St Matthew's
Westminster

Online Safety Policy
And Acceptable Use Agreement

This policy was reviewed in July 2022
This policy was approved by the Governing Body in July 2022
This policy will be reviewed on July 2024
(*unless any changes are necessary prior to this date)*

BELONGING | BELIEVING | ACHIEVING

"You are the light of the world."
Matthew 5:14

This policy is part of the school's statutory Child Protection Safeguarding Policy. Any issues and concerns with online safety must follow the school's Child Protection and Safeguarding Policy and procedures.

Designated Safeguarding Lead at St Matthew's Primary School: Helen Selinas (Head of School, Inclusion)
Deputy Designated Safeguarding Leads at St Matthew's Primary School: Rachel Jewitt (Executive Headteacher) and Sarah Green (Head of School, Curriculum)
Lead Safeguarding Governor: Louise McCullough
Chair of Governors: Fr Philip Chester

INTRODUCTION

At St Matthew's Primary School we are committed to providing a caring, friendly and safe environment in line with our school vision for all of our pupils so that they can become confident learners. We are dedicated to safeguarding and promoting the welfare of pupils and young people and expect all staff and volunteers to share this commitment. In line with our school Behaviour Policy, a bullying incident should be addressed as a child protection concern when there is 'reasonable cause to suspect that a pupil is suffering, or is likely to suffer, significant harm'.

This policy should be read alongside our Behaviour Policy (& Anti-Bullying Statement), Child Protection and Safeguarding Policy, curriculum plans, Staff Code of Conduct and the school's vision.

This policy applies to all members of St Matthew's Primary School who have access to and are users of the IT systems, both in and out of school. This includes staff, pupils, governors, volunteers, parents/carers, visitors, community users.

AIMS

The purpose of this policy is to:

- set out the key principles expected of all members of the school community at St Matthew's Primary School with respect to the use of IT-based technologies
- safeguard and protect the children, staff, parents and governors at St Matthew's Primary School

- assist school staff working with children to work safely and responsibly with the internet and other IT and communication technologies
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use
- have clear structures to deal with online abuse such as online bullying
- 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 members of our school community are (this list is not exhaustive):

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.)
- cyber-bullying in all forms
- social or commercial identity theft, (including 'frape' (hacking Facebook profiles)) and sharing 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 (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film)

ROLES AND RESPONSIBILITIES

Role	Key Responsibilities
Executive Headteacher (also the Deputy Designated Safeguarding Lead)	• 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 procedures • Ensure that policies and procedures are followed by all staff • Lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information • To take overall responsibility for online safety provision • To take overall responsibility for data management and information security 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 • To ensure that governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety • To ensure school website meets statutory DfE requirements • Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents • Work with the DPO and governors to ensure a GDPR-compliant framework for storing data • Promote an awareness and commitment to online safety throughout the school community • Ensure that online safety education is embedded within the curriculum To communicate regularly with governors to discuss current online safety 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 • Oversee any pupil surveys / pupil feedback on online safety issues • Liaise with the Local Authority and relevant agencies in line with statutory documents
Computing Subject Leader	As listed in the 'teachers' section, plus: • To oversee the delivery of the online safety element of the computing curriculum in accordance with the national curriculum • Work closely with the *Executive* Headteacher and DSL and all other staff to ensure an understanding of the issues, approaches and messaging within computing • Collaborate with technical staff and others responsible for IT use in school to ensure a common and consistent approach, in line with acceptable-use agreements • To ensure parents are kept up to date with relevant online safety advice
Teachers, all staff,	(Appendix 3 – Acceptable Use Agreement)

Governors, volunteers and contractors	I agree to adhere to the Staff/Governor Code of Conduct in addition to the guidance in this Acceptable Use Agreement ● I understand that online safety is a core part of safeguarding procedures ● I will embed the teaching of online safety in the curriculum ● I will supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) ● I will ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws in an age appropriate manner ● I will report any suspected misuse or problem to the Executive Headteacher and record online safety incidents in the same way as any safeguarding incident and report in accordance with school safeguarding procedures (CPoms) ● I will maintain an awareness of current online safety issues and guidance (e.g. through CPD) ● I will use the school email account for professional use and will not use my personal email address for school business ● I will 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) ● I will not make reference in social media to students/pupils, parents/carers or school staff ● TEACHERS - I will not be online 'friends' with any pupil, parent or carer GOVERNORS – I will not be online 'friends' with a pupil and will adhere to the Governors' Code of Conduct for online 'friends' who may be a parent/carer at the school ● I will not engage in online discussion on personal matters relating to members of the school community ● I understand that personal opinions I share in my personal life should not be attributed to the school and must not compromise the professional role of a staff member, nor bring the school into disrepute ● I will regularly check security settings on personal social media profiles to minimise risk of loss of personal information ● I will not use mobile phones or SMART devices in the classroom or around the school building in the presence of pupils (except in an emergency situation) ● I will model safe, responsible and professional behaviours in my own use of technology, including outside of the school hours and off-site to uphold the reputation of the school and of the professional reputation of all staff (teachers should refer to Part Two of the DfE Teachers' Standards) ***Exit strategy*** ● *I understand that at the end of the period of employment/placement, I have 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. I may meet with the Executive Headteacher or School Business Manager as necessary in order for settings and devices to be reset.*
Pupils	● See Appendix 1 and Appendix 2 for Pupils' Online Safety Agreements

