***FROEBEL HOUSE SCHOOL***
***E-SAFETY POLICY***

## 1. Introduction

Froebel House School recognises that ICT and the Internet are fantastic tools for learning and communication that can be used in school to enhance the curriculum, challenge pupils, and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone within the school community, but it is important that the use of the Internet and ICT is seen as a responsibility and that pupils, staff and parents use it appropriately and practise good e-safety. It is important that all members of the school community are aware of the dangers of using the Internet and how they should conduct themselves online.

## 2. Aim

The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the pupil or liability to the school.

## 3. Managing Internet Access

### Authorising Internet Access

- All staff must read and sign the "ICT Acceptable Use Agreement for Staff" before using any School ICT resources.
- All pupils must read and sign the "ICT Acceptable Use Agreement for Pupils" before using any school ICT resource.
- The School will maintain a current record of all staff and pupils who are granted access.
- Parents will be asked to sign and return a consent form.

### Information System Security

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- School network system security will be reviewed regularly.
- Virus protection will be updated regularly.
- Servers, wireless systems and cabling must be securely located and physical access restricted. All users will have clearly defined access rights to school technical systems and devices
- Internet access is filtered for all users. Illegal content is filtered by the filtering provider. Content lists are regularly updated, and internet use is logged and regularly monitored.
- School staff regularly monitor and record the activity of users on the School network and users are made aware of this in the Acceptable Use Agreements

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly.
- The School infrastructure and individual workstations are protected by up to date virus software.

At Froebel House School we understand there may be the possibility that pupils may encounter inappropriate material on the Internet, however, we will actively take all reasonable precautions to restrict pupils' access to both undesirable and illegal material.
All staff are responsible for guiding pupils in their on-line activities, by providing clear objectives for internet use. Teaching staff will also ensure that pupils are aware of what is regarded as acceptable and responsible use of the Internet.

## 4. Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation (GDPR) 2018 or any UK legislation which replaces it.
Froebel House School ensures that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against accidental loss of, or damage to, personal data. This is in relation to data belonging to all members of the school community. As such, no member of staff is permitted to remove sensitive personal data from school premises, whether in paper or electronic form and wherever stored, without prior consent of the Headteacher. Where a member of staff is permitted to download data off site it will need to be password protected.

## 5. Safe Use

**Internet** – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this e-safety and the staff Acceptable Use Policy; pupils upon signing and returning their acceptance of the Acceptable Use Policy.

**Email** – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.

**Photos and videos** – Working with children and young people may involve the taking or recording of images. Any such work should take place with due regard to the law and the need to safeguard the privacy, dignity, safety and well-being of children and young people. Informed written consent from parents, should always be sought before an image is taken for any purpose.

**Notice and take down policy** – should it come to the school's attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

**Incidents** - Any e-safety incident is to be brought to the immediate attention of the Headteacher. The Headteacher will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

**Online sexual harassment**

Sexual harassment is likely to: violate a child's dignity, make them feel intimated, degraded or humiliated and/or create a hostile, offensive or sexualised environment. Online sexual harassment, which might include: non-consensual sharing of sexual images and videos and sharing sexual images and videos (both often referred to as 'sexting'; inappropriate sexual comments on social media; exploitation; coercion and threats.

Any reports of online sexual harassment will be taken seriously, and the police and Children's Social Care may be notified.

Froebel House School follows and adheres to the national guidance - UKCCIS: Sexting in schools and colleges: Responding to incidents and safeguarding young people, 2016.

**Searching devices**

The Education Act 2011 allows staff to lawfully search electronic devices, without consent or parental permission, if there is a suspicion that the pupil has a device prohibited by school rules, or the staff member has good reason to suspect the device may be used to:

- cause harm,
- disrupt teaching,
- break school rules,
- commit an offence,
- cause personal injury, or
- damage property.

Where the person conducting the search finds an electronic device they may examine any data or files on the device if they think there is a good reason to do so. Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

The member of staff must have regard to the following guidance issued by the Secretary of State when determining what is a "good reason" for examining or erasing the contents of an electronic device: In determining a 'good reason' to examine or erase the data or files the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.

If inappropriate material is found on the device it is up to the Headteacher to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police.

**Sexting** - All school staff should be aware that behaviours linked to sexting put a child in danger.

**Curriculum** - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Froebel House School will have an annual programme of training which is suitable to the audience.

This will be mostly based around the CEOP ThinkuKnow (http://www.thinkuknow.co.uk) resources.

E-Safety for pupils is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the pupil's learning. As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

**Staff Training** - It is the responsibility of the Headteacher to ensure that E-Safety training for staff is regularly planned, up to date and appropriate.

**Prevent duty**
Froebel House School is fully committed to safeguarding and promoting the welfare of all its pupils. Every member of staff recognises that safeguarding against radicalisation and extremism is no different to safeguarding against any other vulnerability in today's society.

- We protect children from the risk of radicalisation, for example by using filters on the internet to make sure they can't access extremist and terrorist material, or by vetting visitors who come into school to work with pupils.
- Our Safeguarding, Prevent Duty and eSafety policies set out our beliefs, strategies and procedures to protect vulnerable individuals from being radicalised or exposed to extremist views, by identifying who they are and promptly providing them with support.

Staff should ensure that they establish safe and responsible online behaviours, working to local and national guidelines and acceptable use policies which detail how new and emerging technologies may be used. Communication with children both in the 'real' world and through web based and telecommunication interactions should take place within explicit professional boundaries. This includes the use of computers, tablets, phones, texts, e-mails, instant messages, social media such as Facebook and Twitter, chat-rooms, forums, blogs, websites, gaming sites, digital cameras, videos, web-cams and other hand-held devices. (Given the ever-changing world of technology it should be noted that this list gives examples only and is not exhaustive.)

