FRIETH C.E.C SCHOOL

Let your light shine!

Online Safety Policy

Including Acceptable Use Agreements

This policy should be read in conjunction with:

- ICT Policy
- Anti-Bullying Policy
- Safeguarding and Child-protection Policy
- Mobile Phone Policy
- Keeping Children Safe in Education (KCSIE) 2022

At Frieth CEC School we operate within a culture of vigilant safeguarding. This includes our responsibility to keep pupils safe online. We recognise that many forms of abuse can occur online as well as offline and understand the role that technology can play in these. This policy and acceptable use agreements are part of an infrastructure of whole-school awareness, designated responsibilities, robust policies and procedures. This policy has been written with the support of the following documents:

- Safeguarding children in a digital world
- Developing a strategic approach to e-safety
- Superhighway Safety - safe use of the internet
- E-safety - Developing whole-school policies to support effective practice

Roles and Responsibilities

The Designated Safeguarding Lead

- The DSL has overall responsibility for online safety (See KCSIE Annex B) and this cannot be delegated. The DSL is supported by SLT and the ICT Leader in matters of online safety and is the first point of contact for any internet safety issue which may compromise the well-being of a child.
- The DSL will ensure they access appropriate training and/or support to ensure they understand the unique risks associated with online, including the additional risks learners with SEND face online.
- The DSL will ensure they have the relevant knowledge and up to date capability required to keep our children safe online and develop appropriate strategies and policies for dealing with these.

The ICT Lead

The ICT lead will:

- support the DSL, providing up to date relevant information and advice, including from KCSIE Annex C, to support them in their role:
- promote internet safety across the curriculum and throughout the school;
- liaise with Technology Service Providers (Softegg) to ensure the safety of pupils.

The Headteacher

- The Headteacher will ensure that appropriate funding is allocated to support online safety activities and practice throughout the school, including for the technical infrastructure and staff training.

The Governing Body

- The Governing Body will keep themselves up to date on developments and support the IT coordinator, including with statutory guidance within 'Keeping Children Safe in Education' Annex C 2022

All Staff

All staff are expected to:

- familiarise themselves with 'KCSIE 2022 Annex C: Online Safety' and will participate in online safety training at induction and as part of regular child protection training and updates;
- evaluate websites and other online resources in advance of classroom use;
- implement the school curriculum for Online Safety and other activities as directed, such as from the CEOP 'Think you know' website, embedding the teaching of online safety within all curriculum areas as appropriate;
- maintain an appropriate level of professional conduct in their own internet use both within and outside school.

Parents

We ask our parents to:

- ensure that their child understands and adheres to their Acceptable Use Agreement;
- ensure home internet access is carefully monitored. We encourage parents to consider investing in internet security software to keep their children safe online.

Pupils

The Acceptable Use Agreements for each Key Stage are reviewed annually and sent home as part of the home-school agreement process. We expect pupils to:

- adhere to their agreement at all times. (See Appendix A);
- report any incidents of ICT misuse to a member of the teaching staff;
- seek help or advice from a trusted adult if they experience problems when online, or if they receive any content or contact which makes them feel uncomfortable in any way;
- communicate with parents or carers about internet safety issues, and upholding any rules for safe internet use in the home.

Internet access

Our policy in school is to use the county or contractor provided fire-walled broadband internet access only. This is strictly filtered via the provider to provide a safe and secure environment in school. We do not permit the use of any other internet access in school, including other broadband or wireless access.

In the event of a suspected criminal offence being committed related to internet access, whether by a pupil or a member of staff, the police will be consulted at the earliest opportunity.

Pupils are only allowed to use the internet when supervised by an adult, using only sites that have been previously reviewed by a member of the teaching staff. Familiarising ourselves with new apps on iPads before they deployed to children's devises will safeguard children from inappropriate content and adverting. We regard supervision as having an adult in close proximity, regularly checking what is being accessed. Pupils are allowed to search using normal search engines such as Google.

The download of copyrighted materials and the use of web sites that require entering of any personal details, are expressly forbidden for pupil use, unless parental consent has been obtained previously.

