Marriott Primary

Achieving Together

E-SAFETY 2022-23

Adopted	**29th November 2022**
Signed (Chair of Governors)	**Steve Wilson**
Reviewed	
Signed (Chair of Governors)	

1. Introduction

1.1 Marriott Primary School recognises the Internet and other digital technologies provide a vast opportunity for children and young people to learn. The Internet and digital technologies allow all those involved in the education of children and young people to promote creativity, stimulate awareness and enhance learning.

1.2 As part of our commitment to learning and achievement we at Marriott Primary School want to ensure that the Internet and other digital technologies are used to:

- Raise educational standards and promote pupil achievement.
- Develop the curriculum and make learning exciting and purposeful.
- Enable pupils to gain access to a wide span of knowledge in a way that ensure their safety and security.
- Enhance and enrich their lives and understanding.

To enable this to happened we have taken a whole school approach to E- safety as promoted by British Education Communication Technology Agency (BECTA), which includes the development of policies and practices, the education and training of staff and pupils and the effective use of the School's ICT infrastructure and technologies.

1.3 Marriott Primary School as part of this policy holds steadfastly to the ethos that there should be an equitable learning experience for all pupils using ICT technology within the school. We recognise that ICT can allow disabled pupils increased access to the curriculum and other aspects related to learning.

1.4 Marriott Primary School is committed to ensuring that **all** its pupils, where technologically feasible and within the prevailing financial climate, will be able to use existing, as well as up and coming technologies safely. We are also committed to ensuring that all those who work with children and young people, as well as their parents, (home instruction through acceptable use policy) are educated as to the risks that exist so that they can take an active part in safeguarding children.

1.5 The nominated people for the implementation of the School's e-Safety policy are the Co-Heads, Computing Co-ordinator, IT Technician.

2. Scope of Policy

2.1 The policy applies to:

- all pupils;
- all teaching and support staff (including peripatetic), school governors and volunteers;
- all aspects of the School's facilities where they are used by voluntary, statutory or community organisations.

2.2 Marriott Primary School will ensure that the following elements are in place as part of its safeguarding responsibilities to pupils:

- a list of authorised persons who have various responsibilities for E- safety
- a range of policies including acceptable use policies that are frequently reviewed and updated; information to parents that highlights safe practice for children and young people when using the Internet and other digital technologies
- adequate training for staff and volunteers;
- adequate supervision of pupils when using the Internet and digital technologies;
- education that is aimed at ensuring safe use of Internet and digital technologies;
- Use of Policy Central as a reporting procedure for abuse and misuse.

3. Infrastructure and Technology

3.1 Partnership working

3.1.1 Marriott Primary School recognises that as part of its safeguarding responsibilities there is a need to work in partnership. One of our major partners is the Leicester Gateway who provide the network, services and facilities that support the communication requirements of the East Midlands learning community. As part of our commitment to partnership working, we fully support and will continue to work with them to ensure that pupil and staff usage of the Internet and digital technologies is safe.

3.1.2 Marriott Primary School will, as part of its wider safeguarding responsibilities, seek to ensure that voluntary, statutory and community organisation take an approach to their activities that see the welfare of the child as paramount. To this end, we expect any organisation using the school's ICT or digital technologies to have appropriate policies and procedures that are aimed at safeguarding children and young people and reporting concerns.

4. Policies and Procedures

We at Marriott Primary School understand that effective policies and procedures are the backbone to developing a whole-school approach to E- safety. The policies that exist within Marriott Primary School are aimed at providing a balance between exploring the educational potential of new technologies safeguarding pupils.

4.1 Use of Internet facilities, mobile and digital technologies

4.1.1 Marriott Primary School will seek to ensure that Internet, mobile and digital technologies are used effectively for their intended educational purpose, without infringing legal requirements or creating unnecessary risk.

4.1.2 Marriott Primary School expects all staff and pupils to use the Internet, mobile and digital technologies responsibly and strictly according to the conditions below. These expectations are also applicable to any voluntary, statutory and

community organisations that makes use of the school's ICT facilities and digital technologies.

Users shall not:

- Visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
- Indecent images of children
- Promoting discrimination of any kind promoting racial or religious hatred or promoting illegal acts.
- Any other information which may be offensive to peers or colleagues e.g. abusive images; promotion of violence; violent extremism, gambling; criminally racist or religious hatred material.

4.1.3 The School recognises that in certain planned curricular activities, access to otherwise deemed inappropriate sites may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned and recorded and also permission in writing is given by senior leaders, so that the action can be justified, if queries are raised later. All YouTube videos should be downloaded and played from a local device.

4.1.4 Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will be reported to the Police:

- Images of child abuse (images of children whether they are digital or cartoons, apparently under 16 years old, involved in sexual activity or posed to be sexually provocative)
- Adult material that potentially breaches the Obscene Publications Act in the UK
- Criminally racist or anti-religious material
- Violence and bomb making
- Illegal taking or promotion of drugs
- Software piracy, including use of DVD technology
- Any other criminal activity

1 For the purposes of this document, Internet usage means any connection to the Internet via web browsing, external email, news groups or messaging services, mobile technologies e.g. mobile phone, including Bluetooth applications, PDA's etc.

4.1.5 In addition, users may not:

- Use the Talk Straight or an equivalent broadband provider's facilities for running a private business;
- Enter into any personal transaction that involves Talk Straight or Local Authorities in any way;

- Visit sites that might be defamatory or incur liability on the part of Talk Straight or Local Authorities or adversely impact on the image of Talk Straight;
- Upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties outside of Talk Straight, or to Talk Straight itself; (other than authorised and licensed automatic updates via the network / Internet e.g. Microsoft, Adobe etc.)
- Reveal or publicise confidential or proprietary information, which includes but is not limited to: financial information, personal information, databases and the information contained therein, computer/network access codes, and business relationships;
- Intentionally interfere with the normal operation of the Internet connection, including the propagation of computer viruses and sustained high volume network traffic (sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion) that substantially hinders others in their use of the Internet;
- Use the Internet for soliciting, representing personal opinions or revealing confidential information or in any other way that could reasonably be considered inappropriate. (e.g. Facebook etc.)
- Transmit unsolicited commercial or advertising material either to other user organisations, or to organisations connected to other networks, save where the material is embedded within, or is otherwise part of, a service to which the member of the user organisation has chosen to subscribe.
- Assist with unauthorised access to facilities or services accessible via Talk Straight

Undertake activities with any of the following characteristics:

  - Wasting staff effort or networked resources, including time on end systems accessible via the Talk Straight network and the effort of staff involved in support of those systems;
  - corrupting or destroying other users' data;
  - violating the privacy of other users;
  - disrupting the work of other users;
  - using the Talk Straight network in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment);
  - continuing to use an item of networking software or hardware after Talk Straight has requested that use cease because it is causing disruption to the correct functioning of Talk Straight;
  - other misuse of the Talk Straight network, such as introduction of viruses.

- Use any mobile or digital technologies 3G or mobile Internet services in any way to intimidate, threaten or cause harm to others. Moreover, mobile technologies should not be used to access inappropriate materials or encourage activities that are dangerous or illegal.

4.1.6 Where Talk Straight (provider of Internet connectivity and associated services to schools) and/or Talk Straight become aware of an illegal act or an attempted illegal act, they will have to comply with the law as it applies and will take action directed by the police if a Regulation of Investigatory Powers Act (RIPA) Notice is issued.

4.2 Reporting Abuse

4.2.1 There will be occasions when either a pupil or an adult within the school receives an abusive email or accidentally accesses a website that contains abusive material. When such a situation occurs, the expectation of the school is that the pupil or adult should be report the incident **immediately**. Pupils will be introduced to the CEOP website and instructed how to report inappropriate content.

4.2.2 The School also recognises that there will be occasions where pupils will be victims of inappropriate behaviour that could lead to possible or actual significant harm. The response of the School will be to take the reporting of such incidents seriously and where judged necessary, the Designated Senior Person for Child Protection within the School will refer details of an incident to the lead agencies involved in safeguarding children, namely Children's Social Care and the Police.

The School, as part of its safeguarding duty and responsibilities will assist and provide information and advice in support of child protection enquiries and criminal investigations.

5. Education and Training

5.1 Marriott Primary School recognises that the Internet and other digital technologies can transform learning; help to improve outcomes for children and young people; promote creativity; all of which add up to a more exciting and challenging classroom experience.

5.2 As part of achieving this, we want to create within Marriott Primary School an accessible system, with information and services online, which support personalised learning and choice. However, we realise that it will be necessary for our pupils to have the skills of critical awareness, digital literacy and good online citizenship to enable them to use the Internet and other digital technologies safely.

5.3 To this end, Marriott Primary School will:-

- Enable all pupils to exercise the skills of critical awareness, digital literacy and good online citizenship as part of the school curriculum.
- Educate school staff so that they are equipped to support pupils in gaining positive experiences when online and can help pupils develop strategies if they encounter a problem.

- Support parents in gaining an appreciation of Internet safety for their children and provide them with relevant information on the policies and procedures that govern the use of Internet and other digital technologies within the school.

6. Standards and Inspection

Marriott Primary School recognises the need to have regular inspections of policies and procedures in order to ensure that its practices are effective and that the risks to pupils are minimised.

6.1 Monitoring

6.1.1 Monitoring the safe use of the Internet and other digital technologies goes beyond the personal use of the Internet and electronic mail a pupil or member of staff may have. Marriott Primary School recognises that in order to develop an effective whole school E-safety approach there is a need to monitor patterns and trends of use inside school and outside school, through regular survey and home agreement documents. (Education and Inspections Act 2006, Section 89(5)).

6.1.2 With regard to monitoring trends, within the school and individual use by school staff and pupils, Marriott Primary School will audit the use of the Internet and electronic mail in order to ensure compliance with this policy. The monitoring practices of the school are influenced by a range of national and Local Authority guidance documents and will include the monitoring of content and resources by the use of Policy Central.

6.1.3 Another aspect of monitoring, which our school will employ, is the use of mobile technologies by pupils, particularly where these technologies may be used to cause harm to others, e.g. bullying (see anti-bullying policy for further information). We will also ensure that school staff understand the need to monitor our pupils, and where necessary, support individual pupils where they have been deliberately or inadvertently been subject to harm.

6.1.4 The school's internet, network and ICT systems and subscriptions to services should be used with the utmost professionalism at all times. The school will aim to provide its staff with secure systems which will have filtering, monitoring and virus protection included. Anyone with access to the systems should be aware that their use of the systems is monitored, and this can be used to form evidence should any suspected infringements occur.

6.2 Sanctions

6.2.1 Where there is inappropriate or illegal use of the Internet and digital technologies, the following sanctions will be applied:

6.2.2

- Child / Young Person

- The child/young person will be disciplined according to the behaviour policy of the school, which could ultimately include the use of Internet and email being withdrawn.
- Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal Internet use or child protection concerns.
- Adult (Staff and Volunteers)
- The adult may be subject to the disciplinary process, if it is deemed he/she has breached the policy
- Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal Internet use or child protection concerns.

6.2.3 If inappropriate material is accessed, children are taught to immediately turn off the monitor and report to an adult. Adult to then report to a member of the ICT working group. Member of ICT working group to contact filtering services and ICT technician and to speak to the child concerned and their parents. Incident to be logged and reported to the Headteacher. As part of the schools Long Term Plans every class will participate in half termly e-safety lessons.

7. Working in Partnership with Parents and Carers

7.1 Marriott Primary School is committed to working in partnership with parents and carers and understands the key role they play in the Internet safety of their children, through promoting Internet safety at home and elsewhere.

7.2 We at Marriott Primary School also appreciate that there may be some parents who are concerned about the use of the Internet, email and other digital technologies in school. In such circumstances school staff will meet with parents and carers to discuss their concerns and agree upon a series of alternatives that will allow their child to fully access the curriculum, whilst remaining safe.

8. Appendices of the E-safety Policy

8.1 There are multiple aspects of the school's E-safety policy, which include acceptable use policies for both staff and pupils; Social Media policy, ICT equipment (onsite and offsite); data security and retention. The various policy documents relating to these aspects of the school's E-safety policy can be obtained from the ICT Coordinator for scrutiny, if required.

All parents will be required to complete a Pupil Acceptable User form (Appendix A) when their child joins the school.

All staff/governors/volunteers/visitors will be required to complete an Acceptable User form (Appendix B) when they join the school.

8.2 With the introduction of the online platform "ClassDojo", used for remote learning during Coronavirus restrictions and beyond, please see "ClassDojo Policy" for more information and see appendices below appertaining information about eSafety within this platform.

APPENDIX A

PUPILS ACCEPTABLE USER POLICY/AGREEMENT

I understand that while I am a member of Marriott Primary School I must use technology in a responsible way.

For my own personal safety:

- *I understand that my use of technology will be monitored*
- *I will keep my password safe and will not use anyone else's (even with their permission)*
- *I will keep my own personal information safe as well as that of others. (My name, family information, journey to school, my pets and hobbies are all examples of personal information)*
- *I will tell a trusted adult if anything makes me feel uncomfortable or upset when I see it online*
- *I will only use e-mail which has been provided by the school*
- *I will always check with a responsible adult and my parents before I show photographs of myself*
- *I will never meet an online friend in person without taking a responsible adult that I know with me*

For the safety of others:

- *I will not interfere with the way that others use their technology*
- *I will be polite and responsible when I communicate with others*
- *I will not take or share images of anyone without their permission*

For the safety of the school:

- *I will not try and access anything illegal*
- *I will not download anything that I do not have the right to use*
- *I will not deliberately bypass any systems designed to keep the school safe (such as filtering of the internet)*
- *I will tell a responsible person if I find any damage or faults with technology, however this may have happened*
- *I will not attempt to install programmes on ICT devices belonging to the school unless I have permission*
- *I will only use social networking, gaming and chat through the sites the school allows*

I know that once I post a message or an item on the internet then it is completely out of my control. I understand that I am responsible for my actions and the consequences. I have read and understood the above and agree to follow these guidelines

Signed_____ **Childs name**

Signed _____ **Parents name**

Date _____

APPENDIX B – ACCEPTABLE USE AGREEMENT

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Report inadvertent use of a violent, criminal or child pornographic nature at home either by myself or by somebody in my household
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

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

APPENDIX C – COMMON CLASSDOJO POLICY QUESTIONS BY PARENTS

What is Class Dojo used for?
Class Dojo is a school communication platform that connects teachers, students, and families, and brings them closer together. This is done in two ways. One, by sharing what's being learned in the classroom back home through portfolios, photos, videos, and messages. And, two, by helping students build social-emotional skills through in-classroom feedback and engaging activities. These relationships require trust, which is why we've made sure Class Dojo is a safe and private environment for teachers, parents, and students.

Who can view the information teachers enter about a student?
Only the student themselves, their families, and their connected teachers or school leaders can see a student's profile and portfolio.

Where is student data stored?
Class Dojo's servers are in highly secure, military-grade data centres that are access-controlled. Class Dojo uses bank-grade security at the software and network level to ensure all information is transmitted securely. We work with independent security researchers to test Class Dojo's security practices, and those of any third-party partners, including extensive independent audits by world-class cyber-security firms to put our systems and protocols under extreme, unbiased scrutiny.

How long is student information stored?
We protect students with our industry-leading policy: we don't keep student personal information schools don't need and we delete students' feedback points after 12 months.

Will information ever be sold or rented to other organizations?
No. On Class Dojo, your personal information is yours. Class Dojo never sells or rents personal information to any third parties, for any reason.

In Europe, does Class Dojo comply with GDPR?
Yes. Class Dojo will be compliant with GDPR when it comes into effect on May 25, 2018. We are also certified under the EU-US and Swiss-US Privacy Shield.

What if I'm not in the U.S. or the EU?
Class Dojo is used in over 180 countries, so we are always improving how we operate given where our teachers are. For instance, we comply with Canada's Personal Information Protection and Electronic Documents Act (PIPEDA). If you have questions about your specific country, please contact us at privacy@classdojo.com.

APPENDIX D – COMMON CLASSDOJO POLICY QUESTIONS BY TEACHERS

What is ClassDojo used for?
Class Dojo is a school communication platform that connects teachers, students, and families, and brings them closer together. This is done in two ways. One, by sharing what's being learned in the classroom back home through portfolios, photos, videos, and messages. And, two, by helping students build social-emotional skills through in-classroom feedback and engaging activities. These relationships require trust, which is why we've made sure Class Dojo is a safe and private environment for teachers, parents, and students.

Will Class Dojo always be free for teachers?
Yes. Class Dojo will always be free for teachers. In the future, we plan to create premium features that parents, schools, or districts may pay for.

Who can view the information teachers enter about a student?
Only the student themselves, their families, and their connected teachers or school leaders can see a student's profile and portfolio.

Where is student data stored?
Class Dojo's servers are in highly secure, military-grade data centres that are access-controlled. Class Dojo uses bank-grade security at the software and network level to ensure all information is transmitted securely. We work with independent security researchers to test Class Dojo's security practices, and those of any third-party partners, including extensive independent audits by world-class cyber-security firms to put our systems and protocols under extreme, unbiased scrutiny.

How long is student information stored?
We protect students with our industry-leading policy: we don't keep student personal information schools don't need and we delete students' feedback points after 12 months.

Will information ever be sold or rented to other organizations?
No. On Class Dojo, your personal information is yours. Class Dojo never sells or rents personal information to any third parties, for any reason.

In Europe, does Class Dojo comply with GDPR?
Yes. Class Dojo will be compliant with GDPR when it comes into effect on May 25, 2018. We are also certified under the EU-US and Swiss-US Privacy Shield.

What if I'm not in the U.S. or the EU?
Class Dojo is used in over 180 countries, so we are always improving how we operate given where our teachers are. For instance, we comply with Canada's Personal Information Protection and Electronic Documents Act (PIPEDA). If you have questions about your specific country, please contact us at privacy@classdojo.com.

APPENDIX E – CLASSDOJO INFORMATION TRANSPARENCY

ClassDojo is committed to being transparent with how we handle your information, in full compliance with local, national, and international laws like GDPR, COPPA, FERPA, and others.

Below you can see what information we collect, why and how we collect it, where it's stored, and how it's different for each type of user on our platform.

Types of information shared
First and Last Name
Account types that share this information
Teacher, Parent, School leader, and Student (via teacher)

How ClassDojo collects this data
Directly by the user on our website, or mobile app, or if its the student by the teacher; via the School Directory by teachers and school leaders; also, when users fill out surveys or contact us via Customer Service/email

The purpose for ClassDojo collecting this information
Establishing one's identity within a school community, or for support needs/responding to surveys; to invite more teachers via the School Directory

How this information is used
To send an SMS message to invite a (potentially) non-logged in user to ClassDojo; if for support or a survey, to let a ClassDojo team member contact the individual

Where is this data stored (and which third-party service providers hold it, if any)
Data stored on AWS servers in the U.S. and MLab in the U.S.; back-ups are in the same locations (AWS/MLab in the U.S.); Zendesk in the U.S.; SurveyMonkey in the U.S.

Is this data shared with any other third-party service providers, and if so, who and for what reason?
Sendgrid in the U.S., to help us send friendlier emails

Is this information transferred outside of the European Economic Area (EEA)?
Yes - to the U.S.

What is the legal basis for processing this information under the GDPR?
Legitimate interest and performance of contract