive material and not logging off or notifying a member of staff of it	**Refer to Class teacher/ Head of School / Online-Safety Coordinator** Escalate to: removal of Internet access rights for a period / removal of phone until end of day / contact with parent]
PUPIL	
Category C infringements	**Possible Sanctions:**
• Deliberately corrupting or destroying someone's data, violating privacy of others or posts inappropriate messages, videos or images on a social networking site. • Sending an email or MSN message that is regarded as harassment or of a bullying nature (one-off) • Trying to access offensive or pornographic material (one-off) • Purchasing or ordering of items online • Transmission of commercial or advertising material	**Refer to Class teacher / Head of School / Online-Safety Coordinator / removal of Internet and/or Learning Platform access rights for a period** Escalate to: contact with parents / removal of equipment **Other safeguarding actions if inappropriate web material is accessed:** Ensure appropriate technical support filters the site

Category D infringements	Possible Sanctions:
• Continued sending of emails or MSN messages regarded as harassment or of a bullying nature after being warned • Deliberately creating accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent • Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988 • Bringing the school name into disrepute	**Refer to Head of School / Contact with parents** **Other possible safeguarding actions:** • Secure and preserve any evidence • Inform the sender's e-mail service provider. • Liaise with relevant service providers/ instigators of the offending material to remove • Report to Police / CEOP where child abuse or illegal activity is suspected

STAFF	
Category A infringements (Misconduct)	**Possible Sanctions:**
• Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc. • Use of personal data storage media (e.g. USB memory sticks) without considering access and appropriateness of any files stored. • Not implementing appropriate safeguarding procedures. • Any behaviour on the World Wide Web that compromises the staff members professional standing in the school and community. • Misuse of first level data security, e.g. wrongful use of passwords. • Breaching copyright or license e.g. installing unlicensed software on network.	**Referred to / Head of School** Escalate to: *Warning given*
Category B infringements (Gross Misconduct)	**Possible Sanctions:**
• Serious misuse of, or deliberate damage to, any school / Council computer hardware or software; • Any deliberate attempt to breach data protection or computer security rules; • Deliberately creating ,accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent; • Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988; • Bringing the school name into disrepute	**Referred to Head of School / Governors;** **Other safeguarding actions:** ▪ Remove the PC to a secure place to ensure that there is no further access to the PC or laptop. ▪ Instigate an audit of all ICT equipment by an outside agency, such as the schools ICT managed service providers - to ensure there is no risk of pupils accessing inappropriate materials in the school. ▪ Identify the precise details of the material.

	Escalate to: *report to LA /LSCB, Personnel, Human resource.* Report to Police / CEOP where child abuse or illegal activity is suspected.

If a member of staff commits an exceptionally serious act of gross misconduct

The member of staff should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

Schools are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Local Authority Human Resources team.

Child abuse images found

In the case of Child abuse images being found, the member of staff should be **immediately suspended** and the Police should be called.

Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP):

http://www.ceop.gov.uk/reporting_abuse.html

http://www.iwf.org.uk

How will staff and pupils be informed of these procedures?

- They will be fully explained and included within the school's Online Safety Policy. All staff will be required to sign the school's online-safety acceptable use agreement form;
- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'. Pupils will sign an age appropriate online-safety / acceptable use agreement form;
- The school's online safety policy will be made available and explained to parents, and parents will sign an acceptance form when their child starts at the school.
- Information on reporting abuse / bullying etc will be made available by the school for pupils, staff and parents.

APPENDIX 4:
ONLINE SAFETY INCIDENT REPORT FORM

This form should be kept on file and a copy emailed to Camden's online safety officer at jenni.spencer@camden.gov.uk

School/organisation's details:

Name of school/organisation: St Michael's C of E Primary school

Address: 88 Camden St, London, NW1 0JA

Name of online safety co-ordinator: Clare Dyson

Contact details: c.dyson@stmichaels.camden.sch.uk 0207 485 8965

Details of incident

Date happened:

Time:

Name of person reporting incident:

If not reported, how was the incident identified?