Pupils are taught that in the event of exposure to inappropriate materials, they turn the computer monitor off as swiftly as possible and alert the teacher. The DSL will then be notified, along with the pupils' parents. UPDATA, the hosting company, will be notified. A review of how the material was accessed will then be conducted, followed by feedback to all concerned and a review of this policy and our procedures. In the event of deliberate access to inappropriate material by pupils, punishment appropriate to the offence will be sanctioned by the headteacher. In the event of deliberate access by a member of staff, disciplinary proceedings will ensue. Annual pupil workshops, staff training and parent information sessions are delivered by a trained CEOP Ambassador to ensure that the whole school community is educated on up-to-date safe use of computers and connected devices.

Monitoring of internet access and email use of school is partly carried out by the county system in accordance with current legislation such as:

- General Data Protection Regulations 2016 https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

· The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
http://www.hmso.gov.uk/si/si2000/20002699.htm

· Regulation of Investigatory Powers Act 2000
http://www.hmso.gov.uk/acts/acts2000/20000023.htm

· Human Rights Act 1998
http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Restrictions

- Staff and pupils are only permitted to use the school provided email system while in school. This system is strictly filtered by the provider.
- Only educational context video conferencing is permitted in school.
- Pupils are not permitted to use mobile phones in school.
- Staff may not use mobile phones during lesson times or with children present. Mobile phones should be secured in a cupboard or locker during lesson time, with the ring tone set to 'silent'. If a member of staff is anticipating an important call during lesson time, the mobile phone needs to be left with the school office.
- Under no circumstance should staff use mobile phones or personal devices for taking pictures of pupils; school equipment should be used.
- Parents will be advised of restrictions around photography before any performance. This will include guidance to only take photographs/film of their own child and not to publish pictures of other people's children or school events online, including on social media.

ICT Provision

All of the laptops in school have access to the internet. As such, it is important that we adhere to the following points:

- Pupils are not permitted to use any PC in school unsupervised.
- Staff and pupils are not permitted to leave a PC that is logged on to an email or learning platform session unattended, in the interests of maintaining security.
- Staff using school laptops outside of the school environment must adhere to this policy.
- All PCs used in school have 'Sophos' county provided Virus killing software installed. In the event of unusual computer activity, staff are to report the incident as soon as possible to the Internet Safety Coordinator.
- Pupils are not permitted to install software on PCs.
- Any USB keys or CD ROMs must be virus checked before use.

Digital Images

- No images of pupils are to be uploaded to the school web site unless permission has been granted by parents. Names will not be associated with images.
- Only pupils with permission, indicated on the parent/pupil consent form, can have their picture digitally captured.
- Pupil images can only be stored on school equipment.

The School Website

Our school web site is designed for use by the whole school community. Our policy is to agree to the following:

- Only members of staff or governors are to be given password protected access to modify or add materials;
- Only members of staff or governors are to be given password protected access to view restricted areas;
- Members of staff are allowed to upload pupils' work only if the pupil has given permission, no pupil details are revealed;
- Passwords are to be changed periodically to ensure continued security;

- The Internet safety team regularly checks the school website to ensure there is no copyright infringement.

ICT at Home and Supporting Parents

It is our school policy to recommend the following to parents with regard to the use of the Internet at home:

- Pupils should not be allowed to use the internet unsupervised;
- Children are able to access class groups on Microsoft Teams. These groups are managed by class teachers and solely used to distribute homework and for uploading completed tasks.
- We strongly recommend the use of parental control software;
- We strongly recommend that parents do not allow their children to use 'messenger' resources such as MSN unless supervised closely, and that the age restrictions of such resources are adhered to;
- We strongly recommend that parents do not allow children to upload pictures of themselves or personal details to any websites;
- Any incidents of bullying via email or SMS text messaging should be reported to a member of the teaching staff as soon as possible;
- We encourage the use of ICT to support schoolwork;
- We do not encourage pupils to plagiarise text or images for use in homework.

Computer Misuse Act and ICT Use in school

Pupils are not permitted to delete files, change the desktop set-up or introducing viruses with the intent to impair the operation of a computer, or access to programs and data.

