SOAR SHARE STRIVE SPARKLE

The John Moore Primary School
&
Little Foxes Playgroup

E-Safety and Acceptable Use

(Including Social Networking Policy)

School Policy

Version:	1.6		
Review Cycle:	Annually		
Approval Level:	Governing Body, Individual Governor or Head Teacher		
Revision History:	Created April 2007 (1.0) Reviewed July 2011 (1.1) Reviewed January 2015 (1.2) Reviewed November 2019 (1.3) Reviewed and updated October 2020 (1.4) Reviewed September 2021 (1.5) Reviewed September 2022 (1.6)		
Approved By:	Individual Governor/Headteacher	Date:	September 2022

Table of Contents

1 Introduction 4
2 Effective E-safety Practice 4
3 School E-safety Policy 4
3.1 Writing and reviewing the E-safety Policy 4
4 Foundation Concepts 5
5 General Rules 5
6 Network Access / Basic Computer Security 5
7 Physical Behaviour & Care of Equipment 6
8 Software Usage 6
9 Teaching and Learning Using the Internet 7
9.1 Why Internet use is important 7
9.2 Internet use will enhance learning 7
9.3 Pupils will be taught how to evaluate Internet content 7
9.4 Managing Internet Access 7
10 E-mail 8
11 Published Content and the School Website 8
12 Child Protection 8
13 Social Networking and Personal Publishing 9
14 Managing Filtering 9
15 Staff Proxy 9
16 Managing Emerging Technologies 9
17 Protecting Personal Data 10
18 Anti-Virus Precautions 10
19 Policy Decisions 10
20 Assessing Risks 10
21 Handling E-safety Complaints 11
22 Handling E-safety Concerns 11
23 Communicating E-Safety Policy - Introducing to Pupils 11
24 Communicating E-Safety Policy - Introducing to Staff and Governors 11
25 Communicating E-Safety Policy - Introducing to Parents/Carers 11
26 Copyright 11
27 Good Practice 12
28 Use of ICT Resources Out of School/Playgroup 12
29 Disciplinary Action 12

30 Class Dojo (School) 13
31 Cyber Bullying 13
31.1 Understanding Cyber bullying 13
31.2 Procedures to Prevent Cyber bullying 13
32 Other linked policies 13
Appendix 1: Internet Use - Possible Teaching and Learning Activities 15
Appendix 2: E-safety Audit 16
Appendix 3: Rules for Responsible ICT Use/E-safety Rules 17
Appendix 4: Staff, Governor and Visitor, Acceptable Use Agreement 18
Social Networking Policy 20
33 Introduction 20
34 Key Principals 20
35 Social Networking – Code of Conduct 20
36 Class Dojo 22
37 Message from the Headteacher 23
Appendix 5: Acceptable Use of ICT Agreement 24
Appendix 6: Disciplinary Action 25
Appendix 7: Use of Digital / Video Images 27
Appendix 8: Key Stage 1 e-Safety Rules 28
Appendix 9: Key Stage 2 e-Safety Rules 29

1 Introduction

E-safety encompasses internet technologies and electronic communications 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
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs, Vlogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality e.g. iPads, e-readers

It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

2 Effective E-safety Practice

E-safety depends on effective practice at a number of levels:

- Responsible ICT use by all stakeholders involved at The John Moore Primary School and Little Foxes Playgroup, which includes staff, pupils, parents, carers, governors, volunteers; encouraged by education and made explicit through published policies.
- Sound implementation of E-safety Policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the South West Grid for Learning (SWGFL) including the effective management of SWGFL filtering.
- National Education Network standards and specifications.

3 School E-safety Policy

3.1 Writing and reviewing the E-safety Policy

The E-safety Policy relates to other policies including those for Anti-bullying, Data Protection (GDPR), Safeguarding (Child Protection) and all subject policies.

- The school will appoint a Computing and E-safety Subject Leader.
- The school will have a designated E-safety Governor.

- Our E-safety Policy has been written by the school, building on government guidance. It has been agreed by Staff, Senior Leaders and approved by Governors.
- The E-safety Policy and its implementation will be reviewed annually.

4 Foundation Concepts

Access to the ICT resources and computer networks owned by The John Moore Primary School and access to the internet and e-mail using these resources is conditional on observance of the following Rules for Responsible ICT Use and Acceptable Use Agreement (see Appendices)

Rules for Responsible ICT Use and Acceptable Use Agreement have been written by the School's Computing Subject Leader, building on government guidance. They have been agreed by the school and playgroup's staff, senior staff and approved by Governors and will be reviewed annually.

It is the policy of the school and playgroup that access to ICT resources, computer networks, the internet and e-mail is provided to staff and pupils as a privilege rather than a right. This privilege may be withdrawn at any time in line with these rules.

Rules for Responsible ICT Use and Acceptable Use Agreement apply at all times to all users, in and out of school hours, whilst using school equipment.

It is a general expectation that The John Moore Primary School and Little Foxes Playgroup's ICT resources are to be used in a reasonable, efficient, ethical, moral, and legal manner in accordance with the values, understandings and beliefs of the school/playgroup.

5 General Rules

Access to ICT resources will only be provided to staff, pupils and Governors who have read and agreed in writing to abide by the Rules for Responsible ICT Use and Acceptable Use Agreement. In the case of pupils, parent / carer permission will also be required.

Users of the school/playgroup's computer systems are allowed to use the facilities freely for school/playgroup work.

Individual users of school/playgroup ICT resources are responsible for their own behaviour and actions.

Use of school/playgroup ICT resources including e-mail is not considered to be private and should not be treated as such. The school's computing (e-safety) subject leader / senior staff may monitor computer usage at any time with or without the user's knowledge.

School/playgroup ICT resources are provided for academic use and may not be used for any form of personal business or financial gain.

6 Network Access / Basic Computer Security

Users must access the system using only usernames and class work areas that have been assigned to them. Users are personally responsible for the security of resources and passwords issued to them.

Users must not allow anyone else to access the system using a username, password or resource issued to them. Users are reminded that if this situation occurs, they may be charged with illegal actions carried out by the third party.

Users must not attempt to access the system using someone else's username or password or try to access class areas, resources or facilities which have not been made available to them. "Hacking" is illegal under the Computer Misuse Act.

Any user who becomes aware of a breach of network security, loophole or a breach of the Rules for Responsible ICT Use and Acceptable Use Agreement is required to inform a member of the Senior Leadership Team immediately.

With permission certain users of the school/playgroup community are allowed access to the school's Wi-Fi network. This will allow access to the internet on a personal device, for staff to use the internet for personal use. The school/playgroup's monitoring and filtering systems will still be applied in these circumstances.

Guests visiting our school/playgroup are allowed to access the guest Wi-Fi network with a password provided by the school/playgroup. The school/playgroup's monitoring and filtering systems will still be applied in these circumstances.

7 Physical Behaviour & Care of Equipment

Users must not cause any unnecessary noise or disturbance to others, or use facilities in a way that results in degradation or disruption of the service to others.

Users must not eat or drink when using or near ICT resources.

Users must treat with care and respect equipment and resources within the school/playgroup and at other sites accessed through school/playgroup facilities. Malicious action or vandalism will result in immediate suspension from school/playgroup facilities. Never deliberately damage or break anything.

8 Software Usage

Software provided on ICT resources has been carefully selected on the basis of educational value and suitability of content and is subject to strict licensing requirements. For this reason, users are forbidden to install any software for any reason unless prior consent has been given by the Senior Leadership Team.

No games of any kind with the exception of approved "edutainment" titles may be used on school/playgroup ICT resources.

Users accessing software or any services available through school/playgroup facilities must comply with licence agreements or contracts relating to their use and must not alter or remove copyright statements. Some items are licensed for educational or restricted use only.

ICT resources must not be used to hold or process personal data except in accordance with the provisions of the Data Protection Act 2018 (including GDPR). Any person wishing to use facilities for such a purpose are required to inform the Senior Leadership Team in advance and comply with any restrictions that the UK Data Protection Registrar may impose concerning the manner in which data may be held or processed.

9 Teaching and Learning Using the Internet

9.1 Why Internet use is important

The Internet is an essential element in our modern-day life for education, business and social interaction. The school/playgroup has a duty to provide students with quality Internet access as part of their learning experience.

Internet use is a part of the statutory school curriculum and a necessary tool for staff and pupils.

9.2 Internet use will enhance learning

The school/playgroup Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Users are not allowed access to public or unregulated chat rooms or to use instant messaging programs.

The school/playgroup considers all connections to remote locations on the Internet such as Virtual School Trips. Therefore, the rules that apply to conduct on regular school trips also apply to users visiting internet sites. It is important that users realise that they are acting as an ambassador for the school.

With the exception of copyright free pictures and text files, no internet content may be downloaded to or via school/playgroup ICT resources by non-staff users without permission from a member of staff. This includes, but is not limited to, music files, games, screen savers, desktop themes and other software.

As ICT resources are shared between users and linked to the school address, for their own protection, users are not allowed to use the resources to browse auction sites, make any form of personal online order or purchase or use internet banking services.

9.3 Pupils will be taught how to evaluate Internet content

The school/playgroup will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

9.4 Managing Internet Access

The school/playgroup's ICT system capacity and security will be reviewed regularly.

Virus protection will be updated regularly.

10 E-mail

All Users will be issued with an e-mail address for academic purposes.

Members of the school community will be issued with their own email account by approval of the SLT.

As all pupils in the school are at Key Stage 2 and below, pupils' e-mail access will be provided via a class mailbox used under teacher supervision. Personal e-mail accounts will not be provided to pupils.

All email accounts will be password protected and users will be responsible for checking their e-mails regularly and clearing their mailboxes regularly. Passwords and access to mailboxes are governed by the same rules as general network access.

Users may only use approved e-mail accounts on the school/playgroup equipment. Personal e-mail may be accessed on personal devices during your own time.

Excessive social e-mail use can interfere with learning and may be restricted. It is the user's responsibility to ensure e-mail is used sensibly and for academic purposes.

Users should remember that anything that is sent out from the school/playgroup network carries the school e-mail address and therefore represents the school. Users must not send in an e-mail any material that is inappropriate or use offensive or threatening language in e-mails or in any other communication on the Internet.

Pupils must immediately tell a teacher if they receive offensive e-mail.

Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

The forwarding of chain letters is not permitted.

11 Published Content and the School Website

The contact details on the Website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.

The Headteacher and Governors will take overall editorial responsibility and ensure that content is accurate and appropriate.

12 Child Protection

Photographs that include pupils will be selected carefully and pictures will not be used of individual pupils whose parents/carers have not given written permission.

Pupils' full names in association with their photograph will not be used anywhere on the school/playgroup's website or ClassDojo account. The use of full names without a photograph should be discouraged but can be used where permission has been granted.

Written permission from parents or carers will be obtained before photographs of pupils or pupils' work are published on the school/playgroup website or ClassDojo account and these records will be kept in the office.

13 Social Networking and Personal Publishing

The school/playgroup will block/filter access 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 / carers will be advised that the use of social network spaces outside school/playgroup is inappropriate for EYFS and primary aged pupils.

E-safety information evenings will be held on a regular basis in association with the police, when possible.

The school/playgroup's Social Networking Policy outlines the code of conduct for all those involved at The John Moore Primary School and Little Foxes Playgroup and is contained at the end of this policy.

14 Managing Filtering

The school will work with the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.

If staff or pupils discover an unsuitable site, it must be reported immediately to the class teacher and then to a member of the Senior Leadership Team in order for it to be logged with the SWGfL.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

15 Staff Proxy

The School/playgroup has enabled 'Staff Proxy'. This allows staff to use a special login that will provide some unfiltered access to the internet. The Internet Watch Foundation filtering will still apply.

Staff Proxy access will be strictly limited to specific devices and users which is agreed by the SLT.

Staff Proxy should be used with caution especially in the classroom. Staff should only use it for sites they are aware of and checked beforehand (eg Twitter, YouTube). Staff must NEVER leave IT equipment unattended when logged in to Staff Proxy and the browser session must be shut down when finished.

16 Managing Emerging Technologies

Emerging technologies will be examined for educational benefit and discussed with staff and Governors before use in school/playgroup is allowed.

Pupils are not allowed to use their mobile phones during school hours. If a pupil requires the use of a mobile phone before and after school, this must be left at the school office during school hours. Staff must restrict mobile phone use to outside teaching hours and when taking pupils off site.

17 Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

18 Anti-Virus Precautions

A computer virus is a malicious parasitic program written to alter the way that computers operate without permission or knowledge. They can destroy data, display inappropriate messages or destroy functionality. All school/playgroup ICT resources are equipped with anti-virus software but home users may not have this, or have an inadequate level of protection.

Viruses spread by copying themselves to other computers via discs as they are loaded on an infected system. For this reason, users are not allowed to transfer files to and from school/playgroup systems and their own equipment by any means. This includes the use of CDs, memory devices and personal e-mail attachments.

Viruses and malware are also spread by attachments on e-mails. Users receiving mail carrying attachments from unknown users or from a known user with an unusual subject line such as “I love you” or “click me” should delete the message without opening it. Care must also be taken opening e-mails from established companies as hackers are becoming more sophisticated in creating bogus e-mail accounts that appear to be coming from genuine companies. If in any doubt, please do not open the e-mail and seek advice from SLT.

Another source of malicious software is internet downloads and pop ups. While most such items will be blocked by the school/playgroup’s filtering system, users should be aware of the existence of these pop ups and avoid clicking on or activating them.

Any deliberate attempt by a user to introduce virus, malware or similar software will be treated in the same way and with the same severity as physical vandalism to school/playgroup equipment.

19 Policy Decisions

All staff must read and sign the E-safety Policy and Acceptable Use Agreement before using any school/playgroup ICT resource.

The school/playgroup will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil’s access be withdrawn.

Access to the Internet will be adult led with directly supervised access to specific, approved online materials.

20 Assessing Risks

The school/playgroup will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school/playgroup computer. Neither the school/playgroup nor LA can accept liability for the material accessed, or any consequences of Internet access.

The school/playgroup will audit ICT provision to establish if the E-safety Policy is adequate and that its implementation is effective.

21 Handling E-safety Complaints

Complaints of Internet misuse will be dealt with by a senior member of staff.

Any complaint about staff misuse must be referred to the Headteacher.

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures and immediately reported to the Designated Safeguarding Lead.

Pupils and parents / carers will be informed of the complaints procedure.

All complaints must be logged using CPOMS.

22 Handling E-safety Concerns

Pupils that have concerns about E-safety are made aware of the various people they can discuss these with (Parents/carers, staff and Governors).

All issues must be recorded using CPOMS.

23 Communicating E-Safety Policy - Introducing to Pupils

E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year and reminded of them throughout the year.

Pupils will be taught E-safety in specific lessons within PSHCE, SEAL and Computing focused sessions, following the school's scheme of work using educational websites for support such as thinkuknow, childnet and kidscape, etc.

Pupils will be informed that network and Internet use will be monitored.

24 Communicating E-Safety Policy - Introducing to Staff and Governors

All staff will be given the School E-safety Policy and its importance explained.

All staff and governors will have E-safety awareness training provided regularly.

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

25 Communicating E-Safety Policy - Introducing to Parents/Carers

Parents'/Carers' attention will be drawn to the School E-safety Policy in newsletters, the School Prospectus, hardcopies made available/sent out and on the school website.

Parents/Carers will be invited to attend E-safety awareness training regularly.

26 Copyright

Users must not take information from the Internet and pass it off as their own work (plagiarism).

Users must not publish information on the school/playgroup website or other websites that is protected by copyright.

No user may copy programs or data which are copyright or subject to restrictive licence agreements on to removable media or on to computers' hard discs. Users should assume that ALL software is subject to such a restriction.

27 Good Practice

Storage space on the network is limited and all users are requested to ensure that old, unwanted data is removed from their area. Users unsure of what can safely be deleted should ask a member of the Senior Leadership Team for advice.

ICT resources are backed up continuously. This means files can be restored if deleted or lost in error.

Users should save their work regularly (approximately every 15 minutes). The network is very reliable, but problems do occur (programmes crash, power can fail). If you save your work regularly and the network does fail for any reason, you will have only lost approximately 15 minutes work.

28 Use of ICT Resources Out of School/Playgroup

Certain users may be allocated ICT resources for use outside of school/playgroup. Equipment so issued is the responsibility of the user to which it is assigned and may be used by that user only. Use by family and friends is not permitted.

When used off school/playgroup premises, ICT resources and their users are still covered by all of the Rules for Responsible ICT Use and Acceptable Use Agreement including those relating to the installation of software, use of the internet and e-mail.

In exception to the paragraph above, a user allocated a school/playgroup laptop may set up a basic dial-up or broadband connection on the machine to allow internet access from home subject to the other Rules for Responsible ICT Use and Acceptable Use Agreement so long as this does not interfere with the system's operation on the school network. Machines so used will be provided with firewall and anti-malware software to help protect them when used outside of the school's filtered internet environment.

In exception to the above a user allocated a school/playgroup laptop may install printer driver software necessary to allow use of a home printer so long as this does not interfere with the system's operation on the school network.

All other ICT resources, such as staff and class iPads are also subject to the same Rules for Responsible ICT Use and Acceptable Use Agreement as set out above.

29 Disciplinary Action

Any infringement of Acceptable Use Agreement may lead to temporary or permanent suspension of use of ICT resources, internet access or both.

Any alleged infringement will be investigated by the Computing Subject Leader or Senior Leadership Team who can, within their discretion, waive or apply a penalty as the circumstances warrant.

Where the Computing Subject Leader takes the view that it is a particularly serious case, multiple offences have occurred or the possibility of a criminal offence exists, the matter will be referred to the Headteacher, Governing Body and possibly the Police. If it is agreed that it warrants such action, formal disciplinary proceedings will be instituted.

Please refer to Appendix 5 for a full list of sanctions to be applied following a breach of the Acceptable Use Agreement.

30 Class Dojo (School)

The provision of the Class Dojo further enhances the provision of ICT enabling children to share their learning journey both in school and at home.

The use of the Class Dojo is monitored by the class teacher and SLT.

31 Cyber Bullying

31.1 Understanding Cyber bullying

Cyber bullying is the use of ICT (usually a mobile phone/tablet device and/or the internet) to abuse another person.

It can take place anywhere and involve any number of people.

Anyone can be targeted including pupils, school staff, Governors etc.

It can include threats, intimidation, harassment, cyber-stalking, vilification, defamation, exclusion, peer rejection, impersonation, unauthorised publication of private information or images etc.

31.2 Procedures to Prevent Cyber bullying

Staff, pupils, parents/carers and Governors are made aware of issues surrounding cyber bullying.

Pupils and parents/carers will be urged to report all incidents of cyber bullying to the school. These will be recorded on CPOMS.

Staff CPD will assist in learning about current technologies through regular E-safety training.

Pupils will learn about cyber bullying through such things as PSHCE, assemblies, anti-bullying week activities and other curriculum projects alongside their E-safety lessons.

Staff, Governor and Visitors will sign an Acceptable Use of ICT Agreement/Code of Conduct (Appendix 3).

Parents/carers will be provided with information and advice on how to combat cyber bullying.

Parents/carers and pupils will be expected to sign an Acceptable Use of ICT agreement after discussing its meaning with their children (Appendix 4).

32 Other linked policies

- Child protection (Safeguarding) Policy
- Special Educational Needs and/or Disability Policy (including JMPS Local Offer)
- Behaviour in Schools Policy
- School Exclusion Policy
- Early Help Offer

Appendix 1: Internet Use - Possible Teaching and Learning Activities

Activities	Key E-safety Issues	Relevant Websites
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	Web directories Folders on Network
Using search engines to access information from a range of websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. - Swiggle - Google - CBBC Search
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should only use approved e-mail accounts. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. Outlook	Outlook E-mail a children's author E-mail Museums and Galleries
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted.	School's Website Class Dojo
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name.	School's Website Class Dojo
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.	
Audio and video conferencing to gather information and share pupils' work	Pupils should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password should be used.	

Appendix 2: E-safety Audit

This quick self-audit will help the Senior Leadership Team (SLT) assess whether the E-safety basics are in place to support a range of activities that might include those detailed within Appendix 1.

Has the school an E-safety Policy that complies with guidance?	Y/N
Date of latest update:	
The Policy was agreed by Governors on:	
The Policy is available for Staff at:	
The Policy is available for Parents/Carers at:	
The Designated Safeguarding Lead is:	
The E-safety Subject Leader is:	
The E-safety Governor is:	
Has E-safety training been provided for both students and staff?	Y/N
Do all staff sign an ICT Acceptable use Agreement/Code of Conduct?	Y/N
Do parents/carers sign and return an agreement that their child will comply with the School E-safety Rules?	Y/N
Have school E-safety Rules been set for pupils?	Y/N
Are these Rules displayed in all rooms with computers?	Y/N
Internet access is provided by an approved educational Internet Service Provider and complies with DfE requirements for safe and secure access.	Y/N
Have SLT, Governors and the E-safety lead completed a 'dummy' walkthrough of the E-safety reporting procedure to ensure processes are being followed correctly?	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act/GDPR?	Y/N

Appendix 3: Rules for Responsible ICT Use/E-safety Rules

E-safety Policy for Pupils

We know that using the internet is a really fun and exciting thing to do. To ensure that everyone is safe and happy these are the things I must remember when on the internet:

- If I have any concerns about any E-safety issues, I will speak to the Computing subject lead or a teacher.
- I will only use ICT in school for school purposes.
- I will consider the reliability of the information I read on the internet and will take care to check that it is accurate.
- I will not download anything that is protected by copyright.
- I will only use my class e-mail address when e-mailing.
- I will only open/ send e-mail attachments from/ to people I know, or who my teacher has approved.
- I will not take or distribute images of anyone without their permission.
- I understand that my mobile phone should not be brought to school unless my parent has requested this, in this instance my mobile phone will be left in the school office.
- 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 tell a teacher immediately.
- I will not give out my own or others' details such as name, phone number, school details 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 E-safety.
- Let's have fun whilst being safe!

Appendix 4: Staff, Governor and Visitor, Acceptable Use Agreement

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/playgroup. This policy is designed to ensure that all staff, Governors and visitors are aware of their professional responsibilities when using any form of ICT. All staff, Governors and Visitors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Computing Subject Leader.

- 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 Headteacher or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school/playgroup or other related authorities. If I need to disclose my password for maintenance work to be carried out I will change my password immediately once all work has been completed.
- 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/playgroup business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school/playgroup, taken off the setting premises or accessed remotely.
- Personal data can only be taken out of school/playgroup or accessed remotely when authorised by the Headteacher or Governing Body.
- I will not use or install any hardware (including USB sticks) or software without permission from the Computing Subject Leader or Senior Leadership Team.
- 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/playgroup 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 Headteacher. I will not hold any of the above images on my own device, they will be kept on the shared areas of the school's network.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request by the Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school/playgroup and outside setting, will not bring my professional role into disrepute.
- I will support and promote the school/playgroup'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/carers have given permission for them to use the Internet and ICT are enabled to do so at school/playgroup.
- I will report any damage or faults involving equipment or software to the SLT or Computing Lead.
- I will use 'Staff Proxy' with care. I will only use it for sites I am aware of and have checked before using with children. I will never leave the computer unattended and close the browser when the session is finished.
- I understand that if I fail to comply with this acceptable use policy agreement I could be subject to disciplinary action, this could include a warning, suspension, referral to governors and or the local authority and in the event of legal activities the involvement the police.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature …… Date ……

Full Name ……..... (printed)

Job title: ……..

Social Networking Policy

33 Introduction

This policy is written to establish the key principles and code of conduct for everyone to adhere to in order to protect the children and families of the school/playgroup. It should be read alongside the school/playgroup's E-Safety policy.

To outline, social networking activities conducted online outside of the school/playgroup environment, can include blogging, (the writing of personal journals to publicly accessible web pages), involvement in social networking sites (such as Facebook, Twitter, Instagram, etc) posting material such as photos, videos, messages and opinions. The unintended consequences of using social media to voice frustrations and annoyances can be wide ranging, and affect children other than your own, and their families, and can have potential unforeseen legal consequences.

34 Key Principals

Everyone at The John Moore Primary School and Little Foxes Playgroup has a responsibility to ensure that they protect the reputation of the school/playgroup, and to treat colleagues, friends and members of staff with the professionalism and privacy that they deserve.

It is important to protect everyone at The John Moore Primary School and Little Foxes Playgroup from any allegations and misinterpretation / misrepresentations which can arise from inappropriate use of social networking sites.

Safeguarding children is a key responsibility of all members of staff and it is essential that everyone considers this and acts responsibly if they are using social networking sites out of school/playgroup. Anyone working at or attending the school/playgroup either as a paid employee, volunteer or visitor must not communicate with children via social networking.

It is advised that all staff working at The John Moore Primary School and Little Foxes Playgroup consider who their 'online friends' are. It is advised to consider your personal settings, content of your social networking page and accessibility. You may be potentially leaving yourself open to allegations of inappropriate contact or conduct or even find yourself exposed to unwanted contact.

No photos, videos or other images should be posted to any public or restricted availability website without full permission and knowledge of the parents or guardians of all children involved.

This limitation extends to publishing any names of children or families without permissions as outlined above.

35 Social Networking – Code of Conduct

The John Moore Primary School and Little Foxes Playgroup recognises that the use of Social Networking sites is an important part of our everyday lives. Many parents / carers will want to share proud moments and images of their children on social media especially to other family members and friends.

The John Moore Primary School and Little Foxes Playgroup has a duty to protect the school/playgroup and members of the school/playgroup Community. The school/playgroup must therefore balance the rights and wishes of people to use Social media with a need to protect members of the school/playgroup Community, especially our children.

The school/playgroup will therefore put in place advice for the use of Social Media and strict guidelines especially over areas where it has control (such as images taken on school/playgroup premises or on school/playgroup trips or sporting activities referred to here as 'School/Playgroup Activities').

The following are guidelines for the Use of Social Media in relation to The John Moore Primary School/Little Foxes Playgroup:

- Use of the School/Playgroup's Logo for Commercial or Charitable promotion
    - The use of the school/playgroup's name, logo or any other published material is not allowed without written prior permission from the Headteacher. This applies to any published material including the internet or written documentation.
- Images of your own Children not taken at School/Playgroup or during School/Playgroup Activities
    - The school recognises that parents / carers may wish to post digital images of their children whilst in school/playgroup uniform (such as the first day at school). However, it is recommended that you do not post any images of your children where it would be possible to identify them and the school/playgroup they go to. If images are posted care should be taken with privacy settings so that your child could not be identified by name.
    - All images posted must not be taken on School/Playgroup premises or during School/Playgroup activity and must be of your own child. Images of any other children must not be used unless you have permission from that child's parents / carers.
- Images taken at School/Playgroup or during School/Playgroup Activities
    - The School/Playgroup obtains permission from parents / carers to be able to use images of children or their work, taken on School/Playgroup premises or during School/Playgroup activities. These can be used at School/Playgroup, on the school/playgroup Website or Class Dojo.
    - Images are only used where permission is granted, and any group images are only used when we have permission to use the images of all of the children present. The School/Playgroup must therefore control what images are used when taken on School/Playgroup premises or during School/Playgroup activities.
    - Any images of employees, children, governors or anyone directly connected with the school/playgroup whilst engaged in school/playgroup activities are not allowed to be posted on Social media websites.
    - The School/Playgroup allows parents and carers to take images of their children whilst on School/Playgroup Premises (such as Christmas Plays and

Sporting events). However, these images must not be posted on any social media or public websites.

- If parents / carers abuse this and post images taken on School/Playgroup premises or during School/Playgroup Activities, the School/Playgroup may restrict images being taken in the future.

- The use of Social media to post comments about The John Moore Primary School and Little Foxes Playgroup:
  - The School/Playgroupl recognises the rights of parents / carers to have free speech. However, it must balance this against the need to protect the School, Playgroup, its Staff, Governors, Children or anyone connected to the School/Playgroup, against derogatory, defamatory, rude, threatening or inappropriate comments.
  - Parents / carers are therefore advised not to post any comments, either positive or negative about the School/Playgroup, Staff, Governors or anyone connected with the School/Playgroup.
  - The School/Playgroup has a number of mechanisms available for parents / carers to raise comments or issues with the School/Playgroup directly. This includes an open-door policy or a more formal complaints procedure.
- Monitoring of Social media and internet for comments about The John Moore Primary School and Little Foxes Playgroup:
  - The John Moore Primary School and Little Foxes Playgroup uses tools to monitor Social Media and the internet. If content is found, members of the School/Playgroup Community may be asked into School/Playgroup to discuss any comments further.
- Other Areas – In addition to the above everyone must ensure they:
  - Do not disclose confidential, personal or otherwise sensitive information; or the disclosure of information or images / name identification that could compromise the security of the school/playgroup or its children.
  - Use social networking sites responsibly and ensure that no personal or professional reputation is compromised by inappropriate postings.
  - Are aware of the potential of online identity fraud and to be cautious when giving out personal information about themselves which may compromise their personal safety and security.

36 Class Dojo

The John Moore Primary School uses Class Dojo to share the children's learning journey. The class areas are a 'closed' group and can only be accessed via an invitation. The 'School Story' can be seen by all invited parents / carers but is still classified as a 'closed' group because no other person may see this information.

The School will share key information and show some of the activities and events. Staff will also upload pictures, videos or text to provide information about what their classes have been doing.

The main principles for the use of the Class Dojo are:

- Access to Class Dojo is strictly controlled and will only be granted to members of the School Community.
- Children's full names will never be used
- All photos and images used will only contain images of pupils where prior agreement has been granted by parents and carers (through the Digital images permission form. See Appendix 6 of the E-Safety and Acceptable use policy)

37 Message from the Headteacher

Message from the Headteacher

Dear Parents, Carers, Governors, Pupils and Staff,

In the context of this policy, please note that the term 'everyone' refers to members of staff, governors, parents/carers, pupils and anyone involved with the school/playgroup either in a paid or voluntary capacity.

While we appreciate that social networking is part of many people's daily lives, this policy helps to ensure the safety of all those involved with The John Moore Primary School and Little Foxes Playgroup. Our school/playgroup is a place where we aim to create an environment that is happy, caring and stimulating and this needs to be maintained within the virtual world we live in.

We aim to work in partnership with you for the benefit of your child at the school/playgroup. Therefore, we ask, like the staff at our school, that you as parents/carers set a good example to your child. Please consider what information is present on any social networking page(s) and think about the level of protection you have. Even in your proudest moment as a parent/carer of a child at The John Moore Primary School and Little Foxes Playgroup we ask that you do not name your child's school/playgroup, class etc as this can leave the gateway open to other people commenting on your child's school/playgroup. We educate the children not to reveal such details and make comments good or bad and therefore we are asking you as responsible parents to continue this message at home.

Yours sincerely

Mrs Ruth Laing
Headteacher

Appendix 5: Acceptable Use of ICT Agreement

The John Moore Primary School

Parent/Carer and Pupil E-safety and Acceptable use Agreement

Dear Parents/Carers,

Acceptable Use of ICT Agreement

Information and Communication Technology (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 Computing equipment.

Please read and discuss with your child the Rules for Responsible ICT Use/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/Acceptable Use Policy which is available in full on request at the office or can be viewed on our school website.

Yours sincerely,

Mrs Ruth Laing, Headteacher

Pupil Name:

I have read, understood and agreed with the Rules for Responsible ICT Use/E-safety Rules (Appendix 2 to E-safety /Acceptable Use Policy).

Signed …….

Class……

Parent's/Carer's Consent for Internet Access:

I have read and understood the school rules for E-safety/Acceptable Use Policy 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.

Print Name: ……

Signed…… (Parent/Carer) Date……..

Appendix 6: Disciplinary Action

Pupils **Actions / Sanctions**

Incidents:	Refer to class teacher	Refer to SLT	Refer to Headteacher	Refer to Police	Refer to Computing Subject Leader or E-safety Governor	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal.	X	X	X	X		X			X
Unauthorised use of non-educational sites during lessons	X	X	X			X	X	**X**	**X**
Unauthorised use of mobile phone / digital camera / other mobile device	X	X	X			X		**X**	**X**
Unauthorised use of social media / messaging apps / personal email	X	X	X			X	X	**X**	**X**
Unauthorised downloading or uploading of files	X	X	X			X	X	**X**	**X**
Allowing others to access school / academy network by sharing username and passwords	X	X	X					X	
Attempting to access or accessing the school / academy network, using another student's / pupil's account	X	X	X					X	
Attempting to access or accessing the school / academy network, using the account of a member of staff	X	X	X			X	X	X	
Corrupting or destroying the data of other users	X	X	X			**X**	**X**	X	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	**X**		X	**X**	X	**X**
Continued infringements of the above, following previous warnings or sanctions	X	X	X	**X**		X	X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X			X	**X**	X	
Using proxy sites or other means to subvert the school's / academy's filtering system	X	X	X			X	X	X	
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X			X		X	
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	**X**		X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X			X		X	

X – Depending on severity and or frequency

Staff and Governors **Actions / Sanctions**

Incidents:	Refer to SLT	Refer to Headteacher and or Governing Body	Refer to Local Authority / HR	Refer to Police	Refer to Computing Subject Leader or E-safety Governor	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal.	X	X	X	X				X
Inappropriate personal use of the internet / social media / personal email	X	X				X		
Unauthorised downloading or uploading of files	X	X	**X**	**X**		X	**X**	**X**
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	X	X				X		
Careless use of personal data eg holding or transferring data in an insecure manner	X	X				X		
Deliberate actions to breach data protection or network security rules	X	X				X	**X**	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X				**X**	**X**	**X**
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	**X**	**X**		X	**X**	**X**
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X	**X**	**X**		X	**X**	**X**
Actions which could compromise the staff member's professional standing	X	X				X		
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy	X	X	**X**			X	**X**	**X**
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	**X**			X		
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	**X**		X	X	X
Breaching copyright or licensing regulations	X	X				X		
Continued infringements of the above, following previous warnings or sanctions	X	X	X				X	X

X – Depending on severity and or frequency

Appendix 7: Use of Digital / Video Images

The John Moore Primary School and Little Foxes Playgroup
Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras/iPads to record evidence of activities in lessons and out of school/playgroup. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school/playgroup website, Class Dojo (school) and occasionally in the public media. The school/playgroup will not publish your child's full name alongside their picture.

The school/playgroup will comply with the Data Protection Act/GDPR and request parents' / carers' permission before taking images of members of the school/playgroup. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

Parents/carers are requested to sign the permission form to allow the school/playgroup to take and use images of their children.

Parent / Carers Name:_____

Pupil Name:_____

As the parent / carer of the above pupil, I / We agree/disagree to the following statements. Please answer **Yes or No** in each box.	
I / We agree to the school/playgroup taking and using digital / video images of my child. I / We understand that the images will only be used to support learning activities in school/playgroup that reasonably celebrates success and promotes the work of the school/playgroup.	
I / We do / do not give permission for these images to be electronically published (for example on the school/playgroup website) I / We understand that the images will only be used to support learning activities in school/playgroup or in publicity that reasonably celebrates success and promotes the work of the school/playgroup. **Note: If you sign NO to this, your child may be asked to leave photo opportunities in order for photos to be used of other children.**	
I / We agree that if I take digital or video images at or, of The John Moore Primary School/Little Foxes Playgroup, pupil's work and images of pupils including your own child. I / We will not publish comments, digital images or videos on social networking sites as outlined in the school/playgroup's E-safety and Social Networking Policy.	

Please ensure that both Parents / Carers sign this form on behalf of your family.
(If you require an additional form due to family circumstances please ask).

Signed: Date:

Signed: Date:

Appendix 8: Key Stage 1 e-Safety Rules

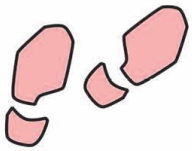
These rules help us to stay
safe on the Internet

Think then Click

We only use the Internet when an adult is with us.

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.



We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly emails to people that we know.

Appendix 9: Key Stage 2 e-Safety Rules

Think then Click

We ask permission before using the internet. When we are searching for websites, we only use criteria agreed by our teacher.

We tell an adult if we see anything we are uncomfortable with.

We can click on buttons or links when we know what they do.

We only email people an adult has approved.

We send e-mails that are polite and friendly.

We do not open e-mails sent by anyone we don't know.

We never give out our own or other people's personal information or passwords (eg names and addresses)

We never arrange to meet anyone we don't know.

We do not use Internet chat rooms.