"Developing potential without limitations"

Frieth C.E.C. School
E-Safety and IT Acceptable Use Policy

Date implemented : Spring 2015
Member of staff responsible: Computing and IT Coordinator
Governing body committee responsible: Curriculum Committee

Headteacher's signature Mrs J Reid

Chair of Governor's signature Mrs M Tebbot

Review date: May 2018	signed: J Reid	date: 18/05/18
Review date:	signed:	date:
Review date:	signed:	date:
Review date:	signed:	date:

E-Safety and Acceptable Use Policy

This policy is organised into the following areas:

- Roles and responsibilities
- Internet Access
- Electronic communication
- ICT provision
- Digital images
- The school website
- ICT at home and Supporting parents
- Computer Misuse Act and ICT use in schools
- Guidelines for staff
- Pupil and parent acceptable use and consent form
- Staff consent form

This policy has been writing 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

Our acceptable use policy is based around an infrastructure of whole-school awareness, designated responsibilities, policies and procedures.

Aims:

- Create a culture of internet safety within the school;
- Ensure pupil safety.

Related policies:

- ICT policy
- Anti-Bullying policy
- Child-protection policy
- Mobile Phone Policy

Roles and Responsibilities

The IT coordinator

It is the responsibility of the IT coordinator and E-Safety Coordinator to liaise with the Senior Leadership Team in order to:

- Give appropriate time, support and authority to carry out the duties of the team effectively;
- Ensure that appropriate funding is allocated to support internet safety activities throughout the school; for both the technical infrastructure and Inset training;
- Promote internet safety across the curriculum.

Governors

It is the responsibility of the governing body to keep up to date on developments and support the IT and E-Safety coordinators.

Teaching Staff

It is the responsibility of the class teacher and teachers to:

- evaluate websites in advance of classroom use;
- implement the school curriculum for Internet Safety, as directed by the internet safety team. Our Internet Safety curriculum is based around the CEOP 'Think you know' website;
- embed teaching of internet safety within curriculum areas as appropriate;
- maintain an appropriate level of professional conduct in their own internet use both within and outside school.

Child Protection Designated Officers

It is the responsibility of the child protection Designated officer to:

- act as the first point of contact for any internet safety issue which may compromise the well-being of a child or young person (for example, trauma resulting from internet use such as exposure to inappropriate materials or grooming);
- ensure that they are fully aware of the issues which they might encounter, and to develop appropriate strategies and policies for dealing with these.

Pupils Should be reviewed at the start of every year as part of the home school agreement process

It is the responsibility of pupils to:

- contribute to school internet safety.
- uphold school policies relating to acceptable use of the internet and other communications technologies after completing the parent/pupil agreement form;
- report any incidents of ICT misuse to a member of the teaching staff;
- seek help or advice from a teacher or 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;

Parents

It is the responsibility of parents to

- sign and adhere to the parent/pupil consent form;
- ensure home internet access is carefully monitored.

We encourage parents to invest in internet security software.

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:

- Dial up access;
- Alternate broadband provision access;
- Wireless access to the internet via any other source other than our own;

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 closely by an adult and using only sites that have been previously reviewed by a member of the teaching staff. We regard supervision as having an adult in close proximity, regularly checking what is being accessed.

Our school policy towards search engines is that pupils are encouraged to search using normal search engines such as Google.

- The use of web sites that require any personal details, including email addresses, to be entered are expressly forbidden for pupil use, unless parental consent has been obtained previously;
- The download of copyrighted materials, including games and music, is forbidden.

In the event of exposure to inappropriate materials, our policy is for the teacher to turn the computer monitor off as swiftly as possible. The Child Protection Liaison Officer, Headteacher and member of the Internet Protection Team need then to be notified, in addition to 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. 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.

Monitoring of internet access and email use of school is partly carried out by the county system and Internet Safety Coordinator, 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

Electronic Communication

Our school policy regarding email is that only the county provided email system is to be used in school. This system is strictly filtered by the provider. The provider also ensures that alternate email providers such as 'Yahoo' are filtered to disable use in school. We advise all staff that a standard disclaimer to be attached to all email correspondence, stating that the views expressed are not necessarily those of the school or the LEA.

Only educational context video conferencing is permitted in school.

Mobile phones – pupils
Pupils are not permitted to use mobile phones in school.

Mobile phones – staff
Staff are not permitted to use mobile phones during lesson times. Staff may use mobile phones for personal calls outside of lesson time under the express condition that such calls take place without any pupils present in the room. 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 for taking pictures of pupils; school equipment should be used. (Please read in conjunction with the Frieth Mobile Phone Policy)

Image capturing devices used by parents
Clear signs should be on display and verbal advice given before performances to indicate the school has a policy whereby parents or visitors are permitted to take photographs of their own child at school functions but should avoid including other pupils. All parents and visitors are asked to abide by our policy of not putting pictures of other people's children or school events on social networking and internet sites.

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:

- No images of pupils to be used, unless parental permission granted;
- 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;
- 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.

Guidelines for Staff

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.

Appendix A

Frieth School Pupils' Internet Code of Practice

1. I will only use the internet when supervised by a teacher or adult.
2. I will log off when I have finished using the computer.
3. I know that my teacher can check the sites I have visited.
4. I understand that I can access only sites and materials relevant to my work in school.
5. I understand that I will not be able to use the Internet if I don't use it as expected by my teacher.
6. I know that information on the Internet may not always be reliable.
7. I know that the Headteacher can monitor the contents of my e-mail messages.
8. I will never tell anyone I meet on the Internet where I live.
9. I will never send anyone my picture.
10. I will never arrange to meet anyone in person.
11. I will never respond to unpleasant, suggestive or bullying e-mails or bulletin boards and I will always report it to a teacher or parent.
12. I will not use e-mail to send or encourage material which is inappropriate, illegal, offensive or annoying or invades another person's privacy.
13. I will not look for bad language or unpleasant images while I am online. I will turn off the monitor and tell a teacher or parent if I think something I come across accidentally is inappropriate.
14. I will always be myself and will not pretend to be anyone or anything I am not.
15. I know that the posting of anonymous messages and the forwarding of chain messages is not allowed.
16. I may not download anything from the Internet.