ONLINE SAFETY POLICY

Policy date: Spring 2024 **Policy review: Spring 2025**

Member of Staff Responsible: Mrs S Graham
Governor: Mrs C Struzzo

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

- School website
- Cloud Environment
- Social networking
- Staff, Volunteers and Contractors
- Pupils
- Parents
- CCTV

5. Data Security
    - Management Information System access
    - Technical Solutions
6. Equipment and Digital Content
    - Personal mobile phones and devices
    - Digital images and video

Appendices (separate documents): (check the BucksGfL web site for the most recent list http://os.BucksGfL.net)

A1: Online Safety Contacts & Resources

A2: Response to an incident of concern

A3: SMAS Incident Log

A4: Pupil acceptable use policy

A5: Staff, Governor & Volunteer acceptable use policy

A6: External photograph contract

1. Introduction and Overview

St Mary and All Saints CE Primary School believes that the use of information and communication technologies in schools brings great benefits. Recognising the Online Safety issues and planning accordingly will help to ensure appropriate, effective and safer use of electronic communications.

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

Breaches of an Online Safety policy can lead to civil, disciplinary and criminal action being taken against staff, pupils and members of the wider school community. It is crucial that we are aware of the offline consequences that online actions can have.

- The school has appointed an Online Safety Coordinator to lead on Online Safety, Mrs S Graham, School's IT Manager. She will work closely with the school's Designated Safeguarding Lead. The DSL must be made aware of any disclosures, incidents or Child Protection concerns.

- The Governing Body will review the Online Safety policy and its implementation regularly. They will take responsibility for revising the Online Safety policy and practice where necessary (such as after an incident or change in national legislation). Mr Bob Mason as the governor responsible for child safety, has been appointed to take lead responsibility for Online Safety within the Governing Body.

- The Online Safety Policy relates to other policies including the Child Protection, Positive Behaviour Policy, all subject policies and the School Improvement Plan and replaces the Internet Policy.

- Parents are requested to sign an Online Safety/Internet agreement as part of the Home School Agreement.

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at St Mary & All Saints CE 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 students.

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 Mary & All Saints CE Primary School community (including staff, students/pupils, volunteers, parents/carers, visitors, community users)

who have access to and are users of St Mary & All Saints CE Primary School IT systems, both in and out of St Mary's Church of England Primary School

Roles and responsibilities

Role	Key Responsibilities
Headteacher (Jenny Barnett)	• 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. Securly 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.

Role	Key Responsibilities
Online Safety Co-ordinator/Designated Child Protection Lead (Sam Graham, Jenny Barnett, Annemarie Philpott and Kathryn Olive)	• 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 • 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 (including online safety) (Claudia Strauzzo)	• 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 (Emily Moss)	• To oversee the delivery of the online safety element of the Computing curriculum

Role	Key Responsibilities
IT/Network Manager (Sam Graham)	• 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) - 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 • 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 (Tina Massie)	• 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
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

Role	Key Responsibilities
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.
Pupils	• Read, understand, sign and adhere to the Student/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

Role	Key Responsibilities
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 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 Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

Review and Monitoring

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 students 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 on the school website.

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, BucksGfL, 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 secure filtering through Securly
- broadband connectivity through Swish
- uses Securly 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 encrypted devices or secure remote access where staff need to access 'protect-level '(sensitive personal) data off-site;
- Works in partnership with Turn IT On to ensure any concerns about the system are communicated so that systems remain robust and protect students.

Network management (user access, backup)

This school

- Uses individual, audited log-ins for all users.
- Uses guest accounts occasionally for external or short-term visitors for temporary access to appropriate services.
- 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.
- 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.
- Maintains equipment to ensure Health and Safety is followed;

- 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;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX);
- 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;

Monitoring

- The school employs monitoring tools to track internet usage.
- Monitoring is conducted to identify inappropriate content, potential security threats, and adherence to school policies.
- Monitoring is transparent, and users are made aware of this practice.

Filtering

- A robust web filtering system is implemented to block access to inappropriate or harmful content.
- The filtering system is regularly updated to adapt to emerging online threats.
- Exceptions to filtering policies require explicit authorisation from the designated authority.

