St Matthew's Church of England Primary School

Online Safety Policy

Policy written by Kirsten Cameron
Governor Link: Chair of Governors

Policy approved in November 2023
Policy to be reviewed in Autumn 2024

St Edmundsbury and Ipswich
Diocesan Multi Academy Trust

Whatever you do, do it with all your heart. *Colossians 3:23*
Our vision is to be a school where pupils have a positive approach to learning and where provision is consistently good or better. Our curriculum is relevant and creative and reflects our diversity. We aim for all pupils to leave St Matthew's well equipped for the future, demonstrating Christian values and showing self-confidence.

Schedule of Development / Monitoring and Review

This Online Safety policy was approved by the Governing Body on:	***October 2023***
The implementation of this Online Safety policy will be monitored by:	***Mrs Kirsten Cameron ~ Online Safety Lead***
Monitoring will take place at regular intervals:	***Annually***
The Governing Body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	***Once a term within the Headteacher's Report***
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	***October 2024***
Should serious online safety incidents take place, the following external persons / agencies should be informed:	***LADO (if staff)*** ***Suffolk Police***

This policy needs to be read in conjunction with:

- Safeguarding and Child Protection Policy
- Behaviour Policy
- Anti-Bullying Policy
- Staff Code of Conduct

The school will monitor the impact of the policy using:

- Logs of reported incidents on CPOMS
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity
- Surveys / questionnaires of pupils, parents / carers and staff

Scope of the Policy

This Online Safety Policy outlines the commitment of St Matthew's Church of England Primary School to safeguard members of our school community online in accordance with statutory guidance and best practice. This policy has been written in accordance with legislative framework. The legal framework has been included in Appendix F.

This policy applies to all members of St Matthew's Church of England Primary School community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

The school will deal with such incidents within this policy and associated Behaviour and Anti-Bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Online Safety Policy:

The school Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world
- describes how the school will help prepare learners to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related acceptable use agreements
- is made available to staff at induction
- is published on the school website.

Acceptable Use:

The school has defined what it regards as acceptable/unacceptable use and this is shown in Table 1.

The Acceptable Use Agreement are documents that outline a school's expectations on the responsible use of technology by its users. These are signed and acknowledged by all staff as part of their conditions of employment. We also require pupils and parents/carers to sign them, though it is more important for these to be understood and followed rather than just signed. The school's Acceptable User Agreements are in Appendices A to C.

The Online Safety Policy and acceptable use agreements define acceptable use at the school. The acceptable use agreements will be communicated/re-enforced through:

- staff induction and handbook
- communication with parents/carers
- built into education sessions
- school website

When using communication technologies, the school considers the following as good practice:

- when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school
- any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. Personal e-mail addresses, text messaging or social media must not be used for these communications
- staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community

- users should immediately report to the Headteacher the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- relevant policies and permissions should be followed when posting information online e.g. school website and social media. Only school e-mail addresses should be used to identify members of staff and learners

Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

Headteacher:

The Headteacher:

- has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day to day responsibility for online safety will be delegated to the Online Safety Lead – Mrs Kirsten Cameron
- is aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- along with the CPD Leader are responsible for ensuring that the Online Safety Lead and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- will receive regular monitoring reports from the Online Safety Lead.
- will work with the Designated Safeguarding Lead (DSL) and IT service providers in all aspects of filtering and monitoring.

Governors:

The named Online Safety Governor is Mr Derek Ramsay

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Leader
- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- ensuring that the filtering and monitoring provision is reviewed and recorded at least annually
- reporting to other members of the Governing Body

The Governing Body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

Designated Safeguarding Lead (DSL):

The named DSL is Mrs Kirsten Cameron

The Designated Safeguarding Lead should take lead responsibility for safeguarding and child protection including online safety and understanding the filtering and monitoring systems and processes in place. The DSL will:

- take lead responsibility for online safety, within their safeguarding role
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- meet regularly with the online safety governor to discuss current issues, review incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out

- attend relevant Governing Body meetings
- report regularly to Headteacher
- be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

Online Safety Lead:
The named Online Safety Lead is Mrs Kirsten Cameron
In addition to the DSL role, the Online Safety Lead will:

- takes day to day responsibility for online safety issues being aware of the potential for serious child protection concerns
- have a leading role in establishing and reviewing the school online safety policies / documents
- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents.
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- provides training and advice for staff
- liaises with school technical staff
- attends relevant meeting / committee of Governors
- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by pupils) with regard to the areas defined in Keeping Children Safe in Education: content, contact, conduct and commerce.

Curriculum Leads
Curriculum Leads will work with the Online Safety Lead to develop a planned and co-ordinated online safety education programme – Education for a Connected World.
This will be provided through:

- PSHE and RSE programmes
- Part of the computing sessions
- assemblies
- through relevant national initiatives and opportunities such as Safer Internet Day

All Teaching and Support Staff:
School staff are responsible for ensuring that:

- they have an awareness of current online safety matters and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood and signed the Staff Acceptable Use Agreement (AUP) (Appendix A)
- they immediately report any suspected misuse or problem to the Online Safety Lead for investigation / action in line with the school safeguarding procedures.
- all digital communications with pupils, parents or carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure pupils understand and follow the Online Safety Policy and Acceptable Use policies, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices

- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media

Technical Support Staff: (External Company: Orchard House Computers)
Technical Support Staff are responsible for ensuring:

- they are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy
- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets (as a minimum) the required online safety technical requirements as identified by the MAT or other relevant body
- there is clear, safe, and managed control of user access to networks and devices
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the Online Safety Lead / DSL for investigation and action
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that monitoring systems are implemented and regularly updated as agreed in school policies

Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement (Appendix C) and Online Safety Policy
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology
- should understand the importance of adopting 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, if related to their membership of the school

Parents and Carers:
Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.
The school will take every opportunity to help parents understand these issues through

- publishing the school Online Safety Policy on the school website
- providing them with a copy of the pupils' acceptable user agreement
- publish information about appropriate use of social media relating to posts concerning the school
- seeking permission concerning digital images, cloud service etc
- parents' evenings, newsletters, letters, website and information about national / local online safety campaigns.

Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events

Community Users:
Community Users who access school systems as part of the wider school provision will be expected to sign a Community User Acceptable User Agreement before being provided with access to school systems. (Appendix B)

Professional Standards:

There is an expectation that required professional standards will be applied to online safety as in other aspects of school life i.e., policies and protocols are in place for the use of online communication

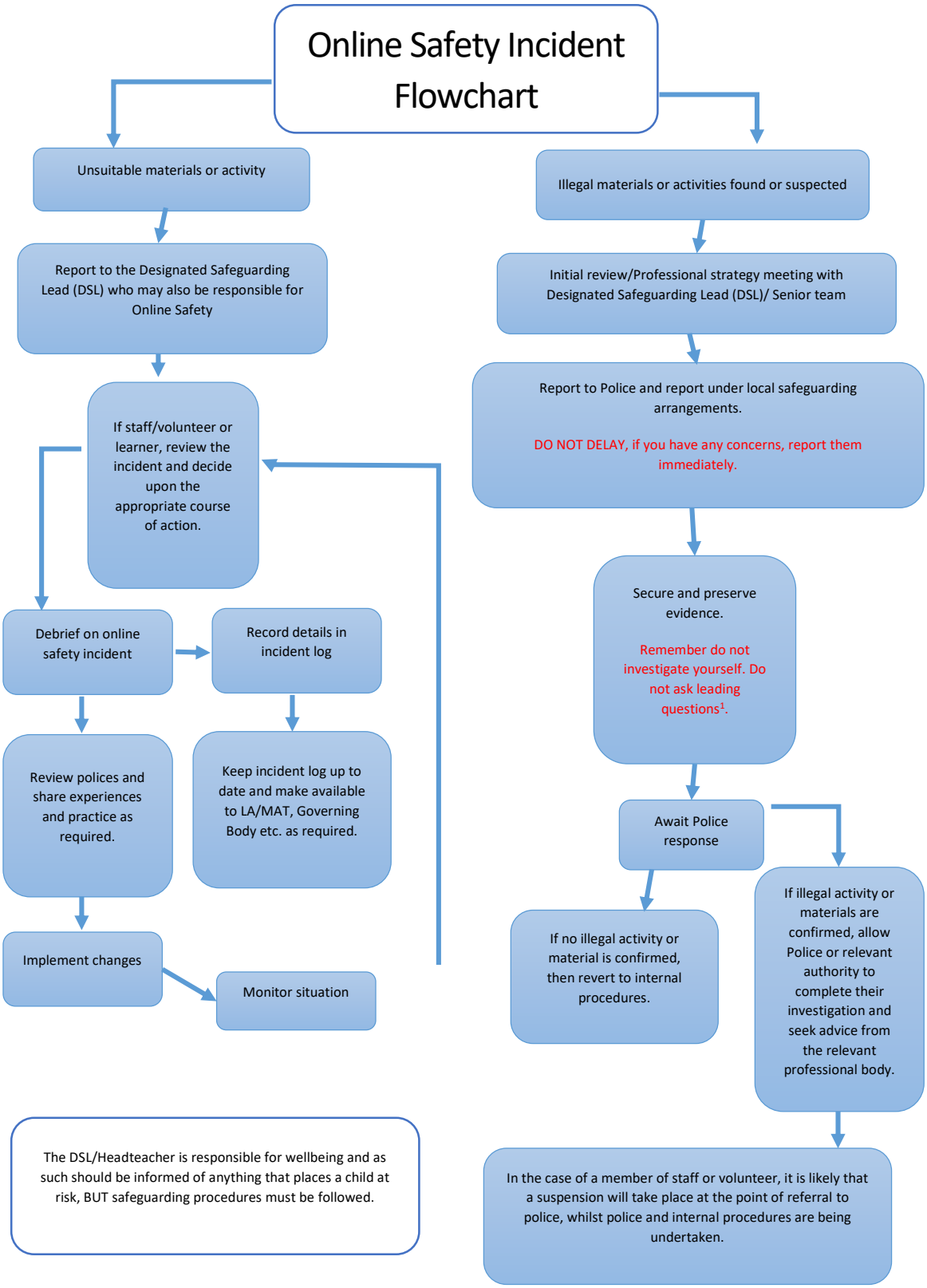
technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms.

Reporting and Responding:

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies
- all members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead / Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm, the incident must be escalated through the agreed school safeguarding procedures. Refer to flow chart on the next page
- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors
- where there is no suspected illegal activity, devices may be checked using the following procedures:
    - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported
    - conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure
    - ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection)
    - record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form
    - once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
        - internal response or discipline procedures
        - involvement by MAT
        - police involvement and/or action
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents should be logged on CPOMS under the category of online
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions if appropriate.
- learning from the incident (or pattern of incidents) will be provided to:
    - staff, through regular briefings
    - learners, through assemblies/lessons
    - parents/carers, through newsletters, school social media, website
    - governors, through regular safeguarding updates

The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.



School Actions:

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with.

It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as outlined in Table 2. All incidents and sanctions for children will be recorded on CPOMS and incidents and sanctions relating to staff will be recorded on their personnel file.