Network Manager/ technician	As listed in the 'teachers' section, plus: ● To report online safety related issues that come to their attention, to the Executive Headteacher (DSL) ● 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 ● That the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the Executive 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
Parents/ carers	● To read, understand and promote the school's Pupil Online Safety 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 follow online safety guidance in the Parent Information Pack ● Will give written consent for pupil mobile phones to be brought into school if their child walks to and from school on their own (usually only Years 5 and 6) ● Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
External groups	● Any external individual/organisation will sign the Acceptable Use agreement prior to using technology or the internet within school (visitors will sign this as part of the Inventry sign-in system) ● To support the school in promoting online safety ● To model safe, responsible and positive behaviours in their own use of technology
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;

CURRICULUM, TRAINING & CONSENT

Pupil online safety curriculum

The school:

- has a clear, progressive online safety education programme as part of the Computing curriculum and wider curriculum. This covers a range of skills and behaviours appropriate to pupils' ages 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 Online Safety Agreement
- 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

The school:

- makes regular training available to staff on online safety issues and the school's online safety education programme
- 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

The school:

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

Digital images and video

The school:

- gains parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their child joins the school (photographs may be used on the school website, twitter account and in photographs around the school)
- does 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
- ensures that staff do not use personal mobile phones or devices to take photographs of pupils in the school
- blocks/filter access to social networking sites unless there is a specific approved educational purpose
- ensures that 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

- ensures that pupils are advised to be very careful about placing any personal photos on any 'social' online network space and how to maintain privacy settings so as not to make public, personal information.
- ensures pupils are taught that they should not post images or videos of others without their permission
- ensures pupils are taught about what to do if they are subject to bullying or abuse

MANAGING IT SYSTEMS

IT Devices (iPads, cameras, school mobile phone etc.)

- devices should be accessed via a school based account
- no personal elements may be added to this device
- PIN access to the device must always be known by the Executive Headteacher/Business Manager

Internet access, security (virus protection) and filtering

The 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 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

Network management (user access, backup)

The school:

- uses individual, audited log-ins for users
- uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services
- uses teacher 'remote' management control tools for controlling workstations/viewing users/setting-up applications and Internet web sites, where useful;
- 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
- ensures that 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 network and USO account
- 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 procedures are 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
- 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 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

Password policy

The school

- trains staff and pupils to keep their passwords private, must not share with others (if a password is compromised the Executive Headteacher should be notified immediately)
- provides all staff with their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private. Supply teachers will have a generic login issued at arrival.
- requires staff to use STRONG passwords
- requires staff to change their passwords regularly

School website

- the Executive Headteacher, supported by the Governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained and complies with DfE statutory requirements

- most material published 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 (including Tapestry and Arbor)

- uploading of information on the school's online spaces is shared between different staff members according to their responsibilities
- photographs and videos uploaded to the school's online environment will only be accessible by members of the school community and parents with specific consent for their own child

CCTV

- CCTV is 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.

DATA SECURITY (INCLUDING MANAGEMENT INFORMATION SYSTEMS)

Strategic and operational practices

At this school:

- the Executive Headteacher is the Senior Information Risk Officer (SIRO).
- staff report any incidents where data protection may have been compromised to the Executive Headteacher
- 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
- staff should log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes idle time
- the LGfL USO AutoUpdate is used to create 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 current disposal legislation guidelines
- where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data

INCIDENT MANAGEMENT

- the school will take all reasonable precautions to ensure online safety
- staff and pupils are given information about infringements in use and possible sanctions
- the Executive Headteacher acts as first point of contact for any incident
- any suspected online risk or infringement is reported to the Executive Headteacher immediately
- any concern about staff misuse is always referred directly to the Executive Headteacher unless the concern is about the Executive Headteacher, in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer)

- support is actively sought from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre helpline, 3BM, CEOP, Prevent Officer, Police, Internet Watch Foundation) in dealing with online safety issues
- 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 or sends online communication that we consider is particularly disturbing or breaks the law

Review and Monitoring

- The online safety policy is referenced within other school policies (see introduction).
- The online safety policy will be reviewed annually with the school community or when any significant changes occur with regard to the technologies in use within the school
- All amendments to the school online safety policy will be disseminated to all members of staff and pupils

APPENDIX 1

PUPIL ONLINE SAFETY AGREEMENT

Early Years and Key Stage 1

I keep **SAFE online** using these rules:

