Leavening Community Primary School

E-Safety & Social Media Policy (including Acceptable Use Agreements)

Adopted by: Full Governing Body
September 2023

Review date: September 2024

General Information

For clarity, the e-safety policy uses the following terms unless otherwise stated:

Users - refers to staff, governing body, school volunteers, pupils and any other person working in or on behalf of the school, including contractors.

Parents – any adult with a legal responsibility for the child outside the school e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits, school trips etc.

Wider school community – pupils, all staff, governing body, parents & volunteers

All staff & volunteers will sign as read and understood both the e-safety policy and the Staff Acceptable Use Agreement. A copy of this policy will be available on the school website and the Pupils Acceptable Use Agreement will be sent home with pupils annually for pupils and parents to sign.

Roles & Responsibilities

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy annually and in response to any e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- Receive regular updates from the headteacher in regards to training, identified risks and any incidents.

Headteacher

Reporting to the governing body, the headteacher has overall responsibility for e-safety within our school.

The headteacher will:

- ensure that e-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. pupils, all staff, governing body, parents & volunteers.
- ensure that all e-safety incidents are dealt with promptly and appropriately.
- engage with parents and the school community on e-safety matters at school and/or at home.
- liaise with the local authority, IT technical support and other agencies as required.
- retain responsibility for the e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- ensure any technical e-safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.
- be aware of any reporting function with technical e-safety measures, i.e. internet filtering reporting function,

ICT Technical Support Staff

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
    - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
    - Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
    - Any e-safety technical solutions such as Internet filtering are operating correctly.
    - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the e-safety officer and headteacher.
    - Passwords are applied correctly to all users regardless of age. Passwords for staff will be a minimum of 8 characters.
    - The Schools ICT Technician will sign the schools Acceptable Use Agreement annually.

All Staff

Staff will ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher.
- Any e-safety incident is reported to the Headteacher (and an e-Safety Incident report is made). If you are unsure, the matter is to be raised with the Headteacher to make a decision.
- The reporting flowcharts contained within this e-safety policy are fully understood.
- The responsibility of online safety lies with all staff and as such all staff have received suitable training.
- Online safety is a key part of the computing and PHSE curriculum. In addition, it is compulsory that , as part of our homework policy, all children complete an online safety learning opportunity each half term.

All Pupils

The boundaries of use of ICT equipment and services in this school are given in the Pupil Acceptable Use Agreement; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the Behaviour Policy.

E-Safety is embedded into our curriculum; pupils will be given the appropriate advice and guidance by staff. Similarly, all pupils will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Through parents evenings, school newsletters and training as appropriate the school will keep parents up to date with new and emerging e-safety risks, and will involve parents in strategies to ensure that pupils use IT safely.

Parents must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded. As such, parents will sign the Pupil Acceptable Use Agreement before any access can be granted to school ICT equipment or services.

The Governing Body

The Governing Body will:

- review & agree this policy annually
- establish the effectiveness (or not) of e-safety training and awareness in the school.
- recommend further initiatives for e-safety training and awareness at the school.

<u>Technology</u>

Leavening CP School uses a range of devices including PC's, laptops and ipads. In order to safeguard the pupil and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – we use virus protection software that prevents unauthorised access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The Headteacher and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher.

Email Filtering – we use software that prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

Encryption – All school devices that hold personal data (as defined by the Data Protection Act 1998) are encrypted. No personal pupil data that is not linked to teaching and learning, is to leave the school on an un-encrypted device. Any breach (i.e. loss/theft of device such as laptop or USB keydrives) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office.

Passwords – *A*ll staff and pupils will be unable to access any device without a unique username and password. The ICT Coordinator and IT Support will be responsible for ensuring that passwords are changed when essential.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated automatically for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns. All USB peripherals such as keydrives are to be scanned for viruses before use.

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 Agreement and pupils upon signing and returning their acceptance of the Acceptable Use Policy. Parents should also sign this agreement

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.
Pupils are not permitted to use the school email system.

Photos and videos – Digital media such as photos and videos are covered in the schools' Child Protection Policy. Staff must use a school ipad in school, during class trips and during residential trips to take photographs of children and also add photos to the Facebook page using a school ipad. All parents must sign a photo/video release slip when their child starts school; non-return of the permission slip will not be assumed as acceptance.

Social Networking – Leavening CP School recognises the use of social networking as a tool to engage with parents and the wider school community. The following social media services are permitted for use within Leavening CP School and have been appropriately risk assessed; should staff wish to use other social media; permission must first be sought via the

Headteacher for a decision to be made. Any new service will be risk assessed before use is permitted.

- Facebook – used by staff to share school information and photos with the wider school community.
- Class Do-Jo for communicating with parents and use of a blog.

In addition, the following is to be strictly adhered to:

- Permission slips must be consulted before any image or video of any child is uploaded.
- There is to be no identification of pupils using first name and surname; first name only is to be used.
- Where services are "comment enabled", comments are to be set to "moderated".
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a license which allows for such use (i.e. creative commons).

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 who will assist you in taking the appropriate action to deal with the incident and filling out an incident log and saving it on Staff Share on the computer.

Training and 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, Leavening CP School will provide training as necessary which is suitable to the audience.

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. Parent E-safety sessions are to be provided every 2 years, to remind parents of the latest guidelines regarding social media and parental controls.

Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headteacher for further CPD.

Acceptable Use Agreement – Staff and Governors

Note: All Internet and email activity is subject to monitoring

You must read this agreement in conjunction with the e-Safety Policy. Once you have read and understood both you must sign this sheet

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 by staff 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 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 password protected. 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.

Viruses and other malware - any virus outbreaks are to be reported to the NYCC IT 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 :**

Acceptable Use Agreement – 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 there will be consequences of my actions and my parents will be told.

Signed (Parent) :

Signed (Pupil) :

Date :

e-Safety Incident Log

Number:	**Reported By:** *(name of staff member)*	**Reported To:** *(e.g. Head, e-Safety Officer)*
	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:**
Signature (Governor)		**Date:**