Online Safety Education Programme

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways

- a planned online curriculum for all year groups matched against a nationally agreed framework Education for a Connected Work Framework by UKCIS and regularly taught in a variety of contexts
- lessons are matched to need; are age-related and build on prior learning
- lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- learner need and progress are addressed through effective planning and assessment
- digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PSHE; RSE; English etc
- it incorporates relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- the programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school
- staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit
- it is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need
- the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

Contribution of Learners

The school acknowledges, learns from, and uses the skills and knowledge of learners in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the school community and how this contributes positively to the personal development of young people. Their contribution is recognised through:

- mechanisms to canvass learner feedback and opinion.
- learners contribute to the online safety education programme e.g. peer education, digital leaders leading lessons for younger learners, online safety campaigns

Staff and Volunteers

All staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- a planned programme of formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- the training will be an integral part of the school's annual safeguarding and data protection training for all staff
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours

- the Online Safety Lead and Designated Safeguarding Lead will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations
- this Online Safety Policy and its updates will be presented to and discussed by staff in meetings
- the Online Safety Lead will provide advice / guidance / training to individuals as required

Governors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are involved in online safety and safeguarding. This may be offered in several ways such as:

- attendance at training provided by the local authority
- participation in school training / information sessions for staff or parents

A higher level of training will be made available to the Online Safety Governor and this will include cyber security and training to allow them to understand the school's filtering and monitoring provision so they can conduct the required checks and review.

Families

The school will seek to provide information and awareness to parents and carers through:

- regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes
- regular opportunities for engagement with parents/carers on online safety issues through awareness workshops
- the learners – who are encouraged to pass on to parents the online safety messages they have learned in lessons
- letters, newsletters, website, Class Dojo
- high profile events / campaigns e.g. Safer Internet Day
- reference to the relevant web sites / publications, e.g. SWGfL; www.saferinternet.org.uk/; www.childnet.com/parents-and-carers (see Appendix G for further links/resources).
- Sharing good practice with other schools in the MAT

Adults and Agencies

The school will provide opportunities for local community groups and members of the wider community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- online safety messages targeted towards families and relatives.
- the school will provide online safety information via their website and Class Dojo

Technology

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

The school filtering and monitoring provision is agreed by Headteacher, DSL, Governors and the IT Service Provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility.

Filtering – Surf Quantum Protect provided by EXA

- the school manages access to content across its systems for all users and on all devices using the school's internet provision. The filtering provided meets the standards defined in the DfE and the guidance provided in the UK Safer Internet Centre Appropriate filtering.

- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content recognising that no system can be 100% effective
- there is a clear process in place to deal with requests for filtering changes
- filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon
- If necessary, the school will seek advice from, and report issues to, the SWGfL Report Harmful Content site.

Monitoring - Securus

The school has monitoring systems in place to protect the school, systems and users:

- The school monitors all network use across all its devices and services.
- monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies strategy informed by the school's risk assessment. These may include:

- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to senior leaders

Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements:

- there will be regular reviews and audits of the safety and security of school technical systems
- servers, wireless systems and cabling are securely located and physical access restricted
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies in the cloud
- all users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the Online Safety Lead
- passwords should comply with guidance on creating secure passwords (National Cyber Security Centre)
- all adult users have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security
- the administrator passwords for school systems are kept in a secure place, e.g. school safe.
- records of pupil usernames and passwords for children in Key Stage 1 or younger can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user.
- password requirements for pupils at Key Stage 2 and above should increase as the children progress through school
- Kirsten Cameron, Deputy Headteacher is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied

- an appropriate system is in place for users to report any actual / potential technical incident / security breach to Kirsten Cameron.
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly.
- the school infrastructure and individual workstations are protected by up-to-date endpoint (anti-virus) software, this is **Sophos**.
- an agreed policy is in place, this is stated in Community Users Acceptable User Policy, for the provision of temporary access to the school systems.
- an agreed policy is in place, this is stated in the Laptop Agreement, regarding the extent of personal use that users and their family members are allowed on school devices that may be used out of school
- an agreed policy is in place, this is stated in the Staff Acceptable User Policy, forbids staff from downloading executable files and installing programmes on school devices. All devices need an administrator password to allow files and programmes to be installed on school devices.
- systems are in place that prevent the unauthorised sharing of personal data unless safely encrypted or otherwise secured.
- guest users are provided with appropriate access to school systems based on an identified risk profile.

Mobile Technologies

Mobile technology devices may be school owned or personally owned and might include smartphone, tablet, wearable devices, laptop or other technology that usually has the capability of utilising the school's wireless network.

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational.

Our mobile technologies policy (Appendix D) is consistent with and inter-related to other relevant school polices including but not limited to those for Safeguarding, Behaviour, Anti-Bullying and Acceptable Use.

Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's online safety education programme.

The school acceptable use agreements for staff, learners, parents, and carers outline the expectations around the use of mobile technologies. The school allows:

	School Devices			**Personal Devices**		
	School owned for individual use	School owned for multiple users	Authorised device	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	Yes	Yes	Yes
Full network access	Yes	Yes	Yes	No	No	No
Internet only				No	No	No
No network access				Yes	Yes	Yes

Social Media

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:

- ensuring that personal information is not published
- education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues
- clear reporting guidance, including responsibilities, procedures and sanctions

- risk assessment, including legal risk
- guidance for learners, parents / carers

School staff should ensure that:
- no reference should be made in social media to learners, parents / carers or school staff
- 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
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- they act as positive role models in their use of social media

When official school social media accounts are established, there should be:
- a process for approval by senior leaders
- clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff
- a code of behaviour for users of the accounts
- systems for reporting and dealing with abuse and misuse
- understanding of how incidents may be dealt with under school disciplinary procedures.

Personal Use
- personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- personal communications which do not refer to or impact upon the school are outside the scope of this policy
- where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- the school does not permit reasonable and appropriate access to personal social media sites during school hours

Monitoring of Public Social Media
- as part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school
- the school should effectively respond to social media comments made by others according to a defined policy or process
- when parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.
- School's Social Media Policy – Appendix E

Digital and Video Images

The school will inform and educate users about risks associated with publishing digital images on the internet and will implement policies to reduce the likelihood of the potential for harm:
- the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies
- when using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.
- staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff must not be used for such purposes
- parents/carers are prevented from taking videos and digital images of their children at school events when the child is with other children. Opportunities will be made for photographs to be taken of their child at events

- staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images
- care should be taken when sharing digital/video images that learners are appropriately dressed
- learners must not take, use, share, publish or distribute images of others without their permission
- photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with Online Safety Policy
- pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs
- written permission from parents or carers will be obtained before photographs of pupils are taken for use in school or published on the school website/social media.
- parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy
- images will be securely stored in line with the school retention policy

Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through:

- Public-facing website
- Online newsletters
- Class Dojo

The school website is managed/hosted by **PrimarySite**. The school ensures that online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.
Where learner work, images or videos are published, their identities are protected, and full names are not published.
The school public online publishing provides information about online safety e.g., publishing the schools Online Safety Policy and Pupil Acceptable Use Agreements; curating latest advice and guidance; creating an online safety page on the school website.
The website includes an online reporting process for parents and the wider community to register issues and concerns to complement the internal reporting process, this is provided by CEOP.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.
The school:

- has a Data Protection Policy
- implements the data protection principles and can demonstrate that it does so
- has paid the appropriate fee to the Information Commissioner's Office (ICO)
- has appointed an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest
- has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- the Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed
- will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'retention schedule" supports this
- data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- provides staff, parents, volunteers, teenagers, and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice
- has procedures in place to deal with the individual rights of the data subject

- carries out Data Protection Impact Assessments (DPIA) where necessary e.g. to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier
- has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors
- understands how to share data lawfully and safely with other relevant data controllers
- has clear and understood policies and routines for the deletion and disposal of data
- reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents
- has a Freedom of Information Policy which sets out how it will deal with FOI requests
- provides data protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff

When personal data is stored on any mobile device or removable media the:

- data will be encrypted, and password protected
- device will be password protected
- device will be protected by up-to-date endpoint (anti-virus) software
- data will be securely deleted from the device, in line with school policy once it has been transferred or its use is complete

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school
- only use encrypted data storage for personal data
- will not transfer any school personal data to personal devices
- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.

Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, learners; parents/carers and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors
- parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
- the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

Appendix A:

St Matthew's Church of England Primary School

Staff (and Volunteer) Acceptable Use Policy Agreement

St Edmundsbury and Ipswich Diocesan Multi Academy Trust

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for learning and will, in return, expect staff and volunteers to agree to be responsible users.

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that learners receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images. Where these images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not access social networking sites with school devices or on the school network.
- I will only communicate with pupils and parents using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school's IT systems
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email
- I will ensure that my data is regularly backed up.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer/iPad settings.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this acceptable use policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology 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 / Volunteer Name: .....

Signed: .....

Date: .....

Our school online safety co-ordinator is Mrs Cameron.
Please feel free to contact her if you have any concerns regarding online safety.

Appendix B:

St Matthew's Church of England Primary School

Community Users Acceptable Use Agreement

St Edmundsbury and Ipswich Diocesan Multi Academy Trust

This Acceptable Use Agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential harm in their use of these systems and devices

Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school:

- I understand that my use of school systems and devices will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist and extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and/or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, whatever the cause.
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

- I understand that if I fail to comply with this acceptable use agreement, the school has the right to remove my access to school systems/devices

I have read and understand the above and agree to use the school digital technology 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.

This information will be shared, stored and destroyed in line with GDPR guidelines. It will be destroyed at the end of your placement within the school or if you are a frequent visitor it will be destroyed at the end of the academic year.

Community User Name: .....

Signed: .....

Date: .....

Our school online safety co-ordinator is Mrs Cameron.

Please feel free to contact her if you have any concerns regarding online safety.

Appendix C:

St Matthew's Church of England Primary School

Key Stage 2 Children: Acceptable Use Agreement

St Edmundsbury and Ipswich Diocesan Multi Academy Trust

Digital technologies have become integral to the lives of children and young people, both within and outside schools. These technologies are powerful tools, which open-up new opportunities for everyone. They can stimulate discussion, encourage creativity and stimulate awareness of context to promote effective learning. Learners should have an entitlement to safe access to these digital technologies.

This Acceptable Use Agreement is intended:

- to ensure that learners will have good access to devices and online content, be responsible users and stay safe while using digital technologies for educational, personal and recreational use
- to help learners understand good online behaviours that they can use in school, but also outside school
- to protect school devices and networks from accidental or deliberate misuse that could put the security of the systems and users at risk.

Acceptable Use Agreement

When I use devices I must behave responsibly to help keep me and other users safe online and to look after the devices.

For my own personal safety:

- I understand that what I do online will be supervised and monitored and that I may not be allowed to use devices in school unless I follow these rules and use them responsibly
- I will only visit internet sites that adults have told me are safe to visit
- I will keep my username and password safe and secure and not share it with anyone else
- I will be aware of "stranger danger" when I am online
- I will not share personal information about myself or others when online
- If I arrange to meet people off-line that I have communicated with online, I will do so in a public place and take a trusted adult with me
- I will immediately tell an adult if I see anything that makes me feel uncomfortable when I see it online.

I will look after the devices I use, so that the school and everyone there can be safe:

- I will handle all the devices carefully and only use them if I have permission.
- I will not try to alter the settings on any devices or try to install any software or programmes.
- I will tell an adult if a device is damaged or if anything else goes wrong.
- I will only use the devices to do things that I am allowed to do.

I will think about how my behaviour online might affect other people:

- When online, I will act as I expect others to act toward me.
- I will not copy anyone else's work or files without their permission.
- I will be polite and responsible when I communicate with others and I appreciate that others may have different opinions to me.
- I will not take or share images of anyone without their permission.

I know that there are other rules that I need to follow:

- If I bring a mobile phone to school, this will be switched off at the school gates and handed to the class teacher. I will sign a copy of the school's mobile phone agreement.
- I will not use social media sites while at school.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I should have permission if I use the original work of others in my own work.

I understand that I am responsible for my actions, both in and out of school:

- I know that I am expected to follow these rules in school and that I should behave in the same way when out of school as well.
- I understand that if I do not follow these rules, I may be subject to disciplinary action. This could include loss of access to the school network/internet, parents/carers contacted and in the event of illegal activities involvement of the police.

Learner Acceptable Use Agreement Form

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems.

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

- I use the school systems and devices
- I bring a mobile phone to school, I have signed a Mobile Phone Agreement (Year 5 & 6 only)
- I am out of school and involved in any online behaviour that might affect the school or other members of the school.

Pupil signature _____ Date _____

Parent/Carer: I confirm that I have explained the school rules regarding online behaviour to my child.

Parent/Carer signature _____ Date _____

Our school online safety co-ordinator is Mrs Cameron.

Please feel free to contact her if you have any concerns regarding online safety.

St Matthew's Church of England Primary School
Mobile Phone Agreement for Years 5 and 6

This agreement is between parents, children and the school and is designed to ensure the safety and security of children and their property.

I give permission for _____ (child's name), in class _____ to be

allowed to bring a mobile phone to school because:

_____

_____

The telephone number of the mobile is: _____

My child agrees:

- ★ I will only bring a mobile phone to school if I need it to keep me safe when I am walking to or from school without an adult, and only if my parents say that I can.
- ★ I will switch my phone off as soon as I get to the school gates in the morning.
- ★ I won't switch it on again after school until I am outside the school gates.
- ★ I will hand my phone to my teacher or teaching assistant as soon as I get into the classroom in the morning.
- ★ I will be responsible for remembering to collect my phone at the end of the day.
- ★ I will not use my phone to take any photographs at school, either in the classroom, playground or anywhere else on the school site.
- ★ The school cannot accept responsibility for damage or loss of a mobile phone brought into school.

I understand that it I break any of these rules, a phone call will be made to my parents which may mean I cannot bring my phone to school.

Parent/Carer: I confirm that I have explained the school rules regarding mobile phones to my child and confirm that they may take a mobile phone into school on that basis.

Parent/Carer signature _____ Date _____

Pupil: I will follow the school mobile phone rules.

Pupil signature _____ Date _____

Our school online safety co-ordinator is Mrs Cameron.

Please feel free to contact her if you have any concerns regarding online safety.

Appendix C:

St Matthew's Church of England Primary School

EYFS and Key Stage 1 Children: Acceptable Use Agreement

St Edmundsbury and Ipswich Diocesan Multi Academy Trust

Digital technologies have become integral to the lives of children and young people, both within and outside schools. These technologies are powerful tools, which open-up new opportunities for everyone. They can stimulate discussion, encourage creativity and stimulate awareness of context to promote effective learning. Learners should have an entitlement to safe access to these digital technologies.

This Acceptable Use Agreement is intended:

- to ensure that learners will have good access to devices and online content, be responsible users and stay safe while using digital technologies for educational, personal and recreational use
- to help learners understand good online behaviours that they can use in school, but also outside school
- to protect school devices and networks from accidental or deliberate misuse that could put the security of the systems and users at risk.

This is how we stay safe when we use computers:

- ★ I will ask a teacher or suitable adult if I want to use the computers/tablets
- ★ I will only use activities that a teacher or suitable adult has told or allowed me to use
- ★ I will take care of computers/tablets and other equipment
- ★ I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- ★ I will tell a teacher or suitable adult if I see something that upsets me on the screen
- ★ I know that if I break the rules I might not be allowed to use a computer/tablet

Pupil signature _____ Date _____

Parent/Carer: I confirm that I have explained the school rules regarding online behaviour to my child.

Parent/Carer signature _____ Date _____

Our school online safety co-ordinator is Mrs Cameron.

Please feel free to contact her if you have any concerns regarding online safety.

Table 1:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate	Child sexual abuse images					✓
	Child sexual abuse / exploitation / grooming					✓
	Terrorism					✓
	Encouraging or assisting suicide					✓
	Offences relation to sexual images ie revenge or extreme pornography					✓
	Incitement to and threats of violence					✓
	Hate crime					✓
	Public order offences - harassment and stalking					✓
	Drug related offences					✓
	Weapons / firearm offences					✓
	Fraud and financial crimes including money laundering					✓
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised)					✓
	Gaining unauthorised access to school networks, data and files, through the use of computers/devices					✓
	Creating or propagating computer viruses or other harmful files					✓
	Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords)					✓
	Disable / Impair / Disrupt network functionality through the use of computers / devices					✓
	Using penetration testing equipment (without relevant permission)					✓
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material / activities online in a school setting including pornography, gambling, drugs.				✓	
	Promotion of any kind of discrimination				✓	
	Using school systems to run a private business				✓	
	Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				✓	
	Infringing copyright				✓	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			✓	✓	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				✓	

Table 1 continued:

Consideration was given for the following activities when undertaken for non-educational purposes: Schools may wish to add further activities to this list.	Staff				Pupils			
	Not Allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not Allowed	Allowed	Allowed at certain times	Allowed for selected staff
Online gaming	✓				✓			
Online shopping/commerce	✓				✓			
File sharing		✓			✓			
Social media			✓		✓			
Messaging/chat			✓		✓			
Entertainment streaming e.g. Netflix, Disney+			✓		✓			
Use of video broadcasting, e.g. YouTube, Twitch, TikTok			✓		✓			
Mobile phones may be brought to school		✓				✓		
Use of mobile phones for learning at school	✓				✓			
Use of mobile phones in social time at school			✓		✓			
Taking photos on mobile phones/cameras	✓				✓			
Use of other personal devices, e.g. tablets, gaming devices	✓				✓			
Use of personal e-mail in school, or on school network / wi-fi	✓				✓			
Use of school e-mail for personal e-mails		✓				✓		

Table 2

Pupils Incidents	Refer to class teacher	Refer to Online Safety Lead / DSL	Refer to Headteacher	Refer to Police / Social Care	Inform parents / carers	Sanctions in line with Behaviour Policy	Remove device / internet access	Refer to technical support staff for action re filtering / security etc.
Deliberately accessing or trying to access material that could be considered illegal		✓	✓	✓				
Attempting to access or accessing the school network, using another user's account (staff or learner) or allowing others to access school network by sharing username and passwords	✓	✓	✓		✓			✓
Corrupting or destroying the data of other users.		✓	✓		✓			✓
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature		✓	✓		✓			
Unauthorised downloading or uploading of files or use of file sharing.		✓			✓			
Using proxy sites or other means to subvert the school's filtering system.		✓			✓			
Accidentally accessing offensive or pornographic material and failing to report the incident.		✓	✓	✓	✓			
Deliberately accessing or trying to access offensive or pornographic material.		✓	✓	✓	✓			
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.		✓			✓			
Unauthorised use of digital devices (including taking images)		✓	✓		✓		✓	
Unauthorised use of online services		✓	✓		✓		✓	
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.		✓	✓		✓		✓	
Continued infringements of the above, following previous warnings or sanctions.		✓	✓		✓			✓

Table 2:

Staff Incidents	Refer to Headteacher	Refer to Local Authority / MAT	Refer to Police	Refer to Technical Support Staff for action re filtering etc.
Deliberately accessing or trying to access material that could be considered illegal	✓	✓	✓	
Deliberate actions to breach data protection or network security rules	✓	✓		✓
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓	✓		✓
Using proxy sites or other means to subvert the school's filtering system	✓	✓		✓
Unauthorised downloading or uploading of files or file sharing	✓			
Breaching copyright or licensing regulations	✓	✓		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	✓			✓
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	✓	✓		
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils and parents/carers	✓			
Inappropriate personal use of the internet / social media / personal email	✓			
Careless use of personal data e.g. holding or transferring data in an insecure manner	✓	✓		
Actions which could compromise the staff member's professional standing	✓			
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓			
Failing to report incidents whether caused by deliberate or accidental actions	✓			
Continued infringements of the above, following previous warnings or sanctions	✓	✓		

Appendix D

St Matthew's Church of England Primary School

Computer Misuse and Cyber Choices Policy

St Edmundsbury and Ipswich Diocesan Multi Academy Trust

All key stakeholders, including the school IT service provider, have responsibility for the safeguarding of young people from computer misuse and are aware of the Cyber Choices programme led by the National Crime Agency (NCA) and managed locally by Regional Organised Crime Units (part of the national policing network).

The risks to young people of crossing the line into committing cybercrimes is a safeguarding issue. This often happens without the individual even realising, young people need support in making the right #CyberChoices in their use of technology.

Young people with an interest in technology, a high IQ, and an appetite to engage in risky behaviours are considered to be at a higher risk of committing a cyber-offence, but many first-time offenders are also unaware of what the law governing cyber offences actually is. The average age of first-time cyber offenders in the UK has fallen significantly in recent years.

The Cyber Choices programme works with individuals committing, or at risk of committing, cybercrimes which can only be carried out with technology, where devices are both the tool for committing the crime, and the target of the crime.

All staff are made aware of the safeguarding risks of computer misuse.

All staff are familiar with the NCA Hacking it Legal Leaflet*, which explains Cyber Choices and the Computer Misuse Act 1990, and lists recommended resources for teachers to use.

Staff are aware of the role of their local Regional Organised Crime Unit as their point of contact for Cyber Choices referrals.

Learners agree to the Acceptable Use Policy (AUP) which outlines acceptable online behaviours and explains that some online activity is illegal. Acceptable computer use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990. Lessons and further resources are available on the NCA Cyber Choices site.

Any breach of the AUP or activity by a learner that may constitute a cybercrime, in school or at home, will be referred to the Designated Safeguarding Lead for consideration as a safeguarding risk.

Where the DSL believes that the learner may be at risk of committing cybercrimes, or to already be committing cybercrimes, a referral to the local Cyber Choices programme will be made. Where the DSL is unsure if a learner meets the referral criteria, advice should be sought from the local Cyber Choices team.

Parents also have the opportunity report potential cybercrime directly to the local Cyber Choices team but are recommended to make school-based concerns through the DSL.

The IT service provider is aware of the safeguarding requirement to refer concerns about computer misuse to the Designated Safeguarding Lead and has a clear process to follow in order to do so.

Appendix E

St Matthew's Church of England Primary School

Mobile Technologies Policy

St Edmundsbury and Ipswich Diocesan Multi Academy Trust

Mobile technology devices may be a school owned / provided or privately owned smartphone, tablet, laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

The absolute key to considering the use of mobile technologies is that the learners, staff and wider school community understand that the primary purpose of having their personal device at school is educational and that this is irrespective of whether the device is school owned / provided or personally owned.

The mobile technologies policy should sit alongside a range of polices including but not limited to the Safeguarding Policy, Anti-Bullying Policy, Acceptable Use Policy, Code of Conduct and the Behaviour Policy. Teaching about the safe and appropriate use of mobile technologies should be included in the online safety education programme.

Potential Benefits of Mobile Technologies

Research has highlighted the widespread uptake of mobile technologies amongst adults and children of all ages. Web-based tools and resources have changed the landscape of learning. Learners now have at their fingertips unlimited access to digital content, resources, experts, databases and communities of interest. By effectively maximising the use of such resources, schools not only have the opportunity to deepen learning, but they can also develop digital literacy, fluency and citizenship in learners that will prepare them for the high tech world in which they will live, learn and work.

Considerations

There are a number of issues and risks to consider when implementing mobile technologies, these include; security risks in allowing connections to your school network, filtering of personal devices, breakages and insurance, access to devices for all learners, avoiding potential classroom distraction, network connection speeds, types of devices, charging facilities, total cost of ownership

Schools may consider implementing the use of mobile technologies as a means of reducing expenditure on school provided devices. However, it is important to remember that the increased network management costs and overheads involved in implementing this properly are likely to counterbalance or outweigh any savings.

The use of mobile technologies brings both real benefits and challenges for the whole school community – including teachers - and the only effective way for a school to implement these successfully is to involve the whole school community from the outset. Before the school embarks on this path, the risks and benefits must be clearly identified and shared with all stakeholders.

- The school acceptable use agreements for staff, learners and community users will give consideration to the use of mobile technologies
- The school has provided technical solutions for the safe use of mobile technology for school devices/personal devices:
    - All school devices are controlled though the use of Mobile Device Management software
    - Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g Internet only access, network access allowed, shared folder network access)
    - The school has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices

    - For all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted
    - Appropriate exit processes are implemented for devices no longer used at a school location or by an authorised user.
    - All mobile devices on the school network are monitored
    - Pro-active monitoring has been implemented to monitor activity
    - The software/apps originally installed by the school must remain on the school owned device in usable condition and be easily accessible at all times. From time to time the school may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps
    - The school will ensure that devices contain the necessary apps for school work. Apps added by the school will remain the property of the school and will not be accessible to learners on authorised devices once they leave the school roll. Any apps bought by the user on their own account will remain theirs.
    - The changing of settings that would stop the device working as it was originally set up and intended to work is not permitted
- When personal devices are permitted:
    - Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school
    - The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home)
    - The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues
    - The school recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Pass-codes or PINs should be set on personal devices to aid security
    - The school is not responsible for the day to day maintenance or upkeep of the user's personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues.
- Users are expected to act responsibly, safely and respectfully in line with current acceptable use agreements, in addition;
    - devices are not permitted in tests or exams
    - there is clear advice and guidance at the point of entry for visitors to acknowledge school requirements
    - Users are responsible for keeping their device up to date through software, security and app updates.
    - Users are responsible for charging their own devices and for protecting and looking after their devices while in the school
    - Confiscation and searching (England) - the school has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.
    - Users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use.
    - The expectations for taking/storing/using images/video aligns with the school's acceptable use policy and use of images/video policy. The non-consensual taking/using of images of others is not permitted.
    - Staff owned devices should not be used for personal purposes during teaching sessions, unless in exceptional circumstances
    - Printing from personal devices will not be possible

Appendix F

St Matthew's Church of England Primary School

Social Media Policy

St Edmundsbury and Ipswich Diocesan Multi Academy Trust

Social media (e.g. Facebook, X, SnapChat, Instagram, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However, some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube have social media elements to them.
St Matthew's school recognises the numerous benefits and opportunities which a social media presence offers. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by the school, its staff, parents, carers and children.

This policy needs to be read in conjunction with:

- Acceptable User Agreement
- Code of Conduct

This policy:

- Applies to all staff and to all online communications which directly or indirectly, represent the school.
- Applies to such online communications posted at any time and from anywhere.
- Encourages the safe and responsible use of social media through training and education
- Defines the monitoring of public social media activity pertaining to the school

The school respects privacy and understands that staff and children may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.

Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

Digital communications with children are also considered. Staff must not use social media to communicate with children.

St Matthew's School currently does not currently have any social media accounts on any platform.

Behaviour

- The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.
- Digital communications by staff must be professional and respectful at all times and in accordance with this policy. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.

- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.
- If a journalist makes contact about posts made using social media staff must follow advice from the MAT.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The use of social media by staff while at work may be monitored, and is actively discouraged during the school day.
- The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

Legal Considerations

- Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

Handling Abuse

- When acting on behalf of the school, respond to harmful and / or offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken
- If you feel that you or someone else is subject to abuse by colleagues through use of online communications, then this action must be reported using the agreed school protocols.

Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing online content are:

- Engaging
- Conversational
- Informative
- Professional

Use of Images

- Under no circumstances should staff share or upload learner pictures online other than via official school channels.

Personal Use

Staff

- Personal communications are those made via a personal online accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive or inappropriate personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

Managing your personal use of Social Media:

- "Nothing" on social media is truly private
- Social media can blur the lines between your professional and private life. Don't use the school logo and/or branding on personal accounts
- Check your settings regularly and test your privacy
- Keep an eye on your digital footprint
- Keep your personal information private
- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem

The Don'ts:

- Don't make comments, post content or link to materials that will bring the school into disrepute
- Don't publish confidential or commercially sensitive material
- Don't breach copyright, data protection or other relevant legislation
- Don't link to, embed or add potentially inappropriate content. Consider the appropriateness of content for any audience of school accounts.
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content
- Don't use social media to air internal grievances

Children

- Staff are not permitted to follow or engage with current or prior pupils of the school on any personal social media account.
- The school's education programme should enable the pupils to be safe and responsible users of social media.
- Pupils are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy

Parents/Carers

- If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.
- The school has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.
- Parents/Carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

Monitoring Posts About the School

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.
- The school should effectively respond to social media comments made by others according to a defined policy or process.

Appendix G:

Legislation

This is the legislative framework under which this online safety policy has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.
It is recommended that legal advice is sought in the advent of an online safety issue or situation.
A useful summary of relevant legislation can be found at: Report Harmful Content: Laws about harmful behaviours

Computer Misuse Act 1990
This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Schools may wish to view the National Crime Agency website which includes information about "Cyber crime – preventing young people from getting involved". Each region in England (& Wales) has a Regional Organised Crime Unit (ROCU) Cyber-Prevent team that works with schools to encourage young people to make positive use of their cyber skills. There is a useful summary of the Act on the NCA site.

Data Protection Act 1998
This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

The Data Protection Act 2018:

Updates the 1998 Act, incorporates the General Data Protection Regulations (GDPR) and aims to:

- Facilitate the secure transfer of information within the European Union.
- Prevent people or organisations from holding and using inaccurate information on individuals. This applies to information regarding both private lives or business.
- Give the public confidence about how businesses can use their personal information.
- Provide data subjects with the legal right to check the information businesses hold about them. They can also request for the data controller to destroy it.
- Give data subjects greater control over how data controllers handle their data.
- Place emphasis on accountability. This requires businesses to have processes in place that demonstrate how they're securely handling data.
- Require firms to keep people's personal data safe and secure. Data controllers must ensure that it is not misused.
- Require the data user or holder to register with the Information Commissioner.

All data subjects have the right to:

- Receive clear information about what you will use their data for.

- Access their own personal information.
- Request for their data to be revised if out of date or erased. These are known as the right to rectification and the right to erasure
- Request information about the reasoning behind any automated decisions, such as if computer software denies them access to a loan.
- Prevent or query about the automated processing of their personal data.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984
It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994
This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003
A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964
Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998
This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial

- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006
Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of learners when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011
Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

http://www.education.gov.uk/schools/learnersupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation)

The Protection of Freedoms Act 2012
Requires schools to seek permission from a parent/carer to use Biometric systems

The School Information Regulations 2012
Requires schools to publish certain information on its website: https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

Serious Crime Act 2015
Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

Criminal Justice and Courts Act 2015
Revenge porn – as it is now commonly known – involves the distribution of private and personal explicit images or video footage of an individual without their consent, with the intention of causing them embarrassment and distress. Often revenge porn is used maliciously to shame ex-partners. Revenge porn was made a specific offence in the Criminal Justice and Courts Act 2015. The Act specifies that if you are accused of revenge porn and found guilty of the criminal offence, you could be prosecuted and face a sentence of up to two years in prison. For further guidance or support please contact the Revenge Porn Helpline

Appendix H:

Links to other Organisations or Documents

The following links may help those who are developing or reviewing a school online safety policy and creating their online safety provision:

UK Safer Internet Centre

Safer Internet Centre – https://www.saferinternet.org.uk/
South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/
Childnet – http://www.childnet-int.org/
Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
Revenge Porn Helpline - https://revengepornhelpline.org.uk/
Internet Watch Foundation - https://www.iwf.org.uk/
Report Harmful Content - https://reportharmfulcontent.com/
Harmful Sexual Support Service

CEOP

CEOP - http://ceop.police.uk/
ThinkUKnow - https://www.thinkuknow.co.uk/

Others

LGfL – Online Safety Resources
Kent – Online Safety Resources page
INSAFE/Better Internet for Kids - https://www.betterinternetforkids.eu/
UK Council for Internet Safety (UKCIS) - https://www.gov.uk/government/organisations/uk-council-for-internet-safety

Tools for Schools / other organisations

Online Safety BOOST – https://boost.swgfl.org.uk/
360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/
360Data – online data protection self-review tool: www.360data.org.uk
SWGfL Test filtering - http://testfiltering.com/
UKCIS Digital Resilience Framework - https://www.gov.uk/government/publications/digital-resilience-framework
SWGfL 360 Groups – online safety self review tool for organisations working with children
SWGfL 360 Early Years - online safety self review tool for early years organisations

Bullying/Online-bullying/Sexting/Sexual Harassment

Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - http://enable.eun.org/
SELMA – Hacking Hate - https://selma.swgfl.co.uk
DfE - Cyberbullying guidance - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf
Childnet – Cyberbullying guidance and practical PSHE toolkit: http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit
Childnet – Project deSHAME – Online Sexual Harrassment
UKSIC – Sexting Resources
Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm
Ditch the Label – Online Bullying Charity
Diana Award – Anti-Bullying Campaign

Social Networking

Digizen – Social Networking
UKSIC - Safety Features on Social Networks
Children's Commissioner, TES and Schillings – Young peoples' rights on social media

Curriculum
SWGfL Evolve - https://projectevolve.co.uk
UKCCIS – Education for a connected world framework
Department for Education: Teaching Online Safety in Schools
Teach Today – www.teachtoday.eu/
Insafe - Education Resources

Data Protection
360data - free questionnaire and data protection self review tool
ICO Guides for Organisations
IRMS - Records Management Toolkit for Schools
ICO Guidance on taking photos in schools

Professional Standards/Staff Training
DfE – Keeping Children Safe in Education
DfE - Safer Working Practice for Adults who Work with Children and Young People
Childnet – School Pack for Online Safety Awareness
UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure/Technical Support/Cyber-security
UKSIC – Appropriate Filtering and Monitoring
SWGfL Safety & Security Resources
Somerset - Questions for Technical Support
SWGfL - Cyber Security in Schools.
NCA – Guide to the Computer Misuse Act
NEN – Advice and Guidance Notes

Working with Parents and Carers
SWGfL – Online Safety Guidance for Parents & Carers
Vodafone Digital Parents Magazine
Childnet Webpages for Parents & Carers
Get Safe Online - resources for parents
Teach Today - resources for parents workshops/education
Internet Matters

Prevent
Prevent Duty Guidance
Prevent for schools – teaching resources
Childnet – Trust Me

Research
Ofcom –Media Literacy Research
Ofsted: Review of sexual abuse in schools and colleges