Where did the incident occur?
□ In school/service setting □ Outside school/service setting

Who was involved in the incident?
□ child/young person □ staff member □ other (please specify

Type of incident:
□ bullying or harassment (online bullying)
□ deliberately bypassing security or access
□ hacking or virus propagation
□ racist, sexist, homophobic religious hate material
□ terrorist material
□ online grooming
□ online radicalisation
□ child abuse images
□ on-line gambling
□ soft core pornographic material
□ illegal hard core pornographic material
□ other (please specify)

Description of incident

Nature of incident

Deliberate access

Did the incident involve material being;
□ created □ viewed □ printed □ shown to others
□ transmitted to others □ distributed

Could the incident be considered as;
□ harassment □ grooming □ online bullying □ breach of AUP

Accidental access

Did the incident involve material being;
□ created □ viewed □ printed □ shown to others
□ transmitted to others □ distributed

Action taken

Staff

□ incident reported to head teacher/senior manager
□ advice sought from LADO
□ referral made to LADO
□ incident reported to police
□ incident reported to Internet Watch Foundation
□ incident reported to IT
□ disciplinary action to be taken
□ online safety policy to be reviewed/amended

Please detail any specific action taken (ie: removal of equipment)

Child/young person

□ incident reported to head teacher/senior manager
□ advice sought from Children's Safeguarding and Social Work
□ referral made to Children's Safeguarding and Social Work
□ incident reported to police
□ incident reported to social networking site
□ incident reported to IT
□ child's parents informed
□ disciplinary action to be taken
□ child/young person debriefed
□ online safety policy to be reviewed/amended

Outcome of incident/investigation

APPENDIX 5:
DESCRIPTION OF ICT APPLICATIONS

	Benefits	**Risks**
Internet	• Enables the storage, publication and retrieval of a vast range of information. • Supports communications systems. • Provides access to a wide range of educational materials, information and resources to support learning. • Enables pupils and staff to communicate widely with others. • Enhances school's management information and business administration systems.	• Information is predominantly for an adult audience and may be unsuitable for children. • The vast array of information makes retrieval difficult without good research skills and ability to critically evaluate information. • Access to sites promoting illegal or anti-social activities, extreme views or commercial and gambling sites.
Email	• Allows written communications over the network and the ability to attach documents. • Enables exchange of information and ideas and supports collaborative working. • Enhances written communications skills. • A good form of communication for children with some disabilities.	• Difficulties controlling contacts and content. • Use as a platform for bullying and harassment. • Risks from unwanted spam mail, particularly for fraudulent purposes or to introduce viruses to systems. • Hacking. • Unsolicited mail.
Chat/instant messaging	• Chat rooms allow users to chat on-line in real time in virtual meeting places with a number of people; • Instant messaging allows real-time chat for 2 people privately with no-one else able to join. Users have control over who they contact through "buddy lists".	• Anonymity means that children are not aware of who they are really talking to. • Chat rooms may be used by predatory adults to contact, groom and abuse children on- line. • Risk of children giving away personal information that may identify or locate them. • May be used as a platform to bully or harass.

	• Enhances social development by allowing children to exchange experiences and ideas and form friendships with peers. • Use of pseudonyms protects the child's identity. • Moderated chat rooms can offer some protection to children. •	
Social networking sites	• On-line communities, including blogs and podcasts, where users can share text, photos and music with others by posting items onto the site and through messaging. • It allows creation of individual profiles. • Users can develop friends lists to allow access to individual profiles and invite comment. • Allows children to network with peers and join forums to exchange ideas and resources. • It provides a creative outlet and improves ICT skills.	• Open access means children are at risk of unsuitable contact. • Risk of children posting unsuitable material on-line that may be manipulated to cause them embarrassment or distress. • Children may post personal information that allows them to be contacted or located. • May be used as a platform to bully or harass.
File sharing (peer-to-peer networking)	• Allows users to share computer capability, networks and file storage. • Used to share music, video and other materials. • Allows children to network within a community of peers with similar interests and exchange materials.	• Illegal download and copyright infringement. • Exposure to unsuitable or illegal materials. • Computers are vulnerable to viruses and hacking.
Mobile phones and multi-media equipment	• Mobile phones now carry other functions such as cameras, video-messaging and access to internet and email. • Provide children with a good means of communication and entertainment.	• Their mobile nature makes supervision of use difficult leading to risks of unsuitable contacts or exposure to unsuitable material on the internet or through messaging. • Risk from violent crime due to theft. • Risk of cyberbullying via mobile phones.

	• They can also keep children safe and allow them to be contacted or stay in contact.	