Should I use my mobile phone to take photographs or video of students?

A school trip is a common situation where photography by pupils and staff should be encouraged, but there are potential dangers. The safest approach is to avoid the use of personal equipment and to use a school-provided item. One potential danger is an allegation that an adult has taken an inappropriate photograph. With a personal camera it would be more difficult for the adult to prove that this was not the case.

Should I continue to use my Social\ Networking site?

Social networking is a way of life for most young people and many adults. However adults working with children and young people should review their use of social networks as they take on professional responsibilities. Strong passwords should be used and security settings should be applied so that you control all access to your profile. Information once published, e.g. photographs, blog posts etc. is impossible to control and may be manipulated without your consent, used in different contexts or further distributed. Some adults have been caught out by posting amusing remarks about their school or colleagues, only to find them re-published elsewhere by "friends". Even innocent remarks such as an interest in "Gang Wars" could be misinterpreted (this is actually a game). False social networking sites have been set up by pupils and staff with malicious information about staff. Here are several school policy points on what is recommended:

- We recommend that you do not allow parents, pupils, and former pupils as 'friends'
- We recommend that you set up any profiles to be 'private'.
- We recommend that you only post information or pictures on a social networking site that you would be happy sharing with the whole school community

What is my responsibility for the use of my school laptop at home?

- Access to wider sites by family members, for instance a gaming site or internet shopping, would increase the possibility of virus attack and identity theft.
- If another member of the family or a friend is allowed to use the computer it is difficult to ensure that the use has been appropriate, for instance that confidential information has not been accessed. Adults vary enormously in their judgements as to what is appropriate.
- Some adults may feel that access via a school laptop to adult material outside school hours and at home is appropriate. It is not; there is always a possibility that this material might be accidentally seen by a child/young person and in some cases this type of use has led to dismissal.

Adults need to remember that in order for anyone else to use a school laptop in the home setting, they would need to be logged on by the person responsible for the laptop. With this in mind, think about who would be culpable in such situations!

What is inappropriate material?

Inappropriate is a term that can mean different things to different people. It is important to differentiate between 'inappropriate and illegal' and 'inappropriate but legal'. All staff should be aware that in the former case investigation may lead to criminal investigation, prosecution, dismissal and barring. In the latter it can still lead to disciplinary action, dismissal and barring even if there is no criminal prosecution. Illegal Possessing or distributing indecent images of a person under 18 – viewing such images on-line may well constitute possession even if not saved. What is regarded as indecent would ultimately be down to a jury to decide. The police have a grading system for different types of indecent image. Remember that children may be harmed or coerced into posing for such images and are therefore victims of child sexual abuse. Hate/Harm/Harassment General: There is a range of offences to do with inciting hatred on the basis of race, religion, sexual orientation etc. Individual: There are particular offences to do with harassing or threatening individuals – this includes cyberbullying by mobile phone, social networking sites etc. It is an offence to send indecent, offensive or threatening messages with the purpose of causing the recipient distress or anxiety. Think about this in respect of professionalism and being a role model. The scope here is enormous, but bear in mind that "actions outside of the workplace that could be so serious as to fundamentally breach the trust and confidence placed in the employee" (SPS 2004) may constitute gross misconduct.

Examples taken from real events:

- Posting offensive or insulting comments about the school on Facebook;
- Accessing adult pornography on school computers during break;
- Making derogatory comments about pupils or colleagues on social networking sites;
- Contacting pupils by email or social networking without senior approval;
- Trading in sexual aids, fetish equipment or adult pornography**.**

How do I ensure safer online activity in the primary classroom?
Most internet use in schools is safe, purposeful and beneficial to pupils and staff. However, there is always an element of risk; even an innocent search can occasionally turn up links to adult content or imagery.
Planning and preparation is vital and the safest approach when using online material in the classroom is to test sites on the school system before use. For younger pupils you should direct them to a specific website or a selection of preapproved websites and avoid using search engines. When working with older pupils, select an appropriate and safe search engine e.g. CBBC Safe Search. Appropriate search terms should be used and pre-checked. Consider carefully the age, ability and maturity of all pupils when planning online activities.