I always follow the school's **Golden Rules** to keep myself and others safe
I **CHECK** it's OK to use a website / game / app
I **ASK** for help if I get lost online
I **THINK** before I click on things
I **KNOW** that people online are strangers and are not 'friends'
I am **RESPONSIBLE** so never share private information
I am **KIND** and polite online
I **TELL** a trusted adult if I am worried about anything
My trusted adults are:

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

APPENDIX 2
PUPIL ONLINE SAFETY AGREEMENT
Key Stage 2

St Matthew's
Westminster

Name of pupil:	
When using the school's IT equipment and accessing the internet in school, I will: ● always follow the school's Golden Rules to keep myself and others safe ● only use them for educational purposes ● use them when a member of staff is present or when I have permission from a member of staff ● only access appropriate websites ● not access social networking sites or chat rooms ● check with a teacher before opening any attachments or links in emails ● never share my password with others or log in to the school's network using someone else's details ● not bring SMART devices (including watches) into school ● not share personal or private information online ● be aware of what a real 'friend' is and will not accept online friend requests from strangers ● immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others I understand that: ● the school will monitor the websites I visit and my use of the school's ICT facilities and systems ● if I walk to/from school on my own and my parent has given permission for me to bring a mobile phone to school, I will leave this in the school office for the duration of the school day	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's IT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's IT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent):	**Date:**

St Matthew's
Westminster

STAFF, GOVERNORS, VOLUNTEERS ACCEPTABLE USE AGREEMENT

**A hard copy of this agreement is made available to visitors when they sign into the school Visitors agree to this Acceptable Use Agreement when they sign into the school building*

Name of member of staff/governor/volunteer:

I agree to adhere to the Staff/Governor Code of Conduct in addition to the guidance in this Acceptable Use Agreement

- I understand that online safety is a core part of safeguarding procedures
- I will embed the teaching of online safety in the curriculum
- I will supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant)
- I will ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws in an age appropriate manner
- I will report any suspected misuse or problem to the Executive Headteacher and record online safety incidents in the same way as any safeguarding incident and report in accordance with school safeguarding procedures (Appendix 5)
- I will maintain an awareness of current online safety issues and guidance (e.g. through CPD)
- I will use the school email account for professional use and will not use my personal email address for school business
- I will 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)
- I will not make reference in social media to students/pupils, parents/carers or school staff
- TEACHERS - I will not be online 'friends' with any pupil, parent or carer

  GOVERNORS – I will not be online 'friends' with a pupil and will adhere to the Governors' Code of Conduct for online 'friends' who may be a parent/carer at the school
- I will not engage in online discussion on personal matters relating to members of the school community
- I understand that personal opinions I share in my personal life should not be attributed to the school and must not compromise the professional role of a staff member, nor bring the school into disrepute
- I will regularly check security settings on personal social media profiles to minimise risk of loss of personal information
- I will not use mobile phones or SMART devices in the classroom or around the school building in the presence of pupils (except in an emergency situation)
- I will model safe, responsible and professional behaviours in my own use of technology, including outside of the school hours and off-site to uphold the reputation of the school and of the professional reputation of all staff (teachers should refer to Part Two of the DfE Teachers' Standards)

Exit strategy

- *I understand that at the end of the period of employment/placement, I have 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. I may meet with the Executive Headteacher or School Business Manager as necessary in order for settings and devices to be reset.*

I have read and understood everything in this agreement and understand that if I have any other questions, I can speak to the Executive Headteacher or School Business Manager

Signed: **Date:**

APPENDIX 4

TAPESTRY PARENTAL CONSENT (For parents/carers of pupils in Nursery and Reception)

St Matthew's
Westminster

Tapestry Consent Form

Pupil's Name:_____ Class:_____

A learning journal will be used to reflect your child's time in the Early Years at St Matthew's. It may include photographs of your child at play with other children (you will not be able to see the names of other children in the photographs).

Please read and indicate your consent clearly:

1. I consent to photographs of my child being taken by the staff of St Matthew's Primary School — Yes ☐ No ☐ (tick as appropriate)

2. I consent to photographs containing my child's image being included in other children's learning journals (your child will **not** be named in other children's observations) — Yes ☐ No ☐ (tick as appropriate)

3. I will treat photographs containing images of <u>any</u> children, including my own child in individual photographs and group photographs, **for my own personal use only*** — Yes ☐ No ☐ (tick as appropriate)

4. I consent to my email address being used to set up the Tapestry account (this will be the primary email address on your child's registration form) — Yes No (tick as appropriate) ☐

*(*This means that the information cannot be shared with others, or published in any way. For example, any such photographs (including screen shots) **cannot** be posted on a social networking site or displayed in a public place, this includes photographs of your own child.)*

Please note that you can withdraw your consent, in writing, or request to see photos taken at any time. This form is valid for the duration of your child's time at St Matthew's Primary School. It is your responsibility to let us know if you want to withdraw or change your consent at any time.

Signed	
Name of parent/carer	
Date	