The Froebelian School

Online Safety Policy

Introduction and Definitions

The provisions in this document apply to all aspects of the school including the EYFS, Breakfast Club, Little Acorns, Homework and Activities Club, Summer Holiday Club, school trips and extra-curricular activities.

The policy should be read in conjunction with the following policies and documents:

- Anti-Bullying
- Personal, Social, Health and Economic Education (PSHEE)
- Safeguarding and Child Protection
- Electronic Communications for Staff (including Acceptable Use Policy – see Appendix 1)
- Pupil Internet Agreement (see Appendix 2)
- Staff iPad Agreement
- Data Protection
- Photo Permissions Guidance

Computing in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- the internet;
- e-mail;
- instant messaging (WhatsApp) often using simple web cams;
- Blogs/Twitter/Snapchat etc. (and other on-line interactive diary/discussion forums etc.);
- podcasting (radio/audio broadcasts downloaded to computer or MP3/4 player);
- social networking sites (Popular www.facebook.com / www.twitter.com/ www.piczo.com // http://www.hi5.com, https://www.instagram.com);
- video broadcasting sites (Popular: http://www.youtube.com/);
- chat Rooms (Popular www.teenchat.com, www.habbohotel.co.uk);
- gaming Sites (Popular www.neopets.com, http://www.miniclip.com/games/en/, http://www.runescape.com/);
- music download sites (Popular http://www.apple.com/itunes/ and http://www.apple.com/uk/ios/facetime/ http://www.napster.co.uk/ http://www-kazzaa.com/, http://www-livewire.com/ https://www.spotify.com)
- mobile phones with camera and video functionality;
- smart phones with e-mail, web functionality and cut down 'office' applications; and
- tablet computers with http://www.apple.com/uk/ios/facetime/ and all the above functions and more.

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers schools to protect and educate the whole school community in their use of technology and establish mechanisms to identify, intervene in and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

• content: being exposed to illegal, inappropriate or harmful material;

• contact: being subjected to harmful online interaction with other users; and

• conduct: personal online behaviour that increases the likelihood of, or causes, harm.

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

This policy establishes the ground rules that the school has for using the internet, electronic communications such as mobile phones, iPads, collaboration tools and personal publishing. 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 experiences. It also describes how these ideas fit into the wider context of child protection, exploitation, discipline and PSHEE policies and demonstrates the methods used to protect children from sites containing pornography, racist or politically extreme views and violence.

Employees should also make themselves aware of the school approach to computing contained in the Electronic Communications Policy.

Roles and Responsibilities

Safety is recognised as an essential aspect of strategic leadership in the school and the Headteacher, with the support of Governors, aims to embed safe practices into the culture of the school. The Headteacher ensures that the policy is implemented, and compliance with the policy monitored. The responsibility for Online Safety has been designated to the ICT/Computing Leader.

It is every teacher's responsibility to be aware of cyber bullying and its results. The following short video should be viewed by employees and this will be shown in PSHEE lessons to FIII and FIV pupils.

http://www.digizen.org/resources/cyberbullying/films/uk/lfit-film.aspx

Employees should not leave their computer/iPad logged in when it is unsupervised.

The school's **Online Safety Lead** is Mr Mike Finan.

The school's **Designated Safeguarding Lead** is Mrs Sharon Stratford.

The Online Safety Lead ensures that the school keeps up-to-date with Online Safety issues and guidance through organisations such as Becta and The Child Exploitation and Online Protection (CEOP).

The policy is available for employees on *Flying*, and for parents on the school website.

Whole School Online Safety

Online Safety depends on effective practice at a number of levels:

- Responsible computing use by all employees and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of the Online Safety Policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband, including the effective management of filtering.

The overriding rule is that no pupil should have *any* unsupervised access to the computers and tablets within school.

Technical Provision and Infrastructure

The school has a part-time Network Manager who oversees the school's technical provision and infrastructure. The Network Manager works closely with the Online Safety Lead to ensure safeguards are in place to filter and monitor inappropriate content and alert the school to safeguarding issues. The school also outsources some of its network management to a private company who provides high-level, specialist technical support and maintains the security and stability of the school's ICT infrastructure and network.

Whilst it is essential that school ensures that appropriate filters and monitoring systems are in place, we are careful that "over-blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

IT System

- *The school system is run from a server located in the IT Suite, providing hard wired access for school laptops and PCs. We also have 11 Wi-Fi routers, located around school, providing approximately 99% Wi-Fi coverage in the school buildings which is available for use by the school's mobile devices. A hub in the LKG/Science building runs a back-up service for school data.*
- *The school's Wi-Fi has 3 entry routes for staff, pupils and guests encrypted password (IT staff). Staff and pupil access is password protected. The Wi-Fi is protected by WPA (Wi-Fi Protected Access).*

Hardware

- *Each classroom/learning area has a Windows 7 or Window 10 laptop or PC with classrooms also having 2 or 3 PCs for use by staff and children.*
- *Each Form Room, Music Room and Art Room has a Smartboard and projector installed, with the Hall and ICT Room having projectors projecting onto a white surface.*
- *All teaching staff currently have an iPad and there are currently 100+ iPads for use by all children.*
- *An up to date inventory of all IT equipment is kept by the Network Manager and a copy is forwarded to the Finance & Operations Manager at least twice a year*.

Safety Features

- *The school subscribes to GFI Unified Protection which provides us with email and antivirus protection.*
- *Microsoft Security Essentials is installed and running on all PCs and laptops.*
- *The server runs open DNS web filtering which prevents access to unsuitable websites.*
- *All staff have a personal password to enable them to log onto school systems.*
- *PCs and laptops are set to lock after periods of inactivity, requiring passwords to log back in.*
- *Bad password entries in school and on the Remote Desktop application now result in a lockout time period.*
- *USB memory devices brought into school for use by children or visitors are checked for malware prior to use by the IT Staff.*
- *Staff wishing to transfer data to and from home must now use a school issued encrypted USB memory device.*
- *Google Parental Control is activated on school iPads.*
- *Children are not left unsupervised when using school IT equipment.*
- *Digital Literacy e.g. Online Safety, is embedded in the school ICT curriculum.*

Teaching and Learning

The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for employees and pupils. In addition to computers, sets of iPads are available to be used around the school.

Internet Use that will Enhance Learning

- The school internet access will be designed expressly for pupil use and will include filtering. **No site should be visited by pupils unless the teacher in charge has first visited the site and checked out links**. Obviously extreme sites are filtered, as are gaming sites, but occasionally as with all systems things can creep through. There are, however, several sites used by the school that are child-friendly and developed specifically for schools and these sites are acceptable for pupils to investigate and produce independent research without any worries about Online Safety.

- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use. This is laid out in the Pupil Internet Agreement.

- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation of information. Indeed, the school should constantly emphasise critical thinking. Critical thinking indicates that the school should not spoon feed children and should encourage them to research and find information for themselves whilst always being critical of what they are learning. This is particularly so in this digital age where anyone can post information on the internet without checking that what they have submitted is correct.

- Teachers will ensure that the use of internet-derived information, for research and projects, complies with copyright law. Pupils should be made aware that the internet is not a free for all and that much of its content is covered by copyright law.

- Pupils should be taught to be critically aware of any internet-derived material that they read and shown how to evaluate and validate the content before accepting its accuracy.

- The school's PSHEE scheme of work also covers cyber bullying and its consequences.

Managing Internet Access

- The school computing system's capacity and security will be reviewed regularly.

- Employees', pupils' and visitors' use of the internet is monitored. Any unacceptable use is sent to the Network Manager and discussed with the Headteacher who will decide on the action to be taken.

- Virus protection and restricted sites are updated regularly.

- Therefore, when using search engines to access information from a range of websites pupils must always be supervised and the search carried out by the teacher prior to the lesson to avoid any unsuitable names and sites appearing.

- When using iPads, controlled access to the internet is vital. It is inevitable that this policy will require further updates as portable devices become more integrated within lessons.

E-mail

- Pupils may only use approved e-mail accounts on the school system.

- Pupils must immediately tell a teacher if they receive offensive e-mail. This will then be sent to the Online Safety Lead, who will discuss its content with the Headteacher. The Headteacher will decide on any further action.

- Pupils must be told not to reveal personal details of themselves or others in any e-mail communication, or arrange to meet anyone.

- Pupil e-mails sent to an external organisation should be written carefully and authorised by a member of staff before sending, in the same way as a letter written on school headed paper.

- The forwarding of chain letters is not permitted.

In reality, much of the above should not be an issue as the teacher is required to monitor e-mails and they should only be sent after they have been read. The school's policy is that these emails should be composed in Microsoft Word and, having first been approved by the teacher, they are then pasted into an e-mail.

Published Content and the School Website

- The contact details on the website should be the school address, e-mail and telephone number. Employee names are published on the open website but staff photographs and email addresses are only published on the secure parent area of the website.

- All parents are required to sign a form indicating whether or not their child's photograph may or may not be published in school magazines, on social media and on the website etc.

- The school generally avoids the use of pupil names and photographs together on the website except when impossible to do so (an individual sports winner, for example). All parents are asked to opt out should they not want an image of their child to appear on the website.

Employee Mobile Phone Use

Employee mobile phones should only be used in class if there is an emergency and should generally be switched to silent. Should a vital phone call be anticipated then this should be discussed with the Headteacher or Deputy Head prior to the phone being turned on in class.

Pupils should, at no time, be given employees' personal mobile phone numbers. It is left to the discretion of the employee whether, in certain circumstances, personal phone numbers are given to parents.

The taking of pictures of pupils by personal mobile phones should be avoided. However, if something does require recording, a sporting victory for example where no camera was available, then this should be emailed at the first opportunity and immediately deleted from the phone.

Social Networking and Personal Publishing

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Managing Filtering

If employees or pupils discover an unsuitable site, it must be reported to the ICT/Computing Leader /form teacher, Headteacher or Deputy Head as soon as possible (they will then contact the Network Manager and arrange for the site to be blocked).

Managing Video-conferencing

IP video-conferencing should only be used when pupils are with a teacher and permission of the Headteacher has been sought.

Video-conferencing will be appropriately supervised for the pupils' age.

Mobile Phone Use and Managing Emerging Technologies

Children at The Froebelian School are not permitted to bring a mobile phone or portable device to school. However, we recognise that we have a duty to educate children on their safe use outside of school.

- New and emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

- The sending of abusive or inappropriate text messages, photographs or any other information meant to hurt, tease or cause distress of any sort is forbidden. Pupils should remember that ALL electronic data is recoverable and anything once done cannot be undone. So a text, picture or email, once sent, can easily be traced, even once it has been deleted. Form teachers must then inform the Headteacher or Deputy Head, who will decide on any action that needs to be taken.

- Using a mobile phone or email to tease, bully or otherwise upset pupils outside school, may be punishable within school.

- Pupils must note that there is no difference between name calling etc. by mobile phone, text or email and verbally teasing someone and it will be treated the same way.

Protecting Personal Data

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

Handling Online Safety Complaints

- Complaints of internet misuse will be dealt with by a member of the Senior Leadership Team. Pupils can, in accordance with the Anti-Bullying, Pastoral Care and other policies, approach any member of staff with a concern.

- Any complaint about employees' misuse must be referred to the Headteacher.

- Complaints of a child protection nature must be dealt with in accordance with school's Safeguarding and Child Protection Policy and procedures.

The school will take all reasonable precautions to ensure Online 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. The school cannot accept liability for material accessed, or any consequences of internet access.

Employees and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- interview/counselling by Online Safety Lead /Headteacher;
- informing parents or carers;
- removal of internet or computer access for a period, and
- referral to the Designated Safeguarding Lead and in extreme situations the police.

Introducing the Online Safety Policy to Pupils

- Online Safety rules will be discussed with the pupils regularly throughout the year when iPads are being used.

- Pupils will be informed that network and internet use will be monitored.

- Lessons on Online Safety will form part of the ICT/Computing curriculum. Details of this can be seen in the schemes of work for each year group.

- Each year, FIII and FIV will watch a video on Online Safety and cyber bullying. Discussions about the topic will take place. http://www.digizen.org/resources/cyberbullying/films/uk/lfit-film.aspx

Employees and the Online Safety Policy

- All employees will be given this Online Safety Policy and its importance explained.

- Employees should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

- Training for staff is provided as part of our on-going safeguarding training updates. The Online Safety Lead is also available to deal with staff concerns and queries regarding the safe use of ICT/Computing and mobile technologies in school.

- Clear guidance for staff is available in the Electronic Communications Policy.

Photographic and Video Images

It is often necessary, from an educational point of view, to record photographic and video images of pupils, or to allow pupils to record images of each other to assist teaching and learning, or to celebrate achievement. There is potential for images of children to be misused for pornographic or grooming purposes and therefore employees should adhere to the following code:

- Only record images when there is a justifiable need.
- Ensure that pupils understand the reason for the recording of the images and how the images will be used and stored.
- Ensure that a member of the Senior Leadership Team is aware of the recordings.
- Ensure that all images recorded are available for scrutiny.
- Avoid making recordings in one-to-one situations.
- On admission to the school, parents give consent that images and recordings of their children can be used for legitimate reasons.
- Where the school has decided that images should be retained for future use, they should be stored and used only by those authorised to do so, in line with GDPR.

Employee Internet Use

- Employees must follow the school policy on the use of ICT equipment and the internet. Accessing child pornography, or making, storing or disseminating such materials is illegal and, if proven, will be treated as gross misconduct and may lead to dismissal. Employees must not use school ICT equipment to access adult pornography on or off site.

Enlisting Parents' Support

- Parents' attention will be drawn to the school Online Safety Policy in newsletters and on the school website. A document giving advice to parents about safe internet use at home will be sent to parents.

- Pupils and parents are informed of the Exploitation and Online Protection Centre: www.thinkyouknow.co.uk.

Weblinks

Suggested suitable weblinks for children are provided on the school website. A further project is to develop a pupil area of the school website which will contain learning resources and weblinks across a range of curriculum topic areas.

Information and Support

There is a wealth of information available to support schools and colleges to keep children safe online. The following is not exhaustive but should provide a useful starting point:

www.thinkuknow.co.uk

www.disrespectnobody.co.uk

www.saferinternet.org.uk

www.internetmatters.org

www.childnet.com/cyberbullying-guidance

www.pshe-association.org.uk

www.educateagainsthate.com

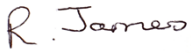
www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

This policy is reviewed regularly by the Headteacher, in consultation with the Designated Safeguarding Lead, Online Safety Lead and governing body, in the light of experience, research and good practice.

Policy Date: January 2019

Policy Review Date: January 2022

Signed (Headteacher): 

Signed (Chair of Governors): 

Appendix 1

Acceptable Use Agreement for School Staff

I confirm that I have read and understood the **Electronic Communications (Staff) Policy** and that I will use all means of electronic communication equipment provided to me by the school and any personal devices which I use for school activity in accordance with the document. In particular:

- Any content I post online (including outside school time) or send from a school email address will be professional and responsible and maintain the reputation of the school;
- To protect my own privacy I will use a school email address and school telephone numbers (including school mobile phone) as contact details for children and their parents whenever possible;
- If I use instant messaging, chat rooms, webcams or forums for communicating with children or parents it will only be via the school's accredited system or VLE;
- I will only use my personal mobile phone during non-teaching time; it will be kept on silent mode during lessons except in an emergency situation with the agreement of my line manager;
- I will not use my personal mobile phone or other electronic equipment to photograph or video children without seeking prior consent from the Headteacher;
- I will take all reasonable steps to ensure the safety and security of school ICT equipment which I take off site and will remove anything of a personal nature before it is returned to school;
- I will take all reasonable steps to ensure that all laptops and memory devices are fully virus protected and that protection is kept up to date;
- I will report any accidental access to material which might be considered unacceptable immediately to my line manager and ensure it is recorded.

I confirm I have read the school's **Data Protection Policy** and will implement the guidelines indicated. In particular:

- Confidential school information, child information or data which I use will only be stored on a device which is encrypted or protected with a strong password. Computers will have a password protected screensaver and will be fully logged off or the screen locked before being left unattended;
- I understand that I have the same obligation to protect school data when working on a computer outside school;

- I will report immediately any accidental loss of confidential information so that appropriate action can be taken.

I understand that the school may monitor or check my use of school based ICT equipment and electronic communications.

I understand that by not following these rules I may be subject to the School's disciplinary procedures.

Name ……..

Signed ……

Date …….

Appendix 2

The Froebelian School
Pupil Internet Agreement

This is to be read through with your parent(s) and then signed by both you and your parents. You will be allowed access to the internet after this is returned to school.

- At the Froebelian School we expect all pupils to be responsible users of the internet. This includes materials they choose to access, and language they use.
- Pupils must ask permission to access the internet and a member of staff should be present throughout the session.
- Pupils using the internet must not deliberately seek out offensive or extremist material. Should this happen accidentally then you must inform the member of staff present.
- Access to social networking sites e.g. Facebook, Twitter, Instagram or any internet chat room is not allowed.
- Pupils are not allowed to download program files, music or video files from the internet.
- Pupils must seek approval from the ICT Leader or another teacher before using 'memory sticks' or any other portable file sharing device.
- When using email pupils will only contact recipients approved by the school and must not give out personal information such as telephone numbers or addresses. Pupils will follow the rules for email etiquette that their teacher will outline, such as appropriate language and topics of conversation. Whole class rather than individual email accounts will be allocated and emails will only be sent as a part of a structured lesson.
- Accessing web based email e.g. 'hotmail' accounts is not allowed.
- Internet use will be monitored.
- Any pupil who persistently fails to comply with the Froebelian Pupil Internet Agreement may be denied access to the resources and additional sanctions may be applied.

<u>The Froebelian School Pupil Internet Agreement</u>

I have read through the agreement with my child and agree to these safety restrictions.
I give my permission for my child to use the school's Internet resources under staff supervision.
I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate material.

Signed:…… parent/carer

Name of child:…….. Form:…….

Signed (pupil):……

Date:……