When encouraging pupils to publish work online, schools should consider using sites such as "Making the News", Microsites (hosted by SEGfL), video hosting sites such as SchoolsTube and TeacherTube and virtual learning environments. For image searching use sites such as the Microsoft Clip Art Gallery and the National Education Network Gallery. If inappropriate material is discovered then turn off the monitor, reassure the pupils and to protect yourself you need to log and report the URL to a member of the senior leadership team. Avoid printing or capturing any material.

Date implemented: Spring 2015

Last updated: February 2023

Frieth Primary School
Acceptable Use Agreement / Online Safety Rules
KS1 Pupils

Think before you click

✓ I will only use school technology for school purposes to help me learn.

✓ I will only go on to websites that my teacher has chosen for me to use.

✓ I will not tell other people my passwords.

✓ I will only open/delete my own files or documents.

✓ I will make sure that all contact with other children and adults is responsible, polite and sensible.

✓ If I see anything that makes me uncomfortable, I will turn the screen off and tell an adult immediately.

✓ I will not give out my own details such as my name, address or phone number.

✓ When using MS Teams and other technology, I will be responsible for my behaviour and actions.

✓ I will not record or take photographs or screenshots of my classmates or teachers during a face-to-face session on MS Teams.

✓ I will not share any school content (resources, videos etc.) on social media platforms.

✓ I understand that when using MS Teams and other applications provided by the school, my use can be monitored and logged and can be made available to my teachers.

✓ I will not make contact with a member of staff through video chat.

✓ I will only contact my teacher through the 'chat' if I have a question related to my learning.

✓ I will only contact other children through 'chat' if I have a question about my learning.

✓ I will follow these rules because they are to keep me safe.

Pupil

As a user of the school network and learning platform, I agree to comply with these rules on its use.

Pupil name ______________________ Date: ___/___/2023

Parent

I have discussed these rules with my child. As a responsible parent, I support school policies on digital technology and the Internet. I will monitor my child's use of the Internet. I will also act as a positive role model and will use social media responsibly and in line with the school's values in respect of all matters relating to the school.

Parent Signature _______________________ Date ___/___/2023

Frieth Primary School
Acceptable Use Agreement / Online Safety Rules
KS2 Pupils

Think before you click

- ✓ I will only use school technology for school purposes to help me learn.
- ✓ I will only access websites that a responsible adult has chosen for me to use.
- ✓ I will only open emails and attachments from people I know.
- ✓ I will not tell other people my passwords.
- ✓ I will only open/delete my own files or documents.
- ✓ I will make sure that all contact with other children and adults is polite and sensible and reflective of our school values.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or offensive. If I accidentally find or am sent something like this I will turn the screen off and tell an adult immediately.
- ✓ I will not give out my own details such as my name, address or phone number.
- ✓ I will not arrange to meet someone that I have met online unless my parent/carer has given their permission and a responsible adult comes with me.
- ✓ I will never share pictures or personal information with people I don't know
- ✓ I will not record or take photographs or screenshots of my classmates or teachers during a face-to-face session on MS Teams.
- ✓ I will not share any school content (resources, videos etc.) on social media platforms.
- ✓ I understand that when using MS Teams and other applications provided by the school, my use can be monitored and logged and can be made available to my teachers.
- ✓ I will not make contact with a member of staff through video chat.
- ✓ I will only contact my teacher through the 'chat' if I have a learning related question.
- ✓ I will only contact other children through 'chat' if I have a question about my learning.
- ✓ I will be responsible for my behaviour and actions when using TEAMS and other technology because I know these rules are to keep me safe.

Pupil

As a user of the school network and learning platform, I agree to comply with these rules on its use.

Pupil name _______________________ Date: ___/___/2023

Parent

I have discussed these rules with my child. As a responsible parent, I support school policies on digital technology and the Internet. I will monitor my child's use of the Internet. I will also act as a positive role model and will use social media responsibly and in line with the school's values in respect of all matters relating to the school.

Parent Signature ________________________ Date ___/___/2023