## 6. Handling E-Safety Complaints

- Complaints of internet misuse will be dealt with by the Headteacher
- Any complaint about staff misuse must be referred immediately to the Headteacher, which may require advice being sought from the Local Authority Designated Officer, as per the school's Child Protection & Safeguarding policy.
- Complaints of a child protection nature must be dealt with in accordance with Safeguarding Policy.
- Pupils and parents will be informed of the Complaints Policy and procedures.
- Pupils and parents will be informed of consequences and sanctions for pupils misusing the internet and this will be in line with the School's Behaviour or Anti-Bullying Policy.

## 7. Awareness raising

Pupils

A unit is included in our personal, social, health and citizenship education medium-term planning and also in our ICT curriculum. At the beginning of the school year, all classes will discuss the safe use of the ICT room during their first lesson when they will be reminded about the acceptable use policy.

Parents

Parents are encouraged to take notice of their children's online activities to discuss the risks with them.

**Teach your child the internet safety code, Click Clever, Click Safe.**

- **Zip It** – Keep your personal stuff private and think about what you say and do online
- **Block It** – Block people who send you nasty messages and don't open unknown links and attachments.
- **Flag It** – Flag up with someone you trust if anything upsets you or if someone asks to meet you online.

School Staff

Staff have a duty to ensure that the pupils in their care stay safe, and also that they themselves are alert to the dangers of internet use.

**Internal Policies**
This policy should be read in conjunction with the following policies:-

- Acceptable User
- Anti-Bullying
- Attendance
- Behaviour
- Child Protection
- Data Protection
- ICT
- Mobile phone
- PSHE
- Staff Code of Conduct
- Whistle Blowing

**National Guidance**
The following national guidance should also be referred to:

- DfE: Keeping Children Safe in Education. Statutory Guidance for schools and colleges – October 2019
- DfE: Searching, screening and confiscation. Advice for Headteachers, school staff and governing bodies, January 2018
- UKCCIS: Sexting in schools and colleges: Responding to incidents and safeguarding young people, August 2016

**Produced by**: Mr A Roberts, Headteacher

***Date issued**: January 2020*
***Date review**: January 2021 (or sooner, if local or national guidance changes)*

## Acceptable Use Policy – Pupils

## Our Charter of Good Online Behaviour

**Note: All Internet and email activity is subject to monitoring**

**I Promise** – to only use the school ICT for schoolwork that the teacher has asked me to do.

**I Promise** – not to look for or show other people things that may be upsetting.

**I Promise** – to show respect for the work that other people have done.

**I will not** – use other people's work or pictures without permission to do so.

**I will not** – damage the ICT equipment, if I accidentally damage something I will tell my teacher.

**I will not** – share my password with anybody. If I forget my password I will let my teacher know.

**I will not** – use other people's usernames or passwords.

**I will not** – share personal information online with anyone.

**I will not** – download anything from the Internet unless my teacher has asked me to.

**I will** – let my teacher know if anybody asks me for personal information.

**I will** – let my teacher know if anybody says or does anything to me that is hurtful or upsets me.

**I will** – be respectful to everybody online ; I will treat everybody the way that I want to be treated.

**I understand –** that some people on the Internet are not who they say they are, and some people can be nasty. I will tell my teacher if I am ever concerned in school, or my parents if I am at home.

**I understand** – if I break the rules in this charter there will be consequences of my actions and my parents will be told.

**Signed (Parent) :**

**Signed (Pupil) :**

**Date :**

# Acceptable Use Policy – Staff

**Note: All Internet and email activity is subject to monitoring**

You must read this policy in conjunction with the e-Safety Policy. Once you have read and understood both you must sign this policy sheet *(it may be easier and tidier to have a separate single sheet that all staff sign).*

**Internet access** - You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an e-safety incident, reported to the e-safety officer and an incident sheet completed.

**Social networking** – is allowed in school in accordance with the e-safety policy only. Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should not become "friends" with parents or pupils on personal social networks

**Use of Email** – staff are not permitted to use school email addresses for personal business. All email should be kept professional. Staff members are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

**Passwords** - Staff should keep passwords private. There is no occasion when a password needs to be shared with another member of staff or pupil, or IT support.

**Data Protection** – If it is necessary for you to take work home, or off site, you should ensure that your device (laptop, USB pendrive etc.) is encrypted. On no occasion should data concerning personal information be taken offsite on an unencrypted device.

**Personal Use of School ICT** - You are not permitted to use ICT equipment for personal use unless specific permission has been given from the Headteacher who will set the boundaries of personal use.

**Images and Videos** - You should not upload onto any internet site or service images or videos of yourself, other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings).

**Use of Personal ICT** - use of personal ICT equipment is at the discretion of the Headteacher. Permission must be sought stating the reason for using personal equipment; a risk assessment will be carried out.

**Viruses and other malware** - any virus outbreaks are to be reported to the Mouchel Helpdesk as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

**e-Safety** – like health and safety, e-safety is the responsibility of everyone to everyone. As such you will promote positive e-safety messages in all use of ICT whether you are with other members of staff or with pupils.

**NAME :**

**SIGNATURE :** **DATE :**

# E-Safety Incident Log

| | | |
|---|---|---|
| **Number**: | **Reported By:** *(name of staff member)* | **Reported To:** *(e.g. Head)* |
| | **When:** | **When:** |
| **Incident Description:** (Describe what happened, involving which children and/or staff, and what action was taken) | | |
| **Review Date:** | | |
| **Result of Review:** | | |

| | | | |
|---|---|---|---|
| **Signature (Headteacher)** | | **Date:** | |