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 twice a year.
- 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 and makes clear personal email should be through a separate account;
- 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.
- We use a number of technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses.

Staff:

- Staff will use Microsoft Outlook 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 Headteacher, 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

- 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

- Within the school environment access to social media and social networking sites will be part of filtering.

- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location systems.

  - Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.

  - Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.

  - Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupil will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.

  - All members of the school community will be advised not to publish specific and detailed private thoughts, especially those that may be considered confidential, sensitive, threatening, hurtful or defamatory.

- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.

- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction.

- Safe and professional behaviour will be outlined in the school Code of Conduct and the Staff, Governor & Volunteer Acceptable Use Policy (Appendix 5)

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 student use on a personal basis or to open up their own spaces to their students, but to use the schools 'preferred system for such communications.
- for the use of any school approved social networking will adhere to school's communications policy.

School staff will ensure that in private use:

- No reference should be made in social media to students/pupils, parents/carers or school staff;
- School staff should not be online friends with any pupil/student. Any exceptions must be approved by the Headteacher.
- 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 /academy 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.
- Students 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

- We have CCTV in the school as part of our site surveillance for staff and student safety. The use of CCTV is clearly signposted in the school. We will not reveal any recordings without appropriate permission.

5. Data security: Management Information System access and Data transfer

Strategic and operational practices

At this school:

- The Chair of Governors 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.
- All servers are 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 into school are entirely at the staff member, students & parents or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- 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.
- Mobile devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets.
- Personal mobile devices will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from Headteacher / SLT.
- Student personal mobile devices, which are brought into school, must be turned off (not placed on silent) and handed into the class teacher on arrival at school for collection at the end of the school day.
- The Bluetooth or similar function of a mobile device should be switched off at all times and not be used to send images or files to other mobile devices.
- Personal mobile devices will only be used during lessons with permission from the teacher.
- No images or videos should be taken on mobile devices without the prior consent of the person or people concerned.
- Staff members may use their phones during school break times.
- All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any personal mobile device is to be avoided, except where it has been explicitly agreed by the Headteacher. Such authorised use is to be recorded. All mobile device use is to be open to monitoring scrutiny and the Headteacher is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary.
- Where permission has been given to record video footage or photographs on a personal device, this must be deleted upon transferral of the data to the school shared drive or after the specified time.
- The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying.
- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.

Storage, Synching and Access

The device is accessed with a school owned account

- The device has a school created account and all apps and file use is in line with this policy. No personal elements may be added to this device.
- PIN access to the device must always be known by the network manager.

The device is accessed with a personal account

- If personal accounts are used for access to a school owned mobile device, staff must be aware that school use will be synched to their personal cloud, and personal use may become visible in school and in the classroom.
- PIN access to the device must always be known by the network manager.
- Exit process – when the device is returned the staff member must log in with personal ID so that the device can be Factory Reset and cleared for reuse.

Students 'use of personal devices

- The School strongly advises that student mobile phones and devices should not be brought into school. The School does though accept that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- Where personal devices are brought into school they must be handed into the school office for safe keeping.
- If a student breaches the school policy, then the device will be confiscated and will be held in a secure place in the school office. Mobile devices will be released to parents or carers in accordance with the school policy.
- Students should protect their phone numbers by only giving them to trusted friends and family members.

Staff use of personal devices

- Any permitted images or files taken in school on staff handheld devices, including mobile phones and personal cameras, must be downloaded from the device and deleted in school before the end of the day.
- Staff are not permitted to use their own mobile phones or devices in a professional capacity, such as for contacting children, young people or their families within or outside of the setting.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Visitor's use of personal devices

- Visitors are not permitted to use their own mobile phones or devices in a professional capacity, such as for photographing, videoing or contacting children, young people or their families.
- Mobile Phones and personally-owned devices must be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used whilst on the school site unless permission has been granted by a member of the senior leadership team in emergency circumstances.

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;
- If specific pupil photos are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term, high profile use
- 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:

Online Safety Contacts and Resources

Action for Children: http://actionforchildren.org.uk/

BBC Chat Guide: http://www.bbc.co.uk/pressoffice/pressreleases/stories/2003/07_july/16/chatguide.shtml

Buckinghamshire Safeguarding Children Board: http://bucks-lscb.org.uk/Online Safety

Bucks e–Safety Guidance: http://www.bucksgfl.org.uk/course/view.php?id=384

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

Childline: www.childline.org.uk

Childnet: www.childnet.com

Click Clever Click Safe Campaign: http://www.nidirect.gov.uk/the-click-clever-click-safe-code-information-for-young-people

Cybermentors/BeatBullying: www.cybermentors.org.uk

Digizen: www.digizen.org.uk

Grid Club and the Cyber Café: http://www.gridclub.com/

Internet Watch Foundation (IWF): www.iwf.org.uk

Kidsmart: www.kidsmart.org.uk

NSPCC: http://www.nspcc.org.uk/help-and-advice/help_and_advice_hub_wdh71748.html

Orange Education: www.orange.co.uk/education

Safe: www.safesocialnetworking.org

Stop Text Bully: www.stoptextbully.com

Teach Today: http://en.teachtoday.eu

Thames Valley Police: In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries dial 101 or use http://www.thamesvalley.police.uk/

Think U Know website: www.thinkuknow.co.uk

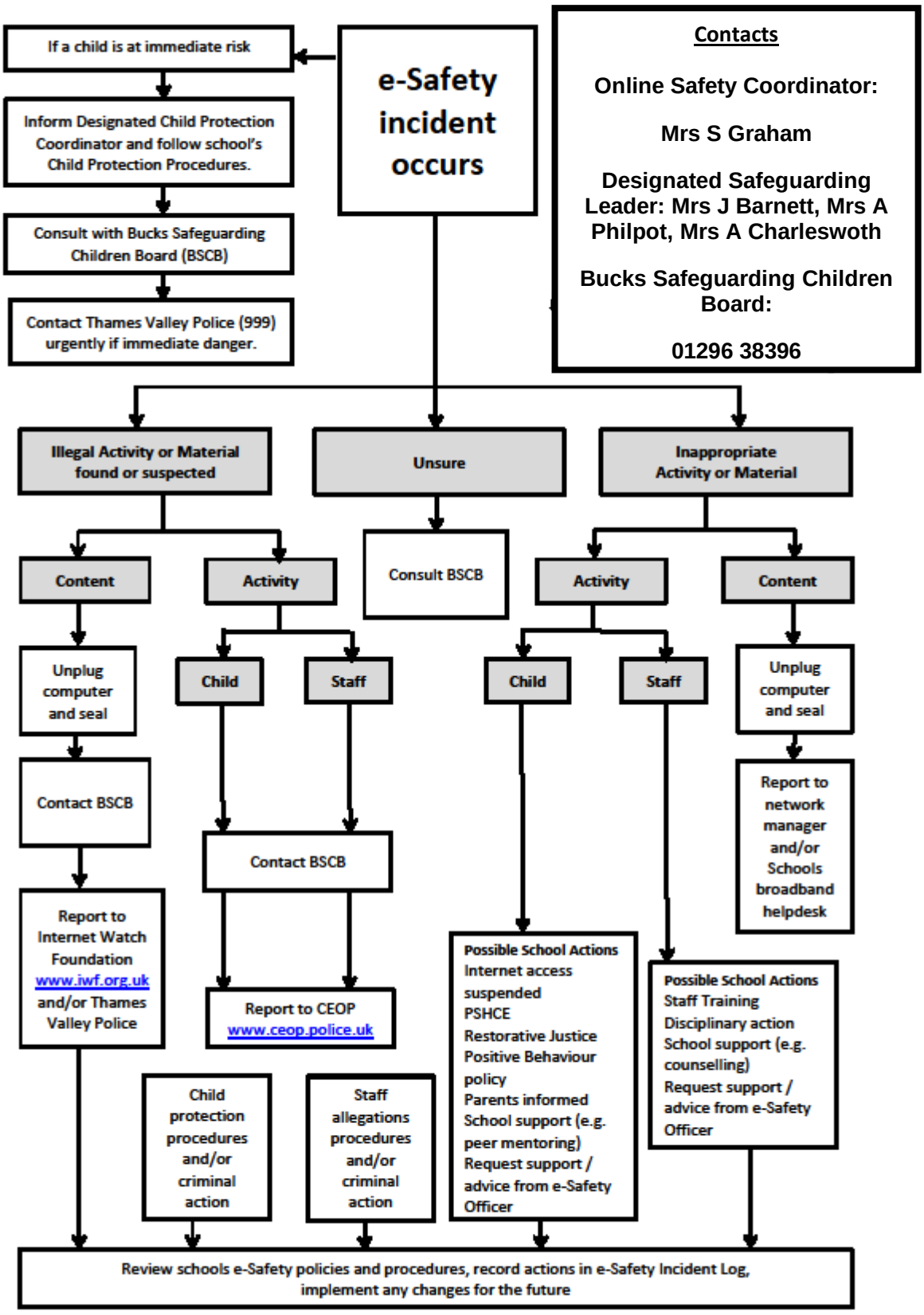
UKCCIS UK Council for Child Internet Safety https://www.education.gov.uk/childrenandyoungpeople/safeguardingchildren/b00222029/child-internet-safety

Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com

Safe: www.safesocialnetworking.org

APPENDIX 2:

Response to an Incident of Concern



APPENDIX 3:

SMAS Incident Log

St Mary & All Saints Primary School e-Safety Incident Log

Date & time	Name of pupil or staff member	Male or Female	Room and computer/ device number	Details of incident (including evidence)	Actions and reasons

St Mary & All Saints Primary School

Pupil Acceptable Use Policy

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

INTERNET:

- I will only use the internet when supervised by a teacher or adult, or when given special permission.
- I understand that the school may monitor the web sites I have visited.
- I understand that I can only access sites and materials relevant to my work in school.
- I know that information on the internet may not always be reliable and sources may need to be checked.
- I know that I will not be allowed to use the internet if I deliberately look at unsuitable material.

SECURITY & PRIVACY:

- I will never tell anyone I meet on the internet my personal information or that of others (home address, telephone number, school's name) unless my teacher or parent/carer specifically gives me permission.
- I will never send anyone my picture without permission from my teacher or parent/carer.
- I will never give my password to anyone, even my best friend.
- I will never arrange to meet anyone in person without first agreeing it with my teacher or parent/carer and I will get them to come along to the first meeting.
- I will never hang around in an internet chat room if someone says or writes something which makes me feel uncomfortable or worried. I will always report it to my teacher or parent/carer.
- I will never respond to unpleasant, suggestive or bullying emails, messages or bulletin boards. I will immediately report this to my teacher or parent/carer.
- I will not look for bad language or distasteful images while I am online. I will report bad language or distasteful images to my teacher or parent/carer if I come across them accidentally.
- I will always be myself and will not pretend to be anyone or anything I am not.
- I know that my teacher can see all the messages I sent through the VLE.
- I will not take or distribute images of anyone without their permission.

- I respect other people's work and will not access, copy, remove or change any other user's files without their knowledge and permission.

- **EMAIL:**
- I will be polite and responsible when I communicate with others.
- I know that posting of anonymous messages and forwarding of chain messages is not allowed.
- I will not use strong, aggressive, racist or inappropriate language.
- I know that the contents of my email messages may be monitored by the school.

EQUIPMENT:

- I will log off when I have finished using the computer.
- I will not download or install software from the internet or attached to emails (including screen savers, games, video clips, audio clips, exe files) without permission.
- I will not deliberately bypass any systems designed to keep us safe.
- I will not eat or drink near computer equipment.
- I will look after all computer equipment and will report any loss or damage immediately, however this may have happened.

St Mary & All Saints Primary School
Pupil Acceptable Use Agreement Form

This form relates to the SMAS Pupil Acceptable Use Policy (AUP), to which it is attached. Please read this document carefully and complete the sections below to show that you have read and understood the AUP, discussed it with your child and agree to the rules included.

If any pupil does not comply with this Acceptable Use Policy (AUP), access to the school ICT systems will be suspended and the student will be subject to disciplinary action. Additional action may be taken in line with the existing positive behaviour policy. For serious violations, suspension or expulsion may be imposed. Where appropriate, the police may be involved or other legal action taken. For more information please see the schools Online Safety Policy.

Only once this agreement form has been signed and returned will access to the school ICT systems be permitted.

I have read and understood the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment
- I use my own equipment out of school in a way that is related to me being a member of the school (e.g. communicating with other members of the school, accessing school e-mail, VLE, web site etc.)

Name of Pupil:	
Pupil Signature	
Parent/Carer Name:	
Parent/Carer Signature:	
Date: DD/MM/YYYY	

APPENDIX 5:

St Mary & All Saints Primary School

Staff, Governor & Volunteer Acceptable Use Policy

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

SECURITY & PRIVACY:

- I understand that the school may monitor my use of the ICT systems, email and other digital communications.
- I will not disclose my username and password to anyone else, nor will I try to use any other person's username and password.
- I will respect system security and will use a 'strong' password. A strong password has numbers, letters and symbols, with 8 or more characters.
- To prevent unauthorized access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to the Headteacher.
- I will not try to use any programmes or software or alter settings that might allow me to bypass the filtering or security systems in place.
- I will not try to download, upload or access any materials which are illegal or inappropriate or may cause harm or distress to others.
- I will only keep professional documents which contain school-related sensitive personal information on any devices that are secure and encrypted.
- I will not use a personal camera or camera phone to record pupil images.
- I will not publish any images of children outside the school environment without express permission from the parents and the Head teacher.
- If offensive materials are found, I will immediately switch off the monitor, leave the computer running, confiscate any printed materials, CDs or memory sticks and report it to the Headteacher immediately.
- I have read and understood the Online Safety policy which covers the requirements for safe ICT use.
- 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 Headteacher.

(EMAIL / INTERNET) COMMUNICATION:

- I will access the internet for educational purposes only.
- I will communicate with others in a professional manner; I will not use aggressive or inappropriate language.
- I will only communicate with pupils, parents/carers and other professionals via the approved communication channels (School Office email address).

- I will only respond to messages received from children relating to school matters.
- I will not open any attachments to emails, unless the source is known and trusted.
- I will not use personal email addresses on the school ICT systems.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos) unless permission has been granted.
- I understand that disciplinary action may be taken if the internet is used inappropriately.

EQUIPMENT:

- I understand that the rules set out in this agreement also apply to use of school ICT systems out of school (e.g. laptops, email, VLE). I will only use the school ICT systems for professional and educational purposes.
- When I use personal portable media I will ensure they are protected by up-to-date virus software and are free from viruses.
- I will not access, copy, remove or alter any other user's file, without prior permission.
- I will not download or install software from the internet or attached to emails (including screen savers, games, exe files) without permission.
- I will protect computer equipment from spillage by eating and drinking well away from them.

St Mary & All Saints Primary School

Staff, Governor & Volunteer Acceptable Use Agreement Form

This form relates to the SMAS Staff, Governor & Volunteer Acceptable Use Policy (AUP), to which it is attached. Please read this document carefully and complete the sections below to show that you have read and understood the AUP.

I understand that if I fail to comply with this Acceptable Use Policy I could be subject to disciplinary action.

I have read and understood the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff /Governor/
Volunteer:

Signature:

Date:
DD/MM/YYYY

APPENDIX 6:

St Mary & All Saints Primary School

External Photograph Contract

I understand the data protection considerations and am capable of meeting all responsibilities and obligations.

- I shall only use the visual images for the purposes indicated by the school.
- Visual images shall be made available to the pupils or their parents only for personal use, either by the school itself or by the photographer.
- All images are stored safely and securely.
- All images will be deleted within a 3 year period of the date below.
- I will not have unsupervised access to children.

I have an up to date Disclosure and Barring Service check which has been seen by the school.

Name:

Signature:

On behalf of St Mary & All Saints Primary School:

Name:

Signature:

Date: