MARISH

Academy Trust

E-Safety Policy and Acceptable Use of ICT Agreements Policy

Date: 6/10/19 **Version:** 5.0

Summary

We understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. This policy describes our approach to e-safety issues.

Authors: Gill Denham

Contents

1. Introduction 4

2. Roles and Responsibilities..5

 2.1. The named e-safety co-ordinators in each Trust school and ICT Team....................5

 2.2. Managing the school e-safety messages 6

3. E-safety in the Curriculum 6

4. Managing Internet Access 7

 4.1. E-mail...7

 4.2. Publishing pupil's images and work 8

 4.3. Social networking and personal publishing 8

 4.4. Personal use of social network sites by staff 9

 4.5. Video Conferencing...10

 4.6. Managing emerging technologies..10

5. Password Security...10

6. Data protection..11

7. Responding to E-Safety Incidents/Complaints 11

8. Cyberbullying 11

 8.1. Preventing Cyberbullying 12

 8.2. Supporting the person being bullied..13

 8.3. Investigating Incidents 13

 8.4. Working with the bully and sanctions...13

9. Communications Policy...14

 9.1. Introducing the e-safety policy to pupils 14

 9.2. Introducing staff to the e-safety policy...14

 9.3. Enlisting parents' support 14

10. Equal Opportunities..15

 10.1. Pupils with additional needs 15

11. Reviewing this Policy...15

12 Approval History 16

Appendix 1 - Primary Pupil Acceptable Use of ICT..17

Appendix 2 - Acceptable Use of ICT Agreement Staff, Governors and Visitors.........................19

Appendix 3 - Guidelines for Staff on social networking...21

Appendix 4 - Marish Academy Trust E-Safety Incident Log 24
Appendix 5 - Advice for Children on Cyber-bullying 25
Appendix 6 - Laptop Loan Form 28

1. Introduction

ICT in the 21st Century is an essential resource to support learning and teaching, as well as being an integral part of the everyday lives of children, young people and adults. Consequently, we need to develop the use of these technologies in order to arm our young people with the skills to access lifelong learning and employment.

Information and Communications Technology covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast-paced evolution of ICT within our society as a whole. Currently, the Internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Marish Academy Trust**,** we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the Internet and related technologies, in and beyond the context of the classroom.

‘Schools are finding that a blocking and banning approach, which merely limits exposure to risk, may no longer be a sustainable approach… Schools need to focus on a model of empowerment; equipping children with the skills and knowledge they need to use technology safely and responsibly, and managing the risks’

Becta Safeguarding Children Online Feb 2009

Marish has a Trust wide approach to the safe use of ICT. Creating a safe ICT learning environment includes three main elements at all our schools

- An effective range of technological tools
- Policies and procedures, with clear roles and responsibilities
- A comprehensive e-safety education programme for pupils, staff and parents.

2. Roles and Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in the Academy Trust and the Executive Head teacher, with the support of the Governors, aims to embed safe practices into the culture of each school. The Executive Head teacher ensures that the policy is implemented and has ultimate responsibility to ensure that the policy and practices are embedded and monitored.

2.1. The named e-safety co-ordinators in each Trust school and ICT Team

The role of the ICT coordinator encompasses the responsibility of monitoring the e-safety policy in each school with the technical support of the Trust Network Manager, the ICT team and a designated safeguarding officer (who is part of the ICT team). The ICT team are required to keep abreast of current issues and guidance through organisations such as Becta, CEOP Command, and Child Net.

The ICT team ensures the Executive Head teacher; Academy Leadership and School Senior Leadership Teams and Governors are updated as necessary. They will meet half termly to address any issues or needs the Trust and pupils within the Trust may have. This will include, but is not limited to: safeguarding issues, updating the website, ensuring staff training is up to date and that parental education and engagement is considered.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following Trust e-safety procedures.

All staff should be familiar with the Trust's policy including:

- safe use of e-mail
- safe use of the Internet
- safe use of the school network, equipment and data
- Ensuring the website is compliant with statutory guidance
- safe use of digital images and digital technologies, such as mobile phones and digital cameras
- publication of pupil information/photographs on the school website
- procedures in the event of misuse of technology by any member of the school community (see appendices)

- their role in providing e-safety education for pupils
- the safe use of social media
- the importance of confidentiality

Staff are reminded/updated about e-safety regularly and new staff receive information on the Trust's acceptable use policy as part of their induction. All Trust employees and supply staff must sign an acceptable use of ICT agreement before using technology equipment in school (see appendix 2 for staff acceptable use agreement).

2.2. Managing the school e-safety messages

- We endeavour to embed e-safety messages across the curriculum whenever the Internet and/or related technologies are used.
- The e-safety policy will be shared with new staff, including the acceptable use policy as part of their induction.
- E-safety posters will be prominently displayed.
- Regular parental engagement supporting the understanding and use of the internet within the home.

3. E-safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety.

- E- folio is set up for every child in the school.
- We provide opportunities within a range of curriculum areas to teach about e-safety.
- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the curriculum.
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling, and activities as part of the ICT curriculum.
- Pupils are aware of the impact of online bullying through PSHE and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies (see Cyberbullying below).
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

4. Managing Internet Access

The Internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to everyone.

- Students will have supervised access to Internet resources through the school's fixed and mobile Internet technology.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- Our Internet access is controlled through web filtering device.
- Staff and pupils are aware that school based email and Internet activity can be monitored and explored further if required.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the ICT co-ordinator and a member of the Trust ICT Team.
- It is the responsibility of the Trust, by delegation to the Trust Network Manager, to ensure that antivirus protection is installed and kept up-to-date on all school machines.

4.1. E-mail

The use of email within school is an essential means of communication for both staff and pupils.

In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age. In order to achieve ICT level 4 or above, pupils must have experienced sending and receiving emails.

- Pupils are introduced to email as part of the ICT Scheme of Work.
- The school gives staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- Under no circumstances should staff contact pupils or parents using personal email addresses.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- The forwarding of chain letters is not permitted in school.

- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
- All pupils must use appropriate language in e-mails and must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone.
- Staff must inform the e-safety co-ordinator if they receive an offensive e-mail.

4.2. Publishing pupil's images and work

On a child's entry to the school, all parents/guardians will be asked to give permission for their child's photo to be taken and to use their child's work/photos in the following ways:

- on the school web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically.)

Pupils' names will not be published alongside their image and vice versa without permission from the parents. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

Before posting pupils' work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

4.3. Social networking and personal publishing

We block/filter access for pupils and staff in school to social networking sites. Pupils will be advised never to give out personal details of any kind which may identify them or their location. Pupils and parents are advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

We acknowledge the prevalence of various formats of social media that may well be used in pupils' homes and that they may well have access to. Regardless of age restrictions, all forms of social media are banned within school. The Trust will seek to actively work with parents to support all pupils to understand the reasons for this.

It is crucial that pupils, parents and the public at large have confidence in the Trust's decisions and services. The principles set out in this policy are designed to ensure that staff members use social media responsibly so that confidentiality of pupils and other staff and the reputation of the schools and Marish Academy Trust are safeguarded. This policy covers personal use of social media as well as the use of social media for official school purposes, including sites hosted and maintained on behalf of the school or the Academy Trust.

The Trust does operate a twitter account. This conforms to our strict confidentiality standards, ensuring no pupils or their locations should ever be disclosed through this account. The primary purpose of this account is to increase lines of communication with parents, it's primary use is to pass on sporting results and celebrate our pupils' achievements.

The Trust also operates an information messaging service through the school app. This is limited to sending school related information and enabling staff, pupils and children to receive reminders.

4.4. Personal use of social network sites by staff

This policy applies to personal webspace such as social networking sites, blogs, microblogs such as *Twitter*, chatrooms, forums, podcasts, open access online encyclopaedias such as *Wikipedia,* social bookmarking sites such as *del.icio.us* and content sharing sites such as *flickr* and *YouTube*. The Internet is a fast moving technology and it is impossible to cover all circumstances or emerging media - the principles set out in this policy must be followed irrespective of the medium.

Marish Academy Trust is committed to ensuring that all staff members provide confidential services that meet the highest standards. All individuals working on behalf of the Trust are bound by a legal duty of confidence and other laws to protect the confidential information they have access to during the course of their work. Disclosure of confidential information on social media is likely to be a breach of a number of laws and professional codes of conduct, including:

- the Human Rights Act 1998
- Common law duty of confidentiality, and
- the Data Protection Act 1998.

Confidential information includes, but is not limited to:

- Person-identifiable information, e.g. pupil and employee records protected by the Data Protection Act 1998
- Information divulged in the expectation of confidentiality
- School or County Council business or corporate records containing organisationally or publicly sensitive information
- Any commercially sensitive information such as information relating to commercial proposals or current negotiations, and
- Politically sensitive information.

Staff members should also be aware that other laws relating to libel, defamation, harassment and copyright may apply to information posted on social media, including:

- Libel Act 1843
- Defamation Acts 1952 and 1996
- Protection from Harassment Act 1997
- Criminal Justice and Public Order Act 1994
- Malicious Communications Act 1998
- Communications Act 2003, and

- Copyright, Designs and Patents Act 1988.

Marish Academy Trust could be held vicariously responsible for acts of their employees in the course of their employment. For example, staff members who harass co-workers online or who engage in cyber bullying or discrimination on the grounds of race, sex, disability, etc or who defame a third party while at work may render Marish Academy Trust liable to the injured party.

4.5. Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences
- All pupils are supervised by a member of staff when video conferencing
- Approval from the Headteacher is sought prior to all video conferences within school.

4.6. Managing emerging technologies

Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed.

- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff mobile usage at school is covered in the Mobile Phone policy

5. Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy
- Users are provided with an individual network and email log-in username.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- If a password may have been compromised or someone else has become aware of the password the child or adult must report this to the e-safety co-ordinator
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, e-mail accounts, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.

6. Data protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998

- Data can only be accessed and used on school computers or laptops. Staff are aware they must not use their personal devices for accessing any school/ children/ pupil data.

The Data Protection Act 1998 requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

http://www.hmso.gov.uk/acts/acts1998/19980029.htm

7. Responding to E-Safety Incidents/Complaints

As a Trust we will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the Academy Trust nor its schools can accept liability for material accessed, or any consequences of Internet access. Complaints relating to e-safety should be made to the ICT co-ordinator, ICT team and the safeguarding officer. Any complaint about staff misuse must be referred to the Executive Head teacher. Incidents should be logged and the flowcharts for managing an e-safety Incident should be followed (see appendices).

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the ICT co-ordinator.

- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT co-ordinator, depending on the seriousness of the offence; investigation by the Head teacher/ Slough LEA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences

- Pupils and parents will be informed of the complaints procedure.

- Parents and pupils will need to work in partnership with staff to resolve issues.

8. Cyberbullying

Cyberbullying is the use of ICT, particularly mobile phones and the Internet, deliberately to upset someone else. The whole trust-wide community has a duty to protect all its members and provide a safe, healthy environment. The Educations and Inspections Act 2006 states that Head teachers have the power ‘to such an extent as is reasonable’ to regulate the conduct of pupils when they are off site.

Although bullying is not a specific criminal offence in the UK law, there are laws that can apply in terms of harassing or threatening behaviour, for example, or indeed menacing and threatening communications.

There are many types of cyber-bullying. Here are some of the more common:

- **Text messages** —that are threatening or cause discomfort - also included here is "bluejacking" (the sending of anonymous text messages over short distances using "Bluetooth" wireless technology)
- **Picture/video-clips** via mobile phone cameras - images sent to others to make the victim feel threatened or embarrassed.
- **Mobile phone calls** — silent calls or abusive messages; or stealing the victim’s phone and using it to harass others, to make them believe the victim is responsible.
- **Emails** — threatening or bullying emails, often sent using a pseudonym or somebody else’s name.
- **Chatroom bullying** — menacing or upsetting responses to children or young people when they are in web-based chatroom.
- **Instant messaging** (IM) — unpleasant messages sent while children conduct real-time conversations online using a range of over changing platforms
- **Bullying via websites** — use of defamatory blogs (web logs), personal websites and online personal “own web space” sites such as, but not limited to Instagram and Facebook.

The best way to deal with Cyberbullying is to prevent it happening in the first place and to have clear steps to take when responding to it.

8.1. Preventing Cyberbullying

It is important that we work in partnership with pupils and parents to educate them about Cyberbullying as part of our e-safety curriculum.

They should:

- understand how to use these technologies safely and know about the risks and consequences of misusing them
- know what to do if they or someone they know are being cyber bullied.
- report any problems with Cyberbullying. If they do have a problem, they can talk to the school, parents, the police, the mobile network (for phone) or the Internet Service Provider (ISP) to do something about it
- See Investigating Incidents below for more detail.

Additional online advice on how to react to Cyberbullying can be found on **www.kidscape.org** and **www.wiredsafety.org**

See appendices for Key Safety Advice for children, parents and carers.

8.2. Supporting the person being bullied

- Give reassurance that the person has done the right thing by telling someone and inform parents.
- Make sure the person knows not to retaliate or return the message.
- Help the person keep relevant evidence for any investigation (taking screen capture shots, not deleting messages.)
- Check the person knows how to prevent it from happening again e.g. blocking contacts, changing contact details.
- Take action to contain the incident when content has been circulated:
    - remove content
    - contact the host (social networking site) to get the content taken down
    - use disciplinary powers to confiscate phones that are being used to cyber bully
    - ask the pupil who they have sent messages to
    - in case of illegal content (see appendix managing an e-safety incident involving illegal activity.)

8.3. Investigating Incidents

All bullying incidents should be recorded and investigated in the Marish Academy Trust e-safety incident log. We will:

- advise pupils and staff to try and keep a record of the bullying as evidence
- take steps to identify the bully, including looking at the schools' systems, identifying and interviewing possible witnesses, and contacting the service provider and police if necessary. The police will need to be involved to enable the service provider to look into the data of another user.

8.4. Working with the bully and sanctions

- Once the bully is identified, steps should be taken to change their attitude and behaviour by educating them about the effects of Cyberbullying on others
- Technology specific sanctions for pupil engaged in Cyberbullying behaviour could include limiting or refusing internet access for a period of time or removing the right to bring a mobile into school.
- Factors to consider when determining the appropriate sanctions include:
- the impact on the victim: was the bully acting anonymously, was the material widely circulated and humiliating, how difficult was controlling the spread of material?

- the motivation of the bully: was the incident unintentional or retaliation to bullying behaviour from others?

9. Communications Policy

9.1. Introducing the e-safety policy to pupils

- E-safety rules will be posted in all networked rooms and discussed with pupils at the start of each year (see appendices for e-safety posters for KS1 and KS2.)
- Pupils will be informed that network and Internet use will be monitored.
- E-safety will be included more prominently in both the PSHE and ICT curriculum. Each new ICT unit for all years will involve e-safety lessons.

9.2. Introducing staff to the e-safety policy

- All staff will be given the e-safety policy and its application and importance will be explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff training in safe and responsible Internet use and on our e-safety policy will be provided as required.

9.3. Enlisting parents' support

We believe that it is essential for parents/ carers to be fully involved with promoting e-safety both in and outside of school. We regularly consult and discuss e-safety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- The Trust disseminates information to parents relating to e-safety where appropriate in the form of:
    - Information and celebration evenings
    - Posters
    - Website postings
    - Newsletter items
- Parents/carers are asked to read through and sign acceptable use of ICT agreements on behalf of their child on admission to school (see appendix).
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website)
- A partnership approach with parents will be encouraged. This includes parents' evenings with suggestions for safe home Internet use.

- Advice on filtering systems and educational activities that include safe use of the Internet will be made available to parents.

10. Equal Opportunities

10.1. Pupils with additional needs

Staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-safety. Internet activities are planned and well managed for these children.

11. Reviewing this Policy

There will be an on-going opportunity for staff to discuss with the ICT co-ordinator and ICT team any issue of e-safety that concerns them. The ICT team will meet each half term to ensure the Trust is up to date and compliant. It will also seek to address and educate the Trust about emerging technology and issues which face pupils and staff with regards to ICT and social media.

This policy will be reviewed bi-annually and consideration given to the implications for future whole school development planning. The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

12 Approval History

Version	Date	Author(s)	Comments
1.0	19/08/2011	HT	
2.0	19/10/2013	HT	
3.0	26/10/2015	AW	
4.0	Oct 2017	AW	
5.0	Oct 2019	AHT	

Version	Approved	Comments
4.0	Oct 2017	SB
5.0	Oct 2019	SB

Appendix 1 - Primary Pupil Acceptable Use of ICT

Agreement/eSafety Rules

- I will only use ICT in school for school purposes.
- I will only use my class e-mail address or my own school e-mail address when e-mailing.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will not bring software, CDs or ICT equipment into school without permission.
- I will only use the Internet after being given permission from a teacher.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be upsetting or not allowed at school. If I accidentally find anything like this, I will close the screen and tell a teacher immediately.
- I will not give out my own details such as my name, phone number or home address.
- I will not use technology in school time to arrange to meet someone unless this is part of a school project approved by a teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I know that the school may check my use of ICT and monitor the Internet sites I have visited, and that my parent/carer will be contacted if a member of school staff is concerned about my eSafety.

MARISH ACADEMY TRUST

Dear Parents/Carers,

ICT, including the internet, e-mail and mobile technologies, has become an important part of learning in schools. We expect all children to be safe and responsible when using any ICT.

Please read and discuss with your child the e-Safety rules overleaf and return this sheet signed by both you and your child. If you have any concerns or would like some explanation, please contact your child's class teacher.

This Acceptable Use of ICT Agreement is a summary of our e-Safety Policy which is available in full, via our publications scheme, on request at the office or can be viewed on our school website.

Yours sincerely,

Headteacher eSafety co-ordinator

Pupil:

I have read, understood and agreed with the Rules for Acceptable use of ICT.

Signed …………………………………………. (child)

Parent's/Carer's Consent for Internet Access

I have read and understood the school rules for Acceptable Use of ICT and give permission for my son / daughter to access the Internet in school. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that should my son/daughter need to access e-folio at home or anywhere else, that I will take all reasonable precautions to ensure he/she cannot access inappropriate materials and that he/she will use the computer in an appropriate manner.

Signed…………………………..…………… (parent/carer) Date………………………….

Appendix 2 - Acceptable Use of ICT Agreement Staff, Governors and Visitors

Acceptable Use Agreement / Code of Conduct

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Trust e-safety coordinators.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- I will not use or install any hardware (including USB sticks) or software without permission from the e-safety co-ordinators.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head teacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged.
- If a password may have been compromised or someone else has become aware of my password I will report this immediately to the e-safety co-ordinator.
- I will ensure that workstations are not left unattended and unlocked.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, including my use of any social networking site swill not bring my professional role into disrepute.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

- I will ensure that only children whose parents have given permission for them to use the Internet and ICT are enabled to do so at school.

By signing this Acceptable Use Agreement I am demonstrating that I have read, understood and agree to be bound by the Trust's e-safety Policy.

Signature …………………………………... Date ……………………

Full Name ………………………………….. Job title: …………………………………………………………..

Appendix 3 - Guidelines for Staff on social networking.

Principles for Staff- when networking– BE PROFESSIONAL, RESPONSIBLE AND RESPECTFUL

1. You must be conscious at all times of the need to keep your personal and professional lives separate. You should not put yourself in a position where there is a conflict between your work for the Trust and your personal interests.

2. You must not engage in activities involving social media which might bring Marish Academy Trust into disrepute.

3. You must not represent your personal views as those of Marish Academy Trust on any social medium.

4. You must not discuss personal information about pupils, Marish Academy Trust and other professionals you interact with as part of your job on social media.

5. You must not use social media and the internet in any way to attack, insult, abuse or defame pupils, their family members, colleagues, other professionals, other organisations, or Marish Academy Trust.

6. You must be accurate, fair and transparent when creating or altering online sources of information on behalf of Marish Academy Trust.

7. Staff members must not identify themselves as employees of Marish Academy Trust or service providers for the schools in their personal webspace. This is to prevent information on these sites from being linked with the Trust and the schools and to safeguard the privacy of staff members, particularly those involved in providing sensitive frontline services.

8. Staff members must not have contact through any personal social medium with any pupil, whether from Marish Academy Trust or any other school, unless the pupils are family members.

9. Staff members must not have any contact with pupils' family members through personal social media if that contact is likely to constitute a conflict of interest or call into question their objectivity.
10. If staff members wish to communicate with pupils through social media sites or to enable pupils to keep in touch with one another, they can only do so with the approval of the Trust and through official school sites created according to the requirements specified in Appendix A.

11. Staff members must decline 'friend requests' from pupils they receive in their personal social media accounts.

12. On leaving Marish Academy Trust's service, staff members must not contact pupils by means of personal social media sites. Similarly, staff members must not contact pupils from their former schools by means of personal social media.

13. Information staff members have access to as part of their employment, including personal information about pupils and their family members, colleagues and other parties and school or Trust corporate information must not be discussed on their personal webspace.

14. School or Trust email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media.

15. Staff members must not edit open access online encyclopaedias such as *Wikipedia* in a personal capacity at work. This is because the source of the correction will be recorded as the employer's IP address and the intervention will, therefore, appear as if it comes from the employer itself.

16. Marish Academy Trust or individual schools' corporate, service or team logos or brands must not be used or published on personal webspace.

17. Marish Academy Trust does not permit personal use of social media while at work. Staff members are expected to devote their contracted hours of work to their professional duties and, in practice, personal use of the internet should not be on the school's time.

18. Caution is advised when inviting work colleagues to be 'friends' in personal social networking sites. Social networking sites blur the line between work and personal lives and it may be difficult to maintain professional relationships or it might be just too embarrassing if too much personal information is known in the work place.

19. Staff members are strongly advised to ensure that they set the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy. Staff members should keep their passwords confidential, change them often and be careful about what is posted online; it is not safe to reveal home addresses, telephone numbers and other personal information. It is a good idea to use a separate email address just for social networking so that any other contact details are not given away.

Appendix 4 - Marish Academy Trust E-Safety Incident Log

Details of **ALL** e-safety incidents to be recorded in the Incident Log by the e-safety coordinator. This incident log will be monitored termly by the e-safety co-ordinator and Headteacher.

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

Appendix 5 - Advice for Children on Cyber-bullying

If you're being bullied by phone or the Internet

- Remember, bullying is never your fault. It can be stopped and it can usually be traced.
- Don't ignore the bullying. Tell someone you trust, such as a teacher or parent, or call an advice line.
- Try to keep calm. If you are frightened, try to show it as little as possible. Don't get angry, it will only make the person bullying you more likely to continue.
- Don't give out your personal details online - if you're in a chatroom, watch what you say about where you live, the school you go to, your email address etc. All these things can help someone who wants to harm you build up a picture about you.
- Keep and save any bullying emails, text messages or images. Then you can show them to a parent or teacher as evidence.
- If you can, make a note of the time and date bullying messages or images were sent, and note any details about the sender.

There's plenty of online advice on how to react to cyberbullying. For example,

www.kidscape.org and **www.wiredsafety.org** have some useful tips:

Text/video messaging

You can easily stop receiving text messages for a while by turning off incoming messages for a couple of days. This might stop the person texting you by making them believe you've changed your phone number. To find out how to do this, visit

www.wiredsafety.org.

- If the bullying persists, you can change your phone number. Ask your mobile service provider.
- Don't reply to abusive or worrying text or video messages. Your mobile service provider will have a number for you to ring or text to report phone bullying. Visit their website for details.
- Don't delete messages from cyberbullies. You don't have to read them, but you should keep them as evidence.

Text harassment is a crime. If the calls are simply annoying, tell a teacher, parent or carer. If they are threatening or malicious and they persist, report them to the police, taking with you all the messages you've received.

Phone calls

If you get an abusive or silent phone call, don't hang up immediately. Instead, put the phone down and walk away for a few minutes. Then hang up or turn your phone off.

Once they realise they can't get you rattled, callers usually get bored and stop bothering you.

- Always tell someone else: a teacher, youth worker, parent, or carer. Get them to support you and monitor what's going on.
- Don't give out personal details such as your phone number to just anyone. And never leave your phone lying around. When you answer your phone, just say 'hello', not your name. If they ask you to confirm your phone number, ask what number they want and then tell them if they've got the right number or not.

You can use your voicemail to vet your calls. A lot of mobiles display the caller's number. See if you recognise it. If you don't, let it divert to voicemail instead of answering it.

- And don't leave your name on your voicemail greeting. You could get an adult to record your greeting. Their voice might stop the caller ringing again.

Almost all calls nowadays can be traced. If the problem continues, think about changing your phone number. If you receive calls that scare or trouble you, make a note of the times and dates and report them to the police. If your mobile can record calls, take the recording too.

Emails

- Never reply to unpleasant or unwanted emails — the sender wants a response, so don't give them that satisfaction.
- Keep the emails as evidence. And tell an adult about them.
- Ask an adult to contact the sender's Internet Service Provider (ISP) by writing abuse@ and then the host, e.g. **abuse@hotmail.com**
- Never reply to someone you don't know, even if there's an option to 'unsubscribe'.
- Replying simply confirms your email address as a real one.

Web bullying

If the bullying is on a website (e.g. Facebook) tell a teacher or parent, just as you would if the bullying was face-to-face – even if you don't actually know the bully's identity.

Serious bullying should be reported to the police - for example threats of a physical or sexual nature. Your parent or teacher will help you do this.

Chat rooms and instant messaging

- Never give out your name, address, phone number, school name or password online.
- It's a good idea to use a nickname. And don't give out photos of yourself.
- Don't accept emails or open files from people you don't know. Remember it might not just be people your own age in a chat room.
- Stick to public areas in chat rooms and get out if you feel uncomfortable.
- Tell your parents or carers if you feel uncomfortable or worried about anything that happens in a chat room.

- Think carefully about what you write; don't leave yourself open to bullying.
- Never give out passwords to your mobile or email account.

Three steps to stay out of harm's way

- Respect other people - online and off. Don't spread rumours about people or share their secrets, including their phone numbers and passwords.
- If someone insults you online or by phone, stay calm – and ignore them.
- Think how you would feel if you were bullied. You're responsible for your own behaviour – make sure you don't distress other people or cause them to be bullied by someone else.

Appendix 6 - Laptop Loan Form

Laptop Make and model: ....

Laptop Serial No: ....

Network ID: ....

May be used for appropriate private use as well as school use.

If laptop is removed from Marish Primary School, security of the laptop whilst off the premises is responsibility of undersigned that must have adequate insurance cover against loss or damage.

The Laptop remains property of Marish Primary School and must be returned to the school should the undersigned case to be a member of the school staff.

Received by:

Name :

....

Role: ....

Address: ....

....

Signature